

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПОДАТКОВОЇ СЛУЖБИ УКРАЇНИ

Л. А. КУРДАЧЕНКО

В. В. КИРИЧЕНКО

М. М. СЕМКО

ВИБРАНІ РОЗДІЛИ **АЛГЕБРИ** ТА ТЕОРІЇ ЧИСЕЛ

*Рекомендовано Міністерством освіти
і науки України як навчальний посібник
для студентів вищих навчальних закладів,
які навчаються за спеціальностями
«Математика», «Статистика».*

СУЧАСНА АЛГЕБРА

УДК 519.41/47
ББК 22.14я73
К93

Гриф Міністерства освіти і науки України
Лист № 14/18.2-1341 від 09.06.05 р.

Рецензенти: д-р фіз.-мат. наук, проф. М. Ф. Кузенний (Інститут математики НАН України); д-р фіз.-мат. наук, проф. В. О. Устименко (Національний університет «Києво-Могилянська академія»).

Курдаченко Л. А.

К93 Вибрані розділи алгебри та теорії чисел: Навч. посіб. для студ. вищ. навч. закл., які навчаються за спец. «Математика», «Статистика» / Л. А. Курдаченко, В. В. Кириченко, М. М. Семко. — К.: [Ін-т математики НАН України], 2005. — 208 с.: іл. — (Сучасна алгебра). — **Бібліогр:** с. 207—208.

ISBN 966-337-036-X

Посібник охоплює всі основні базові поняття, результати та методи сучасного курсу алгебри та теорії чисел. Значна увага приділяється основним розділам алгебри, які повинен знати у наш час студент математичного відділення університету.

ББК 22.14я73+22.13я73

Всі права належать авторам. Будь-яке використання цього видання або його частин (фрагментів), такі як копіювання, тиражування, розповсюдження і т.п. можливе тільки за наявності попередньої письмової згоди авторів.

ISBN 966-337-036-X

© Л. А. Курдаченко, В. В. Кириченко, М. М. Семко, 2005

ЗМІСТ

ВСТУП	4
ЧАСТИНА 1	5
1. Множини, операції над множинами	5
2. Відображення множин	10
3. Добуток відображень, його властивості	19
4. Підстановки скінченних множин	24
ЧАСТИНА 2	33
5. Матриці, операції над матрицями	33
6. Визначники, їх елементарні властивості	41
7. Мінори, алгебричні доповнення, їх роль	48
8. Властивості операції множення матриць	57
ЧАСТИНА 3	66
9. Бінарні алгебричні операції, їх властивості	66
10. Групи	74
11. Приклади груп та підгруп	82
12. Відношення еквівалентності на множинах. Розклад групи в об'єднання суміжних класів	90
13. Нормальні підгрупи. Фактор-групи	98
14. Гомоморфізми груп	106
15. Кільця, підкільця, їх елементарні властивості. Приклади кілець	112
16. Ідеали кілець, фактор-кільця	124
17. Кільця поліномів та формальних степеневих рядів	137
18. Поле комплексних чисел	144
19. Кільце поліномів від кількох невідомих	155
ЧАСТИНА 4	159
20. Розширення арифметики на комутативні кільця	159
21. Евклідові кільця	173
22. Незвідні поліноми	177
23. Арифметичні функції	185
24. Конгруенції	194
ЛІТЕРАТУРА	207

ВСТУП

Метою цієї книги є викладання основних базових понять, результатів та методів сучасного курсу алгебри та теорії чисел. Ми старались викласти ці основи досить систематично і зробити цей виклад більш-менш сучасним із таких причин. Ситуація з підручниками з алгебри у більшості університетів України нині не є задовільною. У кінці книги ми наводимо перелік основних таких підручників. Розглядаючи його, можна побачити, що серед них немає підручників українською мовою. Також можна побачити, що вони були видані більше ніж 15 років тому. Це класичні, випробувані часом підручники. З їх допомогою алгебру вивчало і буде вивчати не одне покоління алгебристів. Але в нашої реальній ситуації весь цей набір підручників не є доступним для будь-якого студента. Тому кожен університет намагається самотужки вирішувати цю проблему. Автори цієї книги також не залишилися осторонь. Слід також зазначити, що за цей час дещо змінилися ролі різних математичних дисциплін. Зокрема, значно зросла роль дискретної математики. Це вказує на реальну потребу змінити акценти у викладанні курсу алгебри та теорії чисел. Ми виділили основні (на наш погляд) розділи алгебри, які повинен знати у наш час студент математичного відділення університету. Дана книга містить трохи більше необхідного мінімуму матеріалу. Все це дає підстави стверджувати, що за своїм потенціалом дана книга дає необхідний фундамент для подальшого більш глибокого вивчення курсу алгебри та теорії чисел.

Автори* висловлюють щире подяку співробітникам кафедри алгебри і геометрії Дніпропетровського національного університету та кафедри алгебри і математичної логіки Київського національного університету імені Тараса Шевченка, з якими вони обговорювали різні питання, висвітлені в даному посібнику. Автори особливо вдячні рецензентам проф. М. Ф. Кузенному і проф. В. О. Устименку за цінні зауваження та плідну співпрацю під час підготовки цього посібника до друку.

Автори сподіваються одержати від фахівців зауваження, рекомендації та побажання, спрямовані на покращення посібника при його подальшому виданні.

* 1. Курдаченко Леонід Андрійович, доктор фізико-математичних наук, професор, Заслужений діяч науки і техніки України, завідувач кафедри Дніпропетровського національного університету, e-mail: lkurdachenko@newmail.ru.

2. Кириченко Володимир Васильович, доктор фізико-математичних наук, професор, завідувач кафедри Київського національного університету імені Тараса Шевченка, e-mail: vkir@univ.kiev.ua.

3. Семко Микола Миколайович, доктор фізико-математичних наук, професор, професор Національної академії державної податкової служби України, e-mail: n_semko@mail.ru.

Частина перша

1

1. МНОЖИНИ, ОПЕРАЦІЇ НАД МНОЖИНАМИ

Поняття множини — одне з основних понять математики. Воно настільки загальне, що дуже важко запропонувати яке-небудь точне означення, яке б не зводилось до простої заміни слова «множина» одним з його синонімів: сукупність, сім'я, ансамбль, набір тощо.

Теорія множин може застосовуватись як бездоганний «будівельний матеріал» для побудови фундаменту математики в цілому лише тоді, коли вона викладається аксіоматично (зауважимо, що це саме справедливо і для багатьох інших розвинених математичних теорій). При аксіоматичному викладі теорії множин спочатку задаються основні поняття елемента і множини, які не мають жодних означень, а тільки пояснюються до певного рівня глибини. Після цього визначається бінарне відношення між множинами, яке виражає належність однієї з множин в якості елемента другої множини. Завершується побудова заданням деякого списку аксіом, які регламентують використання первісних понять і відношення між ними.

Але докладний виклад будь-якої з існуючих на сьогодні аксіоматичних теорій множин може досягти бажаної мети лише у разі значних затрат учбового часу і (що не менш важливо) за наявності певного досвіду слухачів у вивченні математичних дисциплін, які до того ж викладались на відповідному рівні строгості. Хоч в цьому підручнику відчутне бажання подати алгебричні поняття і факти з достатньо прозорим теоретико-множинним і логічним обґрунтуванням, автори не ставили перед собою мети досягти дуже високого рівня строгості викладу. Тому ми зупинимось на традиційному підході, при якому користуються лише, так званою, «наївною теорією множин».

Розглядаючи об'єкти будь-якої природи, часто доводиться з них усіх або ж з їх частини утворювати новий об'єкт — множину цих елементів. Згідно з ідеєю Кантора, множина — це будь-який набір

цілком визначених об'єктів, які добре розрізняються між собою та розглядаються як єдине ціле. Про ці об'єкти кажуть, що вони належать даній множині, складають дану множину або є елементами даної множини. Символічно твердження про належність об'єкта a як елемента до множини A записується таким чином: $a \in A$ (а його заперечення $a \notin A$). Вважатимемо, що для будь-якого елемента a і будь-якої множини A можливий лише один з двох варіантів: $a \in A$ або $a \notin A$. Це не що інше, як теоретико-множинний вираз добре відомого логічного закону — закону виключеного третього.

Істотним пунктом канторового «означення» є те, що набір предметів сам розглядається як один предмет (вважається єдиним цілим). Увага тут переводиться з окремих предметів на їх сукупності, які, в свою чергу, уявляються як предмети. Що ж стосується предметів, які можуть входити в множину, то формулювання не накладає жодних обмежень на їх природу. Множини можуть складатися, наприклад, з овочів, тварин, людей, математичних понять чи навіть з множин або їх сімей. Таке формулювання допускає розгляд множин, елементи яких з тих чи інших причин не можна точно вказати.

Як приклади таких множин можна взяти множину всіх простих чисел, множину вигуків «біс» на концерті М. Задорнова тощо. Тут також виникає питання, якого типу сукупності можна утворювати, чи існують тут які-небудь обмеження? Наступний класичний парадокс показує, що насправді без обмежень тут обійтись неможливо. Множини, елементи яких самі є множинами, надалі найчастіше називатимемо сім'ями множин.

Парадокс Рассела (1902). Як ми вже відзначали, множини можуть бути елементами інших множин. Більшість множин не є елементами самих себе. Наприклад, множина всіх студентів механіко-математичного факультету не є елементом самої себе, оскільки вона сама не є студентом механіко-математичного факультету. Проте, можлива і така множина, яка належить самій собі як елемент.

Як приклад можна розглянути множину всіх непорожніх множин. Нехай тепер X позначає множину всіх таких множин M , що $M \notin M$. За означенням, якщо $X \in X$, то X не може бути елементом X . Якщо ж $X \notin X$, то знову, за означенням множини X маємо $X \in X$. Отримали суперечливі висновки в обох випадках. Оскільки інших випадків не існує, то ми опинились в тупиковій ситуації.

Оскільки наведені міркування не викликають сумнівів, то залишається лише одне: множини типу множини всіх множин просто не можна розглядати взагалі (звичайно, якщо ми не бажаємо час від часу опинятись в тупикових ситуаціях). Але й відкидання множин такого типу не рятує ситуації, оскільки у нас немає гарантії того, що серед тих, які залишились, не знайдуться ще які-небудь «погані» множини.

Парадокс Рассела підкреслює складність становища людини, яка хоче викласти математику абсолютно строго і без посилання на набуті вже знання. Найпростіший компроміс, яким користуються майже всі, хто береться за написання підручників, полягає в тому, що автор лише обіцяє не виходити за рамки, які накладені аксіоматикою теорії множин, не наводячи самої цієї аксіоматики. Саме такої позиції будемо дотримуватися і ми в цьому підручнику.

Якщо число елементів множини A скінченне, то її можна задати шляхом явного переліку елементів:

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

Тут треба зауважити, що елемент a і множина $\{a\}$ — це різні об'єкти; $\{a\}$ — це множина, єдиним елементом якої є a («осібний»). Інший спосіб задання множин полягає у визначенні її як сукупності елементів за допомогою певної властивості, яка об'єднує їх в одну нову множину:

$$A = \{x \mid P(x)\},$$

де $P(x)$ скорочено позначає визначальну властивість, якою володіють всі елементи множини A . Наприклад, множину всіх дійсних чисел, які знаходяться в проміжку $[2, 5]$ можна записати у вигляді $\{x \mid x \in R \text{ і } 2 \leq x \leq 5\}$.

Цей спосіб задання множин відповідає так званому **принципу абстракції**, який Кантор і взяв за основу свого означення множини. За Кантором, якщо розглядається деяка властивість P , то завжди можна утворити новий об'єкт — «множину всіх об'єктів, які володіють властивістю P ». Можливість переходу від формулювання властивості до множини об'єктів, які володіють цією властивістю, якраз і складає суть принципу абстракції. Парадокс Рассела, проте, показує, що при виборі найбільш визначальних властивостей треба дотримуватись певних обмежень. Треба зауважити ще, що саме тут можуть нашкодити так звані лінгвістичні суперечності, навіть якщо ми, яким-небудь чином, обійдемо парадокс Рассела. Крім того, другий спосіб задання множин є більш загальним, хоча б тому, що, наприклад, скінченну множину з трьох елементів $\{1, 2, 3\}$ можна задати у вигляді $\{x \mid x = 1 \text{ або } x = 2 \text{ або } x = 3\}$. Для деяких особливо важливих і часто вживаних множин зручно мати стандартні позначення, які вводитимемо за потребою. Введемо такі стандартні позначення для числових множин:

N — множина всіх натуральних чисел;

Z — множина всіх цілих чисел;

Q — множина всіх раціональних чисел;

R — множина всіх дійсних чисел.

Число 0 за домовленістю не будемо вважати натуральним. Тому для позначення множини всіх натуральних чисел разом з числом 0 будемо використовувати символ N_0 .

Дві множини A і B вважаються рівними між собою, якщо вони складаються з одних і тих самих елементів, тобто кожний елемент множини A є елементом множини B і навпаки.

Це положення є однією з перших аксіом теорії множин, і його називають «принципом об'ємності». Разом з принципом абстракції воно вказує на істотну відмінність між поняттям властивості й поняттям множини: одна і та ж множина може визначатись різними властивостями. Дуже часто встановлення рівності множин, виділених різними властивостями, дає доведення деякої математичної теореми, яка може виявитись досить глибокою.

При розгляді множин закономірно виникає важлива спеціальна множина — *порожня множина*. Це множина, яка не містить жодного елемента. Принцип об'ємності показує, що порожня множина єдина. Її позначають символом $\emptyset$. Порожню множину можна також одержати за допомогою будь-якої суперечливої властивості, наприклад, $\emptyset = \{x \mid x \neq x\}$.

Нехай A і B — дві множини. Якщо кожний елемент множини A є елементом множини B , то кажуть, що A — підмножина B або B містить A .

Це записується в такий спосіб: $A \subseteq B$. Відразу отримуємо, що множини A і B рівні тоді і тільки тоді, коли $A \subseteq B$ і $B \subseteq A$. З означення безпосередньо випливає, що порожня множина є підмножиною будь-якої множини. Кожна множина є підмножиною самої себе.

Підмножина B множини A , відрізняючись від A , називається власною підмножиною множини A .

Дуже важливо не змішувати відношення належності як елемента до множини і відношення включення як підмножини $\subseteq$; якщо $\{a\} \subseteq A$, то $a \in A$ і навпаки; але з відношення $\{a\} \subseteq A$, взагалі кажучи, не випливає $\{a\} \in A$.

Нехай A — множина. Визначимо нову множину $B(A)$, елементами якої є всі підмножини множини A : $B(A) = \{X \mid X \subseteq A\}$. Множину $B(A)$ називають *буліаном* множини A .

Введемо тепер деякі операції над множинами.

Нехай A і B — дві множини. Елементи, які одночасно належать до множин A і B , утворюють нову множину $A \cap B$. Її називають *перетином* або *перерізом* множин A і B . Символічно означення перетину множин записується таким чином

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

Якщо $A \cap B = \emptyset$, то будемо говорити, що множини A і B не перетинаються.

Елементи, які належать принаймні одній з множин A або B , утворюють нову множину, яка називається *об'єднанням* множин A і B і позначається через $A \cup B$. Символічно,

$$A \cup B = \{x \mid x \in A \text{ або } x \in B\}.$$

Елементи, які належать множині A , але не належать множині B , утворюють нову множину, яка називається *різницею* множин A і B і позначається через $A \setminus B$,

$$A \setminus B = \{x \mid x \in A \text{ та } x \notin B\}.$$

Якщо $B \subseteq A$, то $A \setminus B$ називають *доповненням* підмножини B в A .

Елементи, які належать тільки множині A або тільки множині B , але не належать їх перетину, утворюють нову множину, яка називається *симетричною різницею* множин A і B і позначається через $A \Delta B$. Таким чином,

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

1.1. Теорема. Нехай A, B, C — множини.

- (1) $A \subseteq B$ тоді і тільки тоді, коли $A \cap B = A$ або $A \cup B = B$. Зокрема, $A \cup A = A = A \cap A$ (ідемпотентність об'єднання й перетину).
- (2) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (комутативність об'єднання й перетину).
- (3) $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$ (асоціативність об'єднання й перетину).
- (4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивність).
- (5) $A \setminus (A \setminus B) = A \cap B$.
- (6) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
- (7) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
- (8) $A \Delta B = B \Delta A$.
- (9) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$.
- (10) $A \Delta A = \emptyset$.

Д о в е д е н н я. Більша частина цих тверджень дуже проста, а тому наведемо доведення тільки деяких з них. Наприклад, твердження (4).

Нехай $x \in A \cap (B \cup C)$. Це означає, що $x \in A$ і $x \in B \cup C$. Оскільки $x \in B \cup C$, то $x \in B$ або $x \in C$. Таким чином, або x є елементом множин A і B , або x є елементом множин A і C . В кожному з випадків, $x \in (A \cap B) \cup (A \cap C)$.

Навпаки, нехай $x \in (A \cap B) \cup (A \cap C)$. Тоді $x \in A \cap B$ або $x \in A \cap C$. В кожному з випадків, $x \in A$ і x є елементом однієї з множин B або C , тобто $x \in A \cap (B \cup C)$.

Відзначимо ще важливе твердження (9). Для його доведення досить встановити що $A \Delta (B \Delta C) = ((A \cup B) \cup C) \setminus (((A \cap B) \cup (A \cap C)) \cup (B \cap C)) = (A \Delta B) \Delta C$.

Операції об'єднання й перетину можна розповсюдити на випадок будь-якої системи множин. Нехай S — система (або сім'я) множин (тобто множина, елементами якої є множини).

Об'єднанням системи множин S назвемо множину, кожний елемент якої належить хоча б одній множині S з системи S :

$$\cup S = \cup_{S \in S} S = \{x \mid x \in S \text{ для деякої підмножини } S \in S\}.$$

Перетином або перерізом системи множин S зветься множина, кожний елемент якої належить до кожної множини S , взятій з системи S :

$$\cap S = \cap_{S \in S} S = \{x \mid x \in S \text{ для будь-якої підмножини } S \in S\}.$$

Нехай A і B — дві множини. Пару елементів (a, b) , де $a \in A$ і $b \in B$, які беруться саме в такому порядку, називатимемо *впорядкованою парою*, вважаючи при цьому, що $(a, b) = (a_1, b_1)$ тоді і тільки тоді, коли $a = a_1$ і $b = b_1$.

Декартовим добутком множин A і B назвемо множину $A \times B$ всіх упорядкованих пар (a, b) , $a \in A$, $b \in B$. У випадку $A = B$ говоримо про *декартів квадрат* множини A і позначатимемо його через

A^2 . Природним прикладом декартового квадрату є дійсна площа R^2 . Декартів добуток двох відрізків дійсної прямої геометрично інтерпретується прямокутником, сторонами якого є ці відрізки. Інші приклади читач може запропонувати самостійно.

Означення декартового добутку двох множин природно узагальнюються на випадок довільного скінченного числа множин. Нехай $A_1, \dots, A_n$ — множини. *Декартовим добутком цих множин назовемо множину*

$$A_1 \times \dots \times A_n = \prod_{1 \leq i \leq n} A_i = \prod_{i=1}^n A_i$$

всіх впорядкованих наборів $(a_1, \dots, a_n)$, в кожному з яких i -й член, що зветься i -ю координатою, належить множині A_i , $1 \leq i \leq n$. У разі, коли всі множини $A_1, \dots, A_n$ збігаються, замість декартового добутку говорять про n -й декартів степінь A^n множини A . Так, зручно вважати, що для будь-якої не порожньої множини A множина A^0 є просто одноеlementною множиною і ми часто записуємо це так: $A^0 = \{*\}$, де $*$ позначає єдиний елемент множини A^0 . Аналогічно, природно $A^1 = A$. Варто ще відзначити, що для декартового множення множин так само, як і для піднесення їх до декартового степеня, звичні для множення й піднесення до степеня чисел закони, як правило, не виконуються, зокрема, не виконується закон комутативності: $A \times B \neq B \times A$, якщо $A \neq B$; не виконується і закон асоціативності: $A \times (B \times C)$, $(A \times B) \times C$ і $A \times B \times C$ — цілком різні множини. Перевірку справедливості інших загально відомих законів для цих операцій залишаємо читачеві на самостійне опрацювання.

2. ВІДОБРАЖЕННЯ МНОЖИН

Поняття відображення або функції відіграє одну з найсуттєвіших ролей в математиці. На рівні строгості, прийнятому нами, відображення найчастіше визначають наступним чином. Будемо говорити, що задано відображення з множини A в множину B , якщо кожному елементу множини A зіставляється (за яким-небудь правилом або законом) однозначно визначений елемент множини B . Можна було б обмежитись цим звичним для підручників означенням, не звертаючи уваги на те, що термін «зіставляений» залишився невизначеним. Однак, розвинутий до даного моменту понятійний апарат уже дозволяє визначити цей термін, тобто зробити визначення відображення досить строгим. Якщо ми намагатимемося сформулювати яке-небудь «життєве» означення відповідності, то справа зведеться до заміни його деяким синонімом. Тому доведеться йти дещо іншим шляхом. Вважатимемо відповідність заданою, якщо вказані всі пари об'єктів, зв'язаних цією відповідністю. Остаточного, приходимо до такого означення.

Нехай A і B — множини. *Відповідністю (точніше бінарною відповідністю) із A в B називається підмножина Φ декартового добутку*

$A \times B$. Якщо $A = B$, то замість відповідності говоритимемо про бінарне відношення, задане на множині A . Якщо $\alpha = (x, y) \in \Phi$, то говорять, що елементи x, y (у вказаному порядку) відповідають один одному при Φ .

Запис $(x, y) \in \Phi$ часто замінюватимемо на еквівалентний йому, але більш природний, $x \Phi y$. Елемент x називають проекцією на A елемента α , а елемент y — його проекцією на B (формалізацією цих висловлень виступають рівності $x = \text{pr}_A \alpha$, $y = \text{pr}_B \alpha$). Якщо $\Psi \subseteq \Phi$, то покладемо $\text{pr}_A \Psi = \{\text{pr}_A \alpha \mid \alpha \in \Psi\}$, $\text{pr}_B \Psi = \{\text{pr}_B \alpha \mid \alpha \in \Psi\}$.

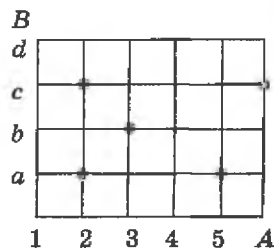
Наприклад, якщо A — множина всіх точок площини, B — множина всіх ліній площини, то відношення *інцидентності* (нагадаємо з геометрії, що за означенням, точка P інцидентна лінії λ , якщо P лежить на λ) визначає відповідність між множиною точок площини й множиною ліній на площині. При цьому кожній точці P відповідають всі лінії, які проходять через точку P , а кожній лінії λ відповідають точки, які лежать на λ . Це приклад, в якому кожному елементу множини A відповідає безмежна множина елементів з B . В загальному випадку фіксованому елементу з A може відповідати багато, один або жодного елемента з B .

Інший приклад. Нехай

$$A = \{1, 2, 3, 4, 5\}, B = \{a, b, c, d\},$$

$$\Phi = \{(1, a), (1, c), (2, b), (2, d), (4, a), (5, c)\}.$$

Відповідність Φ можна описати прямокутною таблицею наступним чином:



Тут елементам множини A відповідають вертикальні лінії, елементам множини B — горизонтальні, точки перетину цих ліній — це елементи множини $A \times B$, а наведеними точками тут позначені елементи з Φ .

Особливо важливий випадок для численних застосувань виникає, коли $A = B = R$, тобто тоді $A \times B = R^2$ — звичайна площина. Довільне відношення на R можна розглядати як деяку множину точок площини. Наприклад, відношення

$$\Phi = \{(x, y) \mid x^2 + y^2 = 1\}$$

графічно зображається колом з центром в початку координат і радіусом одиничної довжини.

Досить часто (особливо це важливо для випадку нескінченних множин) відповідність може задаватись якою-небудь властивістю $P(x, y)$, що зв'яже елементи множин A і B , тобто

$$\Phi = \{(x, y) \mid (x, y) \in A \times B \text{ і твердження } P(x, y) \text{ істинне}\}.$$

Це один з найбільш розповсюджених способів задання відпові-
дностей, який повсякчас використовується в математиці.

Відповідність Φ з множини A в множину B назовемо функціональною, якщо вона задовольняє наступним умовам:

(F1) для любого элемента $a \in A$ найдется такой элемент $b \in B$, что $(a, b) \in \Phi$;

(F2) якщо $(a, b) \in \Phi$ та $(a, c) \in \Phi$, то $b = c$.

Відображенням або функцією f з множини A в множину B називаємо трійку (A, B, Φ) , де Φ — функціональна відповідність з A в B . Множину A називають областю визначення відображення f , множину B — областю значень відображення f , а саму функціональну відповідність Φ — графіком відображення f і використовують позначення $\Phi = \text{Gr}(f)$.

Найчастіше функцію символічно записують у вигляді $f : A \rightarrow B$.

Умова (F1) означає, що $\text{pr}_A \Phi = A$. Таким чином, разом з умовою (F2) отримуємо, що відображення f ставить у відповідність кожному елементу $a \in A$ однозначно визначений елемент $b \in B$.

Однозначно визначений елемент $b \in B$, для якого $(a, b) \in \text{Gr}(f)$, будемо позначати через $f(a)$ і називати образом елемента a (відносно відображення f).

В деяких математичних дисциплінах, зокрема, в алгебрі, використовуються правосторонній запис для образу елемента; а саме, замість $f(a)$ пишуть af . Проте більшість математичних дисциплін використовують лівосторонній запис. Зважаючи на це, ми тут також будемо використовувати лівосторонній запис для образу елемента.

Будь-який елемент $a \in A$ має, і тільки один, образ відносно відображення f . Якщо $U \subseteq A$, то покладемо

$$f(U) = \{f(a) \mid a \in U\};$$

множину $f(U)$ називають образом підмножини U відносно відображення f . Образ $f(A)$ всієї множини A називають ще образом відображення f і позначають через $\text{Im} f$.

Якщо $b = f(a)$ для деякого елемента $a \in A$, то a називається прообразом елемента b (відносно відображення f). Елементи з множини B можуть мати декілька прообразів або взагалі не мати прообразів.

Якщо $V \subseteq B$, то покладемо

$$f^{-1}(V) = \{a \in A \mid f(a) \in V\};$$

множину $f^{-1}(V)$ називають повним прообразом підмножини V відносно відображення f .

Два відображення $f : A \rightarrow B$ і $g : C \rightarrow D$ збігаються тоді і тільки тоді, коли $A = C$, $B = D$ і $f(a) = g(a)$ для будь-якого елемента $a \in A$.

Відображення $f : A \rightarrow B$ називається ін'єктивним або ін'єкцією, якщо образи кожної пари різних елементів з A різні.

Відображення $f : A \rightarrow B$ називається сюр'єктивним (або сюр'єкцією), якщо $B = \text{Im} f$. Про сюр'єкцію кажуть ще, що вона відображає множину A на всю множину B .

Відображення $f : A \rightarrow B$ називається бієктивним (або бієкцією), якщо воно ін'єктивне й сюр'єктивне одночасно. Бієктивне відображення називають ще взаємно однозначним.

2.1. Твердження. Нехай $f : A \rightarrow B$ — відображення.

(1) f ін'єктивне тоді і тільки тоді, коли кожний елемент множини B або не має жодного прообраза, або ж має точно один прообраз в множині A .

(2) f сюр'єктивне тоді і тільки тоді, коли кожний елемент множини B має принаймні один прообраз в множині A .

(3) f бієктивне тоді і тільки тоді, коли кожний елемент множини B має точно один прообраз в множині A .

Ці твердження майже очевидні, тому строге доведення пропонуємо читачеві провести самостійно.

Будемо говорити, що множина A — скінченна, якщо знайдеться таке натуральне число n , що існує бієкція $A \rightarrow \{1, 2, \dots, n\}$. При цьому число n називається порядком множини A (позначення $|A| = n$, або більш розшифроване, $\text{Card } A = n$). Часом це число називають ще потужністю скінченної множини A , але причини такої назви стануть зрозумілими дещо пізніше, коли виникне необхідність підраховувати “кількість” елементів нескінченних множин.

2.2. Наслідок. Нехай A, B — скінченні множини, $f: A \rightarrow B$ — відображення.

(1) Якщо f ін'єктивне, то $|A| \leq |B|$.

(2) Якщо f сюр'єктивне, то $|A| \geq |B|$.

(3) Якщо f бієктивне, то $|A| = |B|$.

Якщо $f: A \rightarrow B$ — відображення, то воно індукує відображення множини $B(A)$ в множину $B(B)$, яке зіставляє підмножині $U \subseteq A$ її образ $f(U)$. Це відображення знову позначатимемо через f і називатимемо розширенням (або продовженням) вихідної функції на буліан множини A .

2.3. Теорема. Нехай $f: A \rightarrow B$ — відображення.

(1) Якщо $U \neq \emptyset$, то $f(U) \neq \emptyset$; $f(\emptyset) = \emptyset$.

(2) Якщо $X \subseteq U \subseteq A$, то $f(X) \subseteq f(U)$.

(3) Якщо $X, U \subseteq A$, то $f(X) \cup f(U) = f(X \cup U)$.

(4) Якщо $X, U \subseteq A$, то $f(X \cap U) \subseteq f(X) \cap f(U)$.

Ці твердження також майже очевидні. Відзначимо, що в (4) знак включення аж ніяк неможливо замінити знаком рівності. В цьому можна переконатися на такому прикладі.

Нехай $f: Z \rightarrow Z$ — відображення, визначене за правилом $f(x) = x^2$ для кожного $x \in Z$; X — множина всіх від'ємних цілих чисел, U — множина всіх додатних цілих чисел. Тоді $X \cap U = \emptyset$, а $f(X) \cap f(U)$ — множина всіх додатних чисел.

Відображення $f: A \rightarrow B$ індукує ще одне відображення $g: B(B) \rightarrow B(A)$, визначене у наступний спосіб: кожній підмножині $V \subseteq B$ ставиться у відповідність її повний прообраз $f^{-1}(V)$.

2.4. Теорема. Нехай $f: A \rightarrow B$ — відображення.

(1) Якщо $Y, V \subseteq B$, то $f^{-1}(Y \setminus V) = f^{-1}(Y) \setminus f^{-1}(V)$.

(2) Якщо $Y \subseteq V \subseteq B$, то $f^{-1}(Y) \subseteq f^{-1}(V)$.

(3) Якщо $Y, V \subseteq B$, то $f^{-1}(Y) \cup f^{-1}(V) = f^{-1}(Y \cup V)$.

(4) Якщо $Y, V \subseteq B$, то $f^{-1}(Y) \cap f^{-1}(V) = f^{-1}(Y \cap V)$.

Д о в е д е н н я. (1) Нехай $a \in f^{-1}(Y \setminus V)$. Це означає, що $f(a) \in Y \setminus V$, тобто $f(a) \in Y$ і $f(a) \notin V$. Але тоді $a \in f^{-1}(Y)$ і

$a \notin f^{-1}(V)$, отже, $a \in f^{-1}(Y) \setminus f^{-1}(V)$. Для отримання зворотного включення потрібно повторити ці ж міркування у зворотному порядку.

Твердження (2) очевидне.

(3) Нехай $a \in f^{-1}(Y) \cup f^{-1}(V)$, тоді $a \in f^{-1}(Y)$ або $a \in f^{-1}(V)$. В першому з випадків $f(a) \in Y$, а в другому $f(a) \in V$. В кожному разі $f(a) \in Y \cup V$, тобто $a \in f^{-1}(Y \cup V)$. Обернене включення утримується за допомогою цілком аналогічних міркувань.

Подібні міркування використовуються і для доведення твердження (4).

Відображення $\epsilon_A : A \longrightarrow A$, визначене за правилом $\epsilon_A(a) = a$ для кожного елемента $a \in A$, називається тотожним або одиничним. Якщо C — підмножина в A , то визначимо тотожне вкладення або канонічну ін'єкцію $j_C : C \longrightarrow A$ за правилом $j_C(c) = c$ для кожного елемента $c \in C$.

Нехай $f : A \longrightarrow B$, $g : C \longrightarrow D$ — відображення. Якщо $A \subseteq C$, $B \subseteq D$ і $f(a) = g(a)$ для будь-якого елемента $a \in A$, то f називається звуженням або обмеженням відображення g , і, в свою чергу, g називається розширенням або продовженням відображення f .

Наприклад, тотожне вкладення буде звуженням тотожного відображення.

Нехай A, B — множини. Сукупність всіх відображень з A в B позначатимемо через B^A . Припустимо, що A, B — скінченні, $|A| = k$, $|B| = n$. Кожне відображення $f : A \longrightarrow B$ однозначно задається образами всіх елементів з A , тобто впорядкованим набором k елементів з множини B . Навпаки, кожний такий набір визначає деяку функцію з A в B . Тепер залишається підрахувати кількість впорядкованих наборів елементів множини B довжини k . Очевидно, воно дорівнює n^k . Таким чином, $|B^A| = |B|^{|A|}$. Ця формула якраз і виправдовує вибір такого, на перший погляд не природного, позначення. Ми будемо його використовувати навіть тоді, коли множини A та B нескінченні.

Нехай A — множина, B — її підмножина. Характеристичною функцією підмножини B назовемо функцію $\chi_B : A \longrightarrow \{0, 1\}$, визначену за таким правилом:

$$\chi_B(a) = \begin{cases} 1, & \text{якщо } a \in B, \\ 0, & \text{якщо } a \notin B. \end{cases}$$

2.5. Теорема. Нехай A — множина. Відображення $B \longrightarrow \chi_B$ є бієкцією $B(A)$ на множину $\{0, 1\}^A$.

Д о в е д е н н я. Очевидно характеристична функція будь-якої підмножини з A буде елементом множини $\{0, 1\}^A$. Навпаки, нехай $f \in \{0, 1\}^A$, $C = \{c \in A \mid f(c) = 1\}$. Тоді $f = \chi_C$. Це означає, що відображення $B \longrightarrow \chi_B$ є сюр'єктивним. Покажемо, що воно також ін'єктивне. Нехай D, E — різні підмножини множини A , тоді або існує такий елемент $d \in D$, що $d \notin E$, або існує такий елемент $e \in E$, що $e \notin D$. В першому з випадків $\chi_D(d) = 1$, $\chi_E(d) = 0$, а в другому — $\chi_E(e) = 1$, $\chi_D(e) = 0$. В кожному разі, $\chi_D \neq \chi_E$.

2.6. Наслідок. Якщо множина A скінченна, то $|B(A)| = 2^{|A|}$.

Справді, з теореми 2.5 та наслідку 2.2 одержуємо рівність

$$|B(A)| = |\{0, 1\}|^{|A|} = 2^{|A|}.$$

Для будь-якої множини A існує ін'єкція A в $B(A)$. Вона отримується зіставленням елемента $a \in A$ підмножини $\{a\} \subseteq A$. Однак, справедлива наступна теорема.

2.7. Теорема (Г. Кантор). Нехай A — множина. Не існує сюр'єктивного відображення $A \longrightarrow B(A)$.

Д о в е д е н н я. Припустимо протилежне. Тоді існує сюр'єктивне відображення $f: A \longrightarrow B(A)$. Покладемо $B = \{a \in A \mid a \notin f(a)\}$. Оскільки B — підмножина A , то знайдеться елемент $b \in A$, для якого $B = f(b)$.

Припустимо, що $b \in B$, тобто $b \in f(b)$, а отже, $b \notin B$. Якщо ж $b \notin B = f(b)$, то з означення підмножини B випливає, що $b \in B$.

Отримана суперечність показує, що не існує сюр'єкції $A \longrightarrow B(A)$.

Множина A називається зліченною, якщо існує бієкція $f: N \rightarrow A$.

В цьому випадку покладемо $a_n = f(n)$, $n \in N$ і тоді

$$A = \{a_1, a_2, \dots, a_n, \dots\} = \{a_n \mid n \in N\}.$$

Іншими словами, елементи зліченної множини можна індексувати (занумерувати) натуральними числами.

Відзначимо деякі властивості злічених множин.

2.8. Теорема. (1) Кожна нескінченна множина містить зліченну підмножину.

(2) Кожна підмножина зліченної множини скінченна або зліченна.

(3) Множина $N \times N$ зліченна.

Д о в е д е н н я. (1) Нехай A — нескінченна множина, $a_1 \in A$. Тоді $A \setminus \{a_1\} \neq \emptyset$, а тому в цій підмножині можна вибрати елемент a_2 . Оскільки A нескінченна, то $A \setminus \{a_1, a_2\} \neq \emptyset$, а тому в ній можна вибрати елемент a_3 , і т.д. Цей процес не може обірватись завдяки нескінченності A , так що A містить зліченну підмножину $\{a_n \mid n \in N\}$.

(2) Нехай $A = \{a_n \mid n \in N\}$ — зліченна множина, $B \subseteq A$. В підмножині B виберемо елемент з найменшим номером і позначимо його через b_1 . Серед елементів, що залишились, знову вибираємо елемент з найменшим номером і позначаємо його b_2 і т.д. Якщо через скінченне число кроків цей процес зупиняється, то підмножина B скінченна. Якщо ж ні, то всі її елементи будуть занумерованими натуральними числами.

(3) Елементи декартового добутку $N \times N$ запишемо у вигляді наступної нескінченної таблиці

$$\begin{aligned}
 &(1, 1), (1, 2), (1, 3), \dots, (1, n), (1, n+1), \dots \\
 &(2, 1), (2, 2), (2, 3), \dots, (2, n), (2, n+1), \dots \\
 &\dots\dots\dots \\
 &(k, 1), (k, 2), (k, 3), \dots, (k, n), (k, n+1), \dots \\
 &\dots\dots\dots
 \end{aligned}$$

Розглянемо наступні підмножини D_n — “діагоналі” —

$$D_n = \{(k, t) \mid k + t = n\}.$$

Розмістимо підмножини D_n за зростанням їх номерів, а в середині кожної з цих підмножин нумерацію введемо за першими індексами. Тоді вся множина $N \times N$ виявиться занумерованою натуральними числами:

$$\begin{aligned}
 &(1, 1) \rightarrow (1, 2), (2, 1) \rightarrow (1, 3), (2, 2), (3, 1) \rightarrow \dots \rightarrow \\
 &\rightarrow (1, n), (2, n-1), (3, n-2), \dots, (n, 1) \rightarrow \dots
 \end{aligned}$$

Твердження (1) теореми 2.8 показує, що множина натуральних чисел (в деякому розумінні) — «найменша нескінченна множина».

2.9. Наслідок. Нехай A, B — множини. Якщо A — зліченна і існує ін'єктивне відображення $f: B \rightarrow A$, то B — скінченна або зліченна множина.

Д о в е д е н н я. Розглянемо відображення $f_1: B \rightarrow \text{Im } f$, визначене за правилом $f_1(b) = f(b)$ для будь-якого елемента $b \in B$. За побудовою f_1 — сюр'єктивне. Оскільки f — ін'єктивне, то і f_1 — ін'єктивне, а отже, f_1 — бієктивне.

Наостанок, з теореми 2.8 отримуємо, що $\text{Im } f$ — скінченна або зліченна.

2.10. Наслідок. Якщо $A = \bigcup_{n \in N} A_n$ і множина A_n скінченна або зліченна при будь-якому $n \in N$, то множина A також зліченна.

Д о в е д е н н я. Множина A_1 скінченна або зліченна, а тому

$$A_1 = \{a_n \mid n \in \Sigma_1\},$$

де або $\Sigma_1 = N$, або $\Sigma_1 = \{1, 2, \dots, k\}$ для деякого $k \in N$. Введемо для її елементів подвійне індексування, задаючи $b_{1n} = a_n$, $n \in \Sigma_1$.

Тоді $A_2 \setminus A_1$ скінченна або зліченна за теоремою 2.8, отже

$$A_2 \setminus A_1 = \{a_n \mid n \in \Sigma_2\},$$

де або $\Sigma_2 = N$, або $\Sigma_2 = \{1, 2, \dots, t\}$ для деякого $t \in N$. Для цієї множини також уведемо подвійне індексування, задаючи $b_{2n} = a_n$, $n \in \Sigma_2$.

Аналогічно індексуємо і множину $A_3 \setminus (A_2 \cup A_1)$ і т.д. В результаті одержимо: $A = \{b_{ij} \mid (i, j) \in \Xi\}$, де Ξ — деяка підмножина множини $N \times N$.

Очевидно, відображення $b_{ij} \rightarrow (i, j)$ буде ін'єктивним, і тепер можна скористатись наслідком 2.9 та теоремою 2.8.

2.11. Наслідок. Множина $\mathbb{Z}$ зліченна.**2.12. Наслідок. Множина $\mathbb{Q}$ зліченна.**

Справді, візьмемо $A_n = \{k/t \mid |k| + |t| = n\}$, тоді кожна підмножина A_n скінченна і $A = \bigcup_{n \in \mathbb{N}} A_n$, так що можна застосувати наслідок 2.10.

З теореми 2.7 випливає, що множина $B(\mathbb{N})$ не є зліченною. Теорема 2.5 показує, що і множина $\{0, 1\}^{\mathbb{N}}$ незліченна. Кожний елемент з $\{0, 1\}^{\mathbb{N}}$ можна ототожнити зі зліченною послідовністю, елементами якої є числа 0, 1. Кожній такій послідовності $(a_1, a_2, \dots, a_n, \dots)$ можна поставити у відповідність дійсне число $0, a_1 a_2 \dots a_n \dots$ з множини $[0, 1]$, зображене у десятковому запису. Звідси отримуємо незліченність множини $[0, 1]$, а, отже, і незліченність множини всіх дійсних чисел.

Наслідок 2.2 показує, що для встановлення того факту, що дві скінченні множини мають однакову кількість елементів, зовсім не потрібно вміти рахувати. Досить встановити взаємно однозначну відповідність між ними. Ця обставина якраз і стала справжнім джерелом виникнення абстрактного поняття числа. Розповсюдивши це спостереження на довільні множини, прийдемо до фундаментального поняття потужності множини.

Дві множини A і B називають *рівнопотужними*, якщо існує бієкція $f: A \longrightarrow B$. Цей факт будемо позначати наступним чином $|A| = |B|$.

Якщо A і B — скінченні множини, то їх рівнопотужність означає, що ці множини містять однакове число елементів. Тому Кантор і запропонував визначити загальне поняття кардинального числа, як те спільне, що мають рівнопотужні множини. Тепер можливо ввести деякий порядок між кардинальними числами.

Будемо говорити, що *потужність множини A не перевищує потужності множини B* (позначення $|A| \leq |B|$), якщо існує ін'єктивна функція $f: A \longrightarrow B$.

У цьому сенсі потужність, що відповідає зліченим множинам, є найменшою серед потужностей нескінченних множин, як показує теорема 2.8. Не будемо надто глибоко занурюватись в проблеми кардинальної арифметики, хоч це, безперечно, дуже захоплюючий розділ теорії множин. Але вважаємо за доцільне у завершення навести ще один важливий результат.

2.13. Теорема (Г. Кантор, Ф. Бернштейн). Нехай A і B — такі множини, що $|A| \leq |B|$ і $|B| \leq |A|$. Тоді $|A| = |B|$.

Доведення. Не обмежуючи загальності можна вважати, що вказані множини мають пустий перетин. Нехай $f: A \longrightarrow B$ та $g: B \longrightarrow A$ — ін'єктивні функції. Розглянемо довільний елемент $a \in A$. Тоді або $a \in \text{Im } g$ і в цьому випадку $a = g(b)$ для деякого елемента $b \in B$, або $a \notin \text{Im } g$. У першому випадку з ін'єктивності g випливає, що елемент b , для якого $a = g(b)$, буде єдиним або $b = f(a_1)$ для деякого елемента $a_1 \in A$, причому елемент a_1 з цією властивістю буде

єдиним, або $b \notin \text{Im } f$. Для елемента $x \in A$ визначимо послідовність $(x_n)_{n \in \mathbb{N}}$ за наступним правилом. Покладемо $x_0 = x$. Припустимо, що елемент x_n вже визначений. Якщо число n є парним, то x_{n+1} — це (єдиний) елемент множини B , для якого $x_n = g(x_{n+1})$. Якщо ж такого елемента не існує, то послідовність не продовжується. Якщо число n є непарним, то x_{n+1} — це (єдиний) елемент множини A , для якого $x_n = f(x_{n+1})$. Якщо ж такого елемента не існує, то послідовність не продовжується. Є можливими тільки наступні два варіанти.

Знайдеться такий номер n , що елемента x_{n+1} не існує. У цьому випадку число n будемо називати глибиною елемента x .

Послідовність $(x_n)_{n \in \mathbb{N}}$ є нескінченною. При цьому кількість різних елементів x_n може бути і скінченною: ці елементи можуть зациклюватись, утворюючи нескінченну послідовність, що містить тільки скінченну множину попарно різних елементів. У цьому випадку будемо говорити, що елемент x має нескінченну глибину.

Розіб'ємо тепер множину A на три підмножини: A_E , що складається з елементів парної глибини, A_O , що складається з елементів непарної глибини, та A_∞ , що складається з елементів нескінченної глибини. За аналогічним принципом розіб'ємо і множину B на три підмножини: B_E , B_O та B_∞ . З побудови цих підмножин випливає, що обмеження f на A_E буде бієкцією між A_E та B_O , обмеження f на A_∞ буде бієкцією між A_∞ та B_∞ . Далі, якщо $x \in A_O$, то існує такий елемент $y \in B_E$, що $g(y) = x$. Визначимо тепер функцію $h: A \rightarrow B$

$$h(x) = \begin{cases} f(x), & x \in A_E, \\ f(x), & x \in A_\infty, \\ y, & x \in A_O. \end{cases}$$

Неважко тепер упевнитись у тому, що відображення h буде бієктивним.

Щоб проілюструвати той факт, як мова множин та функцій може бути використана для опису деяких інформаційних систем, розглянемо коротенько *автомати*. Не вдаючись до загальної теорії, обмежимося тільки наступним.

Автомат — це абстрактний пристрій, що є основною моделлю для цифрових комп'ютерів. Він складається з вхідної стрічки, вихідної стрічки та голівки, яка здатна читати символи на вхідній стрічці та друкувати символи на вихідній стрічці. В будь-який момент часу система знаходиться в одному з можливих станів. Коли автомат читає символ на вхідній стрічці, він переходить до іншого стану і пише символ на вихідній стрічці. Отже, визначимо *автомат* A як набір

$$(I, O, S, v, \sigma),$$

де I та O — множини вхідних та вихідних символів відповідно, S — множина станів, $v: I \times S \rightarrow O$ — вихідна функція, $\sigma: I \times S \rightarrow S$ — функція переходу до наступного стану.

Автомат працює наступним чином. Якщо він знаходиться у стані $s \in S$ та читає вхідний символ $j \in I$, він друкує символ $n(j, s)$ на вихідній стрічці та переходить до стану $s(j, s)$. Таким чином, його режим роботи визначається трьома множинами I, O, S та двома функціями v, σ .

1

3. ДОБУТОК ВІДОБРАЖЕНЬ, ЙОГО ВЛАСТИВОСТІ

Нехай $f: A \longrightarrow B$ та $g: C \longrightarrow D$ — відображення. Добуток (інколи кажуть суперпозиція, або композиція) цих відображень визначений тільки у випадку, коли область визначення g збігається з областю значень f , тобто $C = B$. Тоді добуток $h = g \odot f$ — це відображення множини A у множину D , що визначене за наступним правилом:

$$g \odot f(a) = g(f(a)) \text{ для кожного } a \in A.$$

Точніше кажучи, спочатку на кожний елемент $a \in A$ діє відображення f , а потім на його образ діє відображення g . Оскільки ми домовились використовувати лівосторонній запис, то логічніше було б записувати цей добуток у зворотному порядку. Такий порядок використовується у випадку, коли застосовується правосторонній запис для позначення образу елемента: $a(fg) = (af)g$. Нам буде зручно користуватись цією формою запису при множенні підстановок.

Будемо говорити, що відображення f і g *перестановочні* (або *комутують*), якщо $g \odot f = f \odot g$.

Перестановочність відображень — це ситуація, яка не так часто трапляється. Справді, нехай $f: A \longrightarrow B$ та $g: C \longrightarrow D$. Добуток $g \odot f$ визначений, якщо $B = C$, а добуток $f \odot g$ визначений, якщо $A = D$. Отже, щоб існували обидва добутки $g \odot f$ та $f \odot g$, потрібно щоб виконувались рівності $A = D$ та $B = C$, тобто $f: A \longrightarrow B$ та $g: B \longrightarrow A$. У цьому випадку $g \odot f: A \longrightarrow A$, а $f \odot g: B \longrightarrow B$. Таким чином, якщо $A \neq B$, то $g \odot f \neq f \odot g$. Нарешті, нехай $A = B$. Якщо множина A складається більше ніж з двох елементів, то завжди можна знайти такі відображення $f: A \longrightarrow A$ та $g: A \longrightarrow A$, що $g \odot f \neq f \odot g$. Справді, виберемо у множині A три різних елементи a_1, a_2, a_3 і визначимо f за наступним правилом:

$$f(a_1) = a_2, f(a_2) = a_3, f(a_3) = a_1 \text{ та } f(x) = x, \text{ якщо } x \notin \{a_1, a_2, a_3\};$$

$$g(a_1) = a_3, g(a_2) = a_2, g(a_3) = a_1 \text{ та } g(x) = x, \text{ якщо } x \notin \{a_1, a_2, a_3\}.$$

Тоді маємо $g \odot f(a_1) = g(f(a_1)) = g(a_2) = a_2$, а $f \odot g(a_1) = f(g(a_1)) = f(a_3) = a_1$, тому знову $g \odot f \neq f \odot g$.

Але інша важлива властивість — асоціативність — все ж має місце.

3.1. Теорема. Нехай $f: A \longrightarrow B$, $g: B \longrightarrow C$, $h: C \longrightarrow D$ — довільні відображення. Тоді $h \odot (g \odot f) = (h \odot g) \odot f$.

Доведення. Справді, спочатку утворимо композиції $g \odot f: A \rightarrow C$, $h \odot g: B \rightarrow D$, та $h \odot (g \odot f): A \rightarrow D$, $(h \odot g) \odot f: A \rightarrow D$. Якщо a — довільний елемент множини A , то

$$\begin{aligned}(h \odot (g \odot f))(a) &= h((g \odot f)(a)) = h(g(f(a))) \text{ і } ((h \odot g) \odot f)(a) = \\ &= (h \odot g)(f(a)) = h(g(f(a))).\end{aligned}$$

Це і доводить потрібну рівність $h \odot (g \odot f) = (h \odot g) \odot f$.

Нехай $f: A \longrightarrow B$ — відображення. Легко переконатись, що виконуються такі рівності $\varepsilon_B \odot f = f \odot \varepsilon_A = f$, тобто відображення ε_B та ε_A відіграють роль лівого та правого одиничного елементів відносно операції множення відображень. Також очевидно, що не існує жодного “універсального” одиничного елемента для всіх відображень.

3.2. Лема. Нехай $f: A \longrightarrow B$, $g: B \longrightarrow A$ — відображення. Якщо $g \odot f = \varepsilon_A$, то відображення f буде ін’єктивним, а відображення g — сюр’єктивним.

Доведення. Припустимо, що в множині A існують такі елементи a, c , що $a \neq c$, але $f(a) = f(c)$. Тоді маємо

$$a = \varepsilon_A(a) = g \odot f(a) = g(f(a)) = g(f(c)) = g \odot f(c) = \varepsilon_A(c) = c.$$

Ця суперечність доводить, що f — ін’єктивне відображення. Нехай u — довільний елемент множини A , тоді знову

$$u = \varepsilon_A(u) = g \odot f(u) = g(f(u)),$$

тобто $f(u)$ є прообразом елемента u відносно відображення g . А це якраз і означає, що $\text{Im } g = A$.

Нехай $f: A \longrightarrow B$ — відображення. Відображення $g: B \longrightarrow A$ називається *лівим оберненим до f* (або *ретракцією, асоційованою з f*) (відповідно *правим оберненим до f* або *розрізом, асоційованим з f*), якщо $g \odot f = \varepsilon_A$ (відповідно $f \odot g = \varepsilon_B$).

3.3. Теорема. Нехай $f: A \longrightarrow B$ — відображення. Ліве обернене (відповідно праве обернене) до f існує тоді і тільки тоді, коли відображення f буде ін’єктивним (відповідно сюр’єктивним).

Доведення. Якщо існує відображення g з властивістю $g \odot f = \varepsilon_A$, то з леми 3.2 випливає ін’єктивність f . Навпаки, припустимо, що f є ін’єктивним. У множині A виберемо та зафіксуємо деякий елемент u . Якщо $b \in \text{Im } f$, то елемент a має єдиний прообраз. Покладемо

$$g(b) = \begin{cases} a, \text{ де } f(a) = b, & \text{якщо } b \in \text{Im } f, \\ u, & \text{якщо } b \notin \text{Im } f. \end{cases}$$

Зважаючи на таке задання відображення g , для кожного елемента $a \in A$ маємо тепер

$$g \odot f(a) = g(f(a)) = a = \varepsilon_A(a),$$

тобто g — ліве обернене до f .

Нехай тепер f — сюр'єктивне відображення. Тоді $f^{-1}(b) \neq \emptyset$ для кожного елемента $b \in B$. У кожній підмножині $f^{-1}(b)$ виберемо та зафіксуємо деякий елемент a_b та покладемо $g(b) = a_b$. Тоді одержимо

$$f \odot g(b) = f(g(b)) = f(a_b) = b = \varepsilon_B(b),$$

тобто $f \odot g = \varepsilon_B$. Це означає, що g — обернене справа до f . Навпаки, якщо існує відображення g з властивістю $f \odot g = \varepsilon_B$, то з леми 3.2 випливає сюр'єктивність f .

3.4. Теорема. Нехай $f: A \longrightarrow B$, $f_1: B \longrightarrow C$ — відображення $f_2 = f_1 \odot f$.

(1) Якщо відображення f та f_1 — ін'єктивні, то їх добуток f_2 також ін'єктивний. Якщо g та g_1 — ліві обернені до f та f_1 відповідно, то $g_2 = g \odot g_1$ буде лівим оберненим до f_2 .

(2) Якщо відображення f та f_1 — сюр'єктивні, то їх добуток f_2 також сюр'єктивний. Якщо g та g_1 — праві обернені до f та f_1 відповідно, то $g_2 = g \odot g_1$ буде правим оберненим до f_2 .

(3) Якщо відображення f_2 — ін'єктивне, то f також ін'єктивне. Якщо g_2 — ліве обернене до f_2 , то $g_2 \odot f_1$ буде лівим оберненим до f .

(4) Якщо відображення f_2 — сюр'єктивне, то f_1 також сюр'єктивне. Якщо g_2 — праве обернене до f_2 , то $f \odot g_2$ буде правим оберненим до f_1 .

(5) Якщо відображення f_2 — сюр'єктивне, а f_1 — ін'єктивне, то f — сюр'єктивне. Якщо g_2 — праве обернене до f_2 , то $g_2 \odot f_1$ буде правим оберненим до f .

(6) Якщо відображення f_2 — ін'єктивне, а f — сюр'єктивне, то f_1 — ін'єктивне. Якщо g_2 — ліве обернене до f_2 , то $f \odot g_2$ буде лівим оберненим до f_1 .

Доведення. (1) Нехай a_1, a_2 — два різних елементи множини A . Оскільки відображення f є ін'єктивним, то $f(a_1) = b_1 \neq b_2 = f(a_2)$. Відображення f_1 також є ін'єктивним, тому $f_1(b_1) \neq f_1(b_2)$. Отже,

$$\begin{aligned} f_2(a_1) &= f_1 \odot f(a_1) = f_1(f(a_1)) = f_1(b_1) \neq f_1(b_2) = f_1(f(a_2)) = \\ &= f_1 \odot f(a_2) = f_2(a_2), \end{aligned}$$

так що і f_2 є ін'єктивним. Оскільки $g \odot f = \varepsilon_A$, $g_1 \odot f_1 = \varepsilon_B$, то маємо

$$\begin{aligned} (g \odot g_1) \odot f_2 &= (g \odot g_1) \odot (f_1 \odot f) = g \odot (g_1 \odot f_1) \odot f = \\ &= g \odot \varepsilon_B \odot f = g \odot f = \varepsilon_A, \end{aligned}$$

тобто $g \odot g_1$ — ліве обернене до $f_1 \odot f$.

(2) Оскільки відображення f_1 є сюр'єктивним, то $C = \text{Im } f_1$. Якщо $c \in C$, то існує такий елемент $b \in B$, що $f_1(b) = c$. Оскільки відображення f є сюр'єктивним, то $b = f(a)$ для деякого елемента $a \in A$. Отже,

$$c = f_1(b) = f_1(f(a)) = f_1 \odot f(a) = f_2(a),$$

тобто f_2 також сюр'єктивне. Оскільки $f \odot g = \varepsilon_B$, $f_1 \odot g_1 = \varepsilon_C$, то маємо

$$\begin{aligned} f_2 \odot (g \odot g_1) &= (f_1 \odot f) \odot (g \odot g_1) = f_1 \odot (f \odot g) \odot g_1 = \\ &= f_1 \odot \varepsilon_B \odot g_1 = f_1 \odot g_1 = \varepsilon_C, \end{aligned}$$

тобто $g \odot g_1$ — обернене справа до $f_1 \odot f$.

(3) Припустимо, що існують різні елементи $a_1, a_2 \in A$, для яких $f(a_1) = f(a_2)$. Тоді маємо і $f_1(f(a_1)) = f_1(f(a_2))$, тобто

$$f_2(a_1) = f_1 \odot f(a_1) = f_1(f(a_1)) = f_1(f(a_2)) = f_1 \odot f(a_2) = f_2(a_2),$$

що суперечить ін'єктивності відображення f_2 . Ця суперечність доводить ін'єктивність відображення f . Далі, $g_2 \odot f_2 = \varepsilon_A$, так що отримуємо

$$\begin{aligned} (g_2 \odot f_1) \odot f &= g_2 \odot (f_1 \odot f) = g_2 \odot f_2 = \varepsilon_A, \\ g \odot (g_1 \odot f_1) \odot f &= g \odot \varepsilon_B \odot f = g \odot f = \varepsilon_A, \end{aligned}$$

тобто $g_2 \odot f_1$ — ліве обернене до f .

(4) Оскільки відображення f_2 є сюр'єктивним, то для кожного елемента $c \in C$ існує такий елемент $a \in A$, що $f_2(a) = c$. Але ж

$$c = f_2(a) = f_1 \odot f(a) = f_1(f(a)),$$

так що $f_1^{-1}(c) \neq \emptyset$ для кожного елемента $c \in C$. Це означає, що відображення f_1 є сюр'єктивним. Далі $f_2 \odot g_2 = \varepsilon_C$, і тому

$$f_1 \odot (f \odot g_2) = (f_1 \odot f) \odot g_2 = f_2 \odot g_2 = \varepsilon_C,$$

тобто $f \odot g_2$ — праве обернене до f_1 .

(5) З щойно доведеного твердження (4) випливає, що відображення f_1 є сюр'єктивним, тобто воно є бієктивним. Нехай $b \in B$ та $c = f_1(b)$. Оскільки відображення f_2 є сюр'єктивним, то існує такий елемент $a \in A$, що $f_2(a) = c$. Але ж $c = f_2(a) = f_1 \odot f(a) = f_1(f(a))$, тобто $f(a) \in f_1^{-1}(c)$. Також маємо $b \in f_1^{-1}(c)$, і з того факту, що відображення f_1 є бієктивним, отримуємо рівність $b = f(a)$, тобто f — сюр'єктивне. Далі $f_2 \odot g_2 = \varepsilon_C$, і оскільки f_1 є бієкцією, то для нього існує ліве обернене g_1 , тобто $g_1 \odot f_1 = \varepsilon_B$. Тому

$$\begin{aligned} f \odot (g_2 \odot f_1) &= (\varepsilon_B \odot f) \odot (g_2 \odot f_1) = (g_1 \odot f_1) \odot f \odot (g_2 \odot f_1) = \\ &= g_1 \odot ((f_1 \odot f) \odot g_2) \odot f_1 = g_1 \odot (f_2 \odot g_2) \odot f_1 = g_1 \odot \varepsilon_C \odot f_1 = \\ &= g_1 \odot f_1 = \varepsilon_B, \end{aligned}$$

тобто $g_2 \odot f_1$ — праве обернене до f .

(6) З уже доведеного твердження (3) тепер випливає, що відображення f є ін'єктивним, тобто воно є бієктивним. Нехай b_1, b_2 — два різних елементи множини B . Оскільки відображення f є бієктивним, то існують такі різні елементи $a_1, a_2 \in A$, що $b_1 = f(a_1)$, $b_2 = f(a_2)$. Оскільки f_2 — ін'єктивне, то $f_2(a_1) \neq f_2(a_2)$. У свою чергу,

$$f_1(b_1) = f_1(f(a_1)) = f_2(a_1) \neq f_2(a_2) = f_1(f(a_2)) = f_1(b_2),$$

отже, f_1 — ін'єктивне.

Далі $g_2 \odot f_2 = \varepsilon_A$, і оскільки f є бієкцією, то для нього існує праве обернене g , тобто $f \odot g = \varepsilon_B$. Тому

$$\begin{aligned} (f \odot g_2) \odot f_1 &= (f \odot g_2) \odot f_1 \odot \varepsilon_B = (f \odot g_2) \odot f_1 \odot (f \odot g) = \\ &= (f \odot g_2) \odot (f_1 \odot f) \odot g = f \odot (g_2 \odot f_2) \odot g = f \odot \varepsilon_A \odot g = f \odot g = \varepsilon_B, \end{aligned}$$

тобто $f \odot g_2$ — ліве обернене до f_1 .

Нехай A — множина. Відображення множини A в себе будемо називати *перетворенням* множини A , або її ендоморфізмом. Для сукупності всіх перетворень множини A будемо вживати такі позначення: $P(A)$, A^A або $\text{End}(A)$, залежно від того, яку з властивостей цієї сукупності ми хочемо в даний момент підкреслити. Зауважимо, що добуток будь-якої пари перетворень множини A завжди визначений. Ця операція буде асоціативною і відносно неї існує одиничний елемент — тотожне перетворення ε_A .

Нехай $f : A \longrightarrow B$ — відображення. Відображення $g : B \longrightarrow A$ називається *оберненим до f* , якщо воно є одночасно лівим та правим оберненим до f , тобто якщо $g \odot f = \varepsilon_A$ та $f \odot g = \varepsilon_B$.

З теореми 3.3 випливає, що відображення, обернене до f , існує тоді і тільки тоді, коли f є бієктивним. Обернене відображення, якщо воно існує, буде єдиним. Справді, нехай $g : B \longrightarrow A$ та $h : B \longrightarrow A$ — відображення, що мають властивості $g \odot f = \varepsilon_A$, $f \odot g = \varepsilon_B$ та $h \odot f = \varepsilon_A$, $f \odot h = \varepsilon_B$. Розглянемо наступний добуток $g \odot f \odot h$. Враховуючи асоціативність, яка має місце за теоремою 3.1, маємо

$$h = \varepsilon_A \odot h = (g \odot f) \odot h = g \odot (f \odot h) = g \odot \varepsilon_B = g.$$

Теорема 3.3 також указує шлях до побудови оберненого відображення до бієкції $f : A \longrightarrow B$. Якщо b — довільний елемент множини B , то існує єдиний елемент $a \in A$, для якого $f(a) = b$. Покладемо $g(b) = a$. Тоді маємо

$$g \odot f(a) = g(f(a)) = g(b) = a = \varepsilon_A(a),$$

$$f \odot g(b) = f(g(b)) = f(a) = b = \varepsilon_B(b),$$

так що дійсно $g \odot f = \varepsilon_A$ та $f \odot g = \varepsilon_B$. Оскільки обернене відображення до бієкції $f : A \longrightarrow B$ є єдиним, для нього будемо використовувати наступне позначення f^{-1} (не треба плутати з повним прообразом!). Слід відзначити, що f^{-1} також буде бієкцією (це випливає з леми 3.2).

Нехай A — множина. Бієктивне відображення множини A в себе надалі називатимемо *підстановкою* множини A . Сукупність всіх підстановок множини A позначатимемо через $S(A)$. Якщо $\varphi, \psi \in S(A)$, то з теореми 3.4 випливає, що добуток $\varphi \odot \psi$ буде бієктивним відображенням, тобто $\varphi \odot \psi \in S(A)$. Множення підстановок є асоціативним, одиничне відображення ε_A буде підстановкою. Нарешті, якщо $\varphi \in S(A)$, то для φ існує обернене відображення φ^{-1} , яке також буде підстановкою множини A . Ці три властивості дають нам можливість говорити, що $S(A)$ буде групою відносно операції множення підстановок. Тому далі ми будемо говорити про неї як про групу підстановок множини A .

4. ПІДСТАНОВКИ СКІНЧЕННИХ МНОЖИН

Нехай A — скінченна множина, $A = \{a_1, a_2, \dots, a_n\}$, π — підстановка множини A . Оскільки відображення π є ін'єктивним, то елементи $\pi(a_1), \pi(a_2), \dots, \pi(a_n)$ попарно різні. Отже,

$$|\{\pi(a_1), \pi(a_2), \dots, \pi(a_n)\}| = |\{a_1, a_2, \dots, a_n\}|.$$

Оскільки

$$\{\pi(a_1), \pi(a_2), \dots, \pi(a_n)\} \subseteq \{a_1, a_2, \dots, a_n\},$$

то звідси отримуємо рівність

$$\{\pi(a_1), \pi(a_2), \dots, \pi(a_n)\} = \{a_1, a_2, \dots, a_n\}.$$

Нехай $\pi(a_i) = a_{j(i)}$, $1 \leq i \leq n$. Розглянемо перетворення π_0 множини $\{1, 2, \dots, n\}$, що визначається за наступним правилом:

$$\pi_0(1) = j(1), \pi_0(2) = j(2), \dots, \pi_0(n) = j(n).$$

Нехай $k \neq t$. Оскільки $a_k \neq a_t$, $a_{j(k)} = \pi(a_k) \neq \pi(a_t) = a_{j(t)}$, тобто

$$\pi_0(k) = j(k) \neq j(t) = \pi_0(t).$$

Якщо $1 \leq m \leq n$, то $a_m \in A$. Оскільки відображення π — сюр'єктивне, то $a_m = \pi(a_s)$, де також $1 \leq s \leq n$. Але $\pi(a_s) = a_{j(s)}$, отже, $m = j(s) = \pi_0(s)$. Таким чином, π_0 — підстановка множини $\{1, 2, \dots, n\}$.

Навпаки, якщо σ — підстановка множини $\{1, 2, \dots, n\}$, то відображення $\phi: A \rightarrow A$, що визначається за правилом $\phi(a_i) = a_{\sigma(i)}$, $1 \leq i \leq n$, буде очевидно підстановкою множини A . Далі, якщо $\pi \neq \phi$, то існує індекс r , для якого $\pi(a_r) \neq \phi(a_r)$. Це означає, що $\pi_0(r) \neq \phi_0(r)$, тому $\pi_0 \neq \phi_0$.

Таким чином, за кожною підстановкою π множини A ми можемо побудувати підстановку π_0 множини $\{1, 2, \dots, n\}$ і відповідність $\pi \rightarrow \pi_0$ буде бієкцією. Тому далі, замість того, щоб розглядати підстановки довільних скінченних множин, розглядатимемо підста-

новки множини $\{1, 2, \dots, n\}$. Замість позначення $S(\{1, 2, \dots, n\})$ використовуватимемо більш коротке стандартне позначення S_n . Надалі будемо називати S_n *симетричною групою степеня n* . Якщо $\pi \in S_n$, то будемо говорити ще, що π — підстановка степеня n . Кожну підстановку π степеня n зручно записувати у вигляді матриці з двох рядків. У першому рядку виписуються елементи $1, 2, \dots, n$, у другому — під кожним з цих елементів виписується його образ відносно π :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

Таку форму запису будемо називати табличною. Слід відзначити також, що не обов'язково виписувати елементи першого рядка у порядку зростання, у деяких випадках буде зручним виписати ці елементи в іншому порядку; важлива тільки та обставина, що під кожним елементом першого рядка мусить стояти його образ відносно підстановки π . Наприклад,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 1 & 7 & 8 & 3 & 5 & 2 & 6 \end{pmatrix} \text{ та } \begin{pmatrix} 2 & 5 & 7 & 1 & 9 & 3 & 6 & 4 & 8 \\ 9 & 8 & 5 & 4 & 6 & 1 & 3 & 7 & 2 \end{pmatrix}$$

записи однієї і тієї ж підстановки (на перших порах, коли читач почне практично працювати з підстановками, йому варто в кожному стовпчику писати вертикальну стрілку вниз аж до того часу, поки він особисто не переконається, що їх писати — це зайва робота).

При цьому добутку підстановок π та σ відповідає таблиця

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(\sigma(1)) & \pi(\sigma(2)) & \dots & \pi(\sigma(n)) \end{pmatrix}.$$

Це підказує нам наступне правило множення підстановок. У першому рядку таблиці, що відповідає підстановці σ , беремо довільний індекс i ; те число, що стоїть під ним, відшукаємо у верхньому рядку таблиці, що відповідає підстановці π . Під ним i буде стояти образ i відносно добутку $\pi \circ \sigma$. Схематично це зручно зобразити у такому вигляді:

$$\begin{array}{cccc} 1 & 2 & \dots & n \\ \downarrow & \downarrow & & \downarrow \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ \downarrow & \downarrow & & \downarrow \\ \pi(\sigma(1)) & \pi(\sigma(2)) & \dots & \pi(\sigma(n)). \end{array}$$

4.1. Лема. Нехай A — множина, $f \in S(A)$. Наступні відображення будуть підстановками множини $S(A)$:

$$\vartheta_1 : g \longrightarrow g^{-1} \text{ для кожного } g \in S(A);$$

$$\vartheta_2 : g \longrightarrow f \circ g \text{ для кожного } g \in S(A);$$

$$\vartheta_3 : g \longrightarrow g \circ f \text{ для кожного } g \in S(A).$$

Д о в е д е н н я. Припустимо, що для деяких різних підстановок $g_1, g_2 \in S(A)$ має місце $\vartheta_1(g_1) = \vartheta_1(g_2)$, тобто $g_1^{-1} = g_2^{-1}$. З означення оберненого відображення та того факту, що воно є єдиним, випливає рівність $(g^{-1})^{-1} = g$. З цього отримаємо рівність $g_1 = g_2$, яка суперечить вибору підстановок g_1, g_2 . Ця суперечність доводить ін'єктивність відображення ϑ_1 . Оскільки для кожної підстановки існує обернена, то відображення ϑ_1 сюр'єктивне. Отже, ϑ_1 є бієктивним.

Покажемо тепер, що відображення ϑ_2 є ін'єктивним. Якщо припустити існування таких різних підстановок $g_1, g_2 \in S(A)$, що $\vartheta_2(g_1) = \vartheta_2(g_2)$, то маємо $f \odot g_1 = f \odot g_2$. Тепер множимо обидві частини останньої рівності на f^{-1} та отримуємо

$$\begin{aligned} g_1 &= \varepsilon_A \odot g_1 = (f^{-1} \odot f) \odot g_1 = f^{-1} \odot (f \odot g_1) = f^{-1} \odot (f \odot g_2) = \\ &= (f^{-1} \odot f) \odot g_2 = \varepsilon_A \odot g_2 = g_2. \end{aligned}$$

Отримана суперечність доводить ін'єктивність відображення ϑ_2 . З рівності

$$h = \varepsilon_A \odot h = (f \odot f^{-1}) \odot h = f \odot (f^{-1} \odot h) = \vartheta_2(f^{-1} \odot h)$$

випливає сюр'єктивність ϑ_2 . Отже, і ϑ_2 є бієктивним.

Аналогічно доводиться бієктивність відображення ϑ_3 .

Підстановку τ будемо називати *транспозицією* (більш точно, *транспозицією символів k, t*), якщо $\tau(k) = t$, $\tau(t) = k$ та $\tau(i) = i$ для всіх інших індексів i .

Транспозицію символів k, t будемо позначати символом $\tau_{k,t}$ або $(k\ t)$. Без використання символів можна сказати, що транспозиція — це така підстановка, яка, як відображення, залишає незмінними всі числа, за виключенням двох, а останні переходять одне в інше.

Розглянемо $\tau_{i,j}^2 = \tau_{i,j} \odot \tau_{i,j}$. Маємо

$$\tau_{i,j} \odot \tau_{i,j}(i) = \tau_{i,j}(\tau_{i,j}(i)) = \tau_{i,j}(j) = i,$$

$$\tau_{i,j} \odot \tau_{i,j}(j) = \tau_{i,j}(\tau_{i,j}(j)) = \tau_{i,j}(i) = j,$$

та якщо $k \notin \{i, j\}$, то

$$\tau_{i,j} \odot \tau_{i,j}(k) = \tau_{i,j}(\tau_{i,j}(k)) = \tau_{i,j}(k) = k,$$

так що $\tau_{i,j}^2 = \varepsilon$ — тотожна підстановка.

4.2. Теорема. $|S_n| = n! = 1 \cdot 2 \cdot \dots \cdot n$.

Д о в е д е н н я. Будемо використовувати індукцію за числом n . Нехай $n = 2$. Множина S_2 складається з підстановок

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

так що $|S_2| = 2 = 2!$.

Нехай тепер $n > 2$ і припустимо, що теорема доведена для множин S_k , де $k < n$. Розглянемо множину

$$P_i = \{\pi \in S_n \mid \pi(n) = i\}.$$

Легко бачити, що $P_i \cap P_j = \emptyset$ і якщо $i \neq j$, то

$$S_n = \bigcup_{1 \leq i \leq n} P_i = P_1 \cup P_2 \cup \dots \cup P_n.$$

З цього випливає рівність

$$|S_n| = |P_1| + |P_2| + \dots + |P_n|.$$

Якщо $\pi \in P_i$, то $\tau_{i,n} \odot \pi \in P_n$. Дійсно,

$$\tau_{i,n} \odot \pi(n) = \tau_{i,n}(\pi(n)) = \tau_{i,n}(i) = n.$$

Навпаки, нехай $\sigma \in P_n$. Тоді $\tau_{i,n} \odot \sigma(n) = \tau_{i,n}(\sigma(n)) = \tau_{i,n}(n) = i$, тому $\tau_{i,n} \odot \sigma \in P_i$. Лема 4.1 показує, що відображення $\Phi: S_n \rightarrow S_n$, визначене за правилом $\Phi(\pi) = \tau_{i,n} \odot \pi$, $\pi \in S_n$, буде бієкцією. З доведеного вище випливає, що $\Phi(P_i) = P_n$. В цьому випадку будемо мати $|P_i| = |P_n|$ для кожного i , $1 \leq i \leq n$. Це означає, що $|S_n| = n|P_n|$.

Розглянемо тепер відображення $\Xi: P_n \rightarrow S_n$, яке ставить у відповідність кожній підстановці $\pi \in P_n$ підстановку π' степеня $n-1$, що визначається за наступним правилом:

$$\pi'(1) = \pi(1), \pi'(2) = \pi(2), \dots, \pi'(n-1) = \pi(n-1).$$

Покажемо, що Ξ — бієкція. Нехай π, σ — дві різні підстановки з множини P_n . Тоді існує такий індекс t , що $\pi(t) \neq \sigma(t)$. Оскільки $\pi(n) = n = \sigma(n)$, то $t \neq n$. Отже, $\pi'(t) = \pi(t) \neq \sigma(t) = \sigma'(t)$, а тому $\Xi(\pi) \neq \Xi(\sigma)$. Нехай тепер $\rho \in S_{n-1}$. Розглянемо підстановку σ степеня n , що визначається за правилом

$$\sigma(1) = \rho(1), \sigma(2) = \rho(2), \dots, \sigma(n-1) = \rho(n-1), \sigma(n) = n.$$

Легко бачити, що $\sigma \in P_n$ та $\Xi(\sigma) = \rho$, так що відображення Ξ — сюр'єктивне, а значить, і бієктивне. Звідси випливає, що $|P_n| = |S_{n-1}| = (n-1)!$, а тому $|S_n| = n \cdot |P_n| = n(n-1)! = n!$.

Парність підстановки. Розглянемо будь-які різниці $(t-k)$, де $1 \leq k < t \leq n$, та позначимо через ∇_n їх добуток, тобто

$$\nabla_n = \prod_{1 \leq k < t \leq n} (t-k).$$

Якщо π — підстановка степеня n , то покладемо

$$\pi(\nabla_n) = \prod_{1 \leq k < t \leq n} (\pi(t) - \pi(k)).$$

Для кожної пари чисел t, k , де $1 \leq k < t \leq n$, знайдуться такі числа m, j , що $t = \pi(m)$, $k = \pi(j)$, тобто $t-k = \pi(m) - \pi(j)$. Тут можливі два випадки:

(1) $m > j$; у цьому випадку вираз $(t-k)$ міститься серед множників розкладу $\pi(\nabla_n)$;

(2) $m < j$; у цьому випадку $\pi(m) = t > k = \pi(j)$.

Скажемо, що числа m, j складають інверсію відносно підстановки π , якщо $m < j$, але $\pi(m) > \pi(j)$.

У другому випадку розклад $\pi(\nabla_n)$ містить вираз $(k - t) = -(t - k)$. Таким чином, кожний вираз у дужках з розкладу ∇_n міститься зі знаком «+» або «-» серед множників розкладу $\pi(\nabla_n)$. Оскільки загальні кількості множників у дужках у розкладах ∇_n та $\pi(\nabla_n)$ однакові, то

$$\pi(\nabla_n) = (-1)^{i(\pi)} \nabla_n,$$

де $i(\pi)$ — кількість пар індексів, що утворюють інверсію відносно підстановки π . Покладемо $\text{sign } \pi = (-1)^{i(\pi)}$ та будемо називати це число сигнатурою підстановки π . Так що $\pi(\nabla_n) = \text{sign } \pi \nabla_n$.

Якщо $\pi, \sigma \in S_n$, $\rho = \pi \odot \sigma$, то будемо мати

$$\rho(\nabla_n) = \prod_{1 \leq k < t \leq n} (\pi(\sigma(t)) - \pi(\sigma(k))).$$

За допомогою попередніх аргументів можна довести рівність

$$(\pi \odot \sigma)(\nabla_n) = \text{sign } \pi \text{ sign } \sigma \nabla_n,$$

тобто

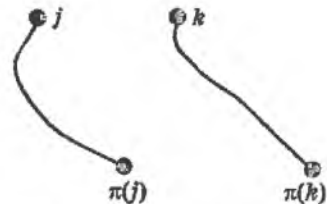
$$\text{sign } (\pi \odot \sigma) = \text{sign } \pi \text{ sign } \sigma.$$

Підстановка π називається парною, якщо $\text{sign } \pi = 1$, тобто кількість пар, що утворюють інверсію відносно π , є парною; та непарною, якщо $\text{sign } \pi = -1$, тобто кількість пар, що утворюють інверсію відносно π , є непарною.

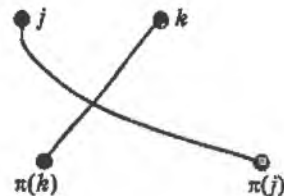
З рівності $\text{sign } (\pi \odot \sigma) = \text{sign } \pi \text{ sign } \sigma$ випливає, що добуток двох парних підстановок є парною підстановкою, добуток двох непарних підстановок є парною підстановкою та добуток парної та непарної підстановок є непарною підстановкою.

Є дуже зручний графічний метод знаходження парності підстановки π . Він базується на наступному спостереженні. Нехай $1 \leq j < k \leq n$. Випишемо всі числа множини $\{1, 2, \dots, n\}$ у два рядки. Кожне число з верхнього рядка з'єднаємо лінією з його образом відносно π , що стоїть у нижньому рядку.

Якщо числа j, k не складають інверсію відносно підстановки π , то це відображається такою частиною малюнка:



Якщо ж числа j, k складають інверсію відносно підстановки π , то це відображається такою частиною малюнка:

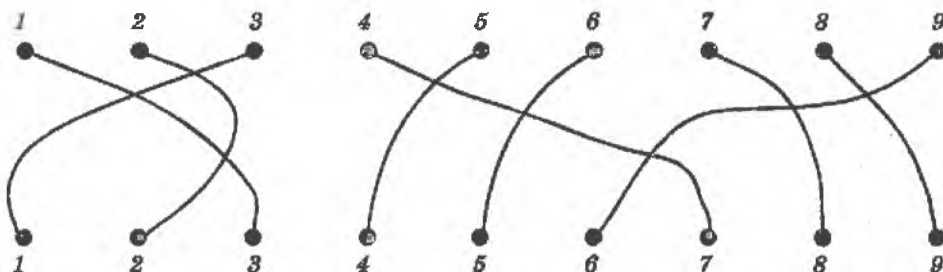


Інакше кажучи, парі чисел, що утворюють інверсію відносно підстановки π , відповідає перетин ліній. Таким чином, підрахувавши кількість перетинів ліній, ми тим самим отримаємо кількість пар індексів, що утворюють інверсії відносно підстановки π .

Проілюструємо це наступним прикладом. Розглянемо наступну підстановку π

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 7 & 4 & 5 & 8 & 9 & 6 \end{pmatrix}.$$

Цій підстановці відповідає наступний малюнок:



Ми бачимо, що 8 пар чисел утворюють інверсії відносно цієї підстановки. І на малюнку маємо 8 точок перетину.

Позначимо через A_n сукупність всіх парних підстановок степеня n .

Знайдемо тепер кількість пар, що утворюють інверсію відносно транспозиції $\tau_{k,t}$, де $k < t$. Розглянемо довільну пару чисел i, j , де $1 \leq i < j \leq n$, та з'ясуємо, коли вона буде утворювати інверсію відносно $\tau_{k,t}$. Якщо $\{i, j\} \cap \{k, t\} = \emptyset$, то $\tau_{k,t}(i) = i$, $\tau_{k,t}(j) = j$, тобто пара i, j не утворює інверсії. Якщо $j = k$, то $\tau_{k,t}(i) = i$, $\tau_{k,t}(j) = t$ і $t > k > i$, тому і в цьому випадку пара i, j інверсію не утворює. Інверсія виникає у випадках, коли $i = k, j = t$; $i = k, j < t$; $t > k, j = t$. Кількість таких пар чисел дорівнює $2(t - k - 1) + 1$. Зскрема, загальна кількість пар чисел, що утворюють інверсію відносно транспозиції, є непарною, тобто транспозиція є непарною підстановкою.

Нехай $1 \leq i < j \leq n$ та розглянемо відображення $\vartheta : S_n \rightarrow S_n$, яке визначається за правилом $\vartheta(\sigma) = \tau_{i,j} \circ \sigma$, $\sigma \in S_n$. З леми 4.1 випливає, що ϑ — бієкція. Нехай π — парна підстановка, тоді, як уже відзначалось вище, $\vartheta(\pi)$ — непарна підстановка. І навпаки, якщо π — непарна підстановка, то $\vartheta(\pi)$ буде парною підстановкою. Це означає, що $\vartheta(A_n) \subseteq S_n \setminus A_n$ та $\vartheta(S_n \setminus A_n) \subseteq A_n$. Більше того, неважко довести, що $\vartheta(A_n) = S_n \setminus A_n$ та $\vartheta(S_n \setminus A_n) = A_n$. Оскільки ϑ — бієкція, то $|A_n| = |\vartheta(A_n)| = |S_n \setminus A_n|$, $|S_n \setminus A_n| = |\vartheta(S_n \setminus A_n)| = |A_n|$, тобто $|A_n| = |S_n \setminus A_n|$, і зокрема, $|A_n| = (n!)/2$.

На важливість ролі транспозицій указує наступна теорема.

4.3. Теорема. *Кожна підстановка є добутком транспозицій.*

Доведення. Якщо $\pi \in S_n$, то покладемо

$$\text{Inv}(\pi) = \{k \mid 1 \leq k \leq n \text{ та } \pi(k) = k\}.$$

Теорему будемо доводити методом індукції за числом $r(\pi) = n - |\text{Inv}(\pi)|$. Якщо $r(\pi) = 0$, то $n = |\text{Inv}(\pi)|$. Але ж це означає, що $\pi = \varepsilon$ — тотожна підстановка степеня n . У цьому випадку $\varepsilon = \tau_{1,1} \odot \tau_{1,1}$ для будь-якої транспозиції $\tau_{1,1}$.

Нехай тепер $r(\pi) > 0$ та припустимо, що теорему вже доведено для всіх підстановок σ , які мають властивість $r(\sigma) < r(\pi)$.

Оскільки $r(\pi) > 0$, то $\text{Inv}(\pi) \neq \{1, 2, \dots, n\}$. Це означає, що існує число k , для якого $\pi(k) = t \neq k$. Оскільки π — підстановка, то $\pi(t) \neq t$, тобто $t \notin \text{Inv}(\pi)$. Розглянемо тепер добуток $\pi_1 = \tau_{k,t} \odot \pi$. Маємо

$$\pi_1(k) = \tau_{k,t} \odot \pi(k) = \tau_{k,t}(\pi(k)) = \tau_{k,t}(t) = k,$$

так що $k \in \text{Inv}(\pi_1)$. Якщо $m \in \text{Inv}(\pi)$, то, як уже відзначалось вище, $m \neq k$, $m \neq t$ і

$$\pi_1(m) = \tau_{k,t} \odot \pi(m) = \tau_{k,t}(\pi(m)) = \tau_{k,t}(m) = m,$$

тобто $m \in \text{Inv}(\pi_1)$. Таким чином, $\text{Inv}(\pi) \subseteq \text{Inv}(\pi_1)$, та $\text{Inv}(\pi) \neq \text{Inv}(\pi_1)$, а тому $r(\pi_1) < r(\pi)$. За індуктивним припущенням існує розклад

$$\pi_1 = v_1 \odot v_2 \odot \dots \odot v_s,$$

де v_i , $1 \leq i \leq s$ — деякі транспозиції. Інакше кажучи,

$$\tau_{k,t} \odot \pi = v_1 \odot v_2 \odot \dots \odot v_s.$$

Помноживши тепер обидві частини цієї рівності зліва на транспозицію $\tau_{k,t}$ і, врахувавши ту обставину, що $\varepsilon = \tau_{k,t} \odot \tau_{k,t}$, отримуємо рівність

$$\pi = \tau_{k,t} \odot v_1 \odot v_2 \odot \dots \odot v_s.$$

Треба відзначити, що розклад підстановки у добуток транспозицій не є єдиним. Наприклад, для підстановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 3 & 6 & 7 & 5 \end{pmatrix}$$

маємо принаймні два таких розклади

$$\pi = \tau_{5,7} \odot \tau_{5,6} \odot \tau_{3,4} \odot \tau_{1,3} \quad \text{та} \quad \pi = \tau_{1,4} \odot \tau_{3,4} \odot \tau_{5,6} \odot \tau_{6,7}.$$

Нехай $\pi \in S_n$. Множину $\text{Supp}(\pi) = \{1, 2, \dots, n\} \setminus \text{Inv}(\pi)$ будемо називати носієм підстановки π . Зразу відзначимо, що $\text{Supp}(\pi) = \text{Supp}(\pi^{-1})$. Точніше покажемо, що $\text{Inv}(\pi) = \text{Inv}(\pi^{-1})$, звідси буде випливати потрібна нам рівність. Нехай $j \in \text{Inv}(\pi)$, тоді $\pi(j) = j$. Діючи на обидві частини цієї рівності підстановкою π^{-1} , отримаємо $j = \pi^{-1}(j)$, тобто $j \in \text{Inv}(\pi^{-1})$. За допомогою аналогічних міркувань можна довести включення $\text{Inv}(\pi^{-1}) \subseteq \text{Inv}(\pi)$, і отже, $\text{Inv}(\pi) = \text{Inv}(\pi^{-1})$.

Нехай $1 \leq r \leq n$, то підстановка π називається циклом довжини r , якщо $\text{Supp}(\pi) = \{j_1, j_2, \dots, j_r\}$ та

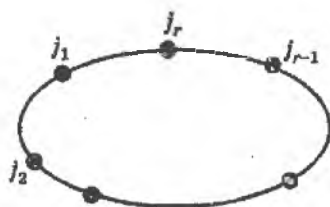
$$\pi(j_1) = j_2, \pi(j_2) = j_3, \dots, \pi(j_{r-1}) = j_r, \pi(j_r) = j_1.$$

Інакше кажучи, індекси $j_1, j_2, \dots, j_r$ підстановки π переставляє циклічно, а всі інші залишає нерухомими. Тому для циклу використовується наступна форма запису

$$\pi = (j_1 j_2 \dots j_r) (j_{r+1}) \dots (j_n),$$

або коротше

$$\pi = (j_1 j_2 \dots j_r).$$



Зокрема, транспозиція — це цикл довжини 2. Також слід відзначити, що у запису циклу порядок розташування індексів не фіксується, важливо тільки, щоб за кожним індексом йшов його образ, наприклад,

$$(j_1 j_2 \dots j_r) = (j_1 j_2 \dots j_r j_1) = (j_3 \dots j_r j_1 j_2).$$

Підстановки $\pi, \sigma \in S_n$ називаються розділеними або незалежними, якщо $\text{Supp}(\pi) \cap \text{Supp}(\sigma) = \emptyset$. Зазначимо зразу важливу властивість таких підстановок.

4.4. Пропозиція. Нехай $\pi, \sigma \in S_n$. Якщо підстановки π, σ є розділеними, то $\pi \odot \sigma = \sigma \odot \pi$.

Доведення. Нехай $j \in \{1, 2, \dots, n\}$, покажемо, що $\pi(\sigma(j)) = \sigma(\pi(j))$. Якщо $j \notin \text{Supp}(\pi) \cup \text{Supp}(\sigma)$, то $\pi(\sigma(j)) = j = \sigma(\pi(j))$. Нехай тепер $j \in \text{Supp}(\pi)$, тоді $j \notin \text{Supp}(\sigma)$, тобто $\sigma(j) = j$ і тому $\pi(\sigma(j)) = \pi(j)$.

Припустимо тепер, що $\pi(j) \in \text{Supp}(\sigma)$, тоді $\pi(j) \notin \text{Supp}(\pi)$ і $\pi(\pi(j)) = \pi(j)$. Діючи на обидві частини останньої рівності підстановкою π^{-1} , отримаємо $\pi(j) = j$, а це означає, що $j \notin \text{Supp}(\pi)$, а це суперечить вибору індексу j . Отримана суперечність показує, що $\pi(j) \notin \text{Supp}(\sigma)$, тобто $\sigma(\pi(j)) = \pi(j)$. Таким чином, $\pi(\sigma(j)) = \pi(j) = (\sigma(\pi(j)))$.

Аналогічно розглядається і випадок $j \in \text{Supp}(\sigma)$.

4.5. Теорема. Кожна неединична підстановка є добутком попарно розділених циклів.

Доведення. Нехай $\varepsilon \neq \pi \in S_n$. Теорему будемо доводити індукцією за числом $r(\pi) = |\text{Supp}(\pi)|$. Якщо $r(\pi) = 2$, то очевидно, π буде транспозицією, зокрема, вона сама буде циклом довжини 2. Нехай тепер $r(\pi) > 2$ та припустимо, що теорему вже доведено для всіх підстановок σ , які мають властивість $r(\sigma) < r(\pi)$. Знайдемо такий індекс j , що $\pi(j) \neq j$. Розглянемо числа

$$j, \pi(j), \pi^2(j) = \pi(\pi(j)), \dots, \pi^n(j_1) = \pi(\pi^{n-1}(j)), \dots$$

Всі вони належать до скінченної підмножини $\{1, 2, \dots, n\}$. Тому знайдуться такі числа t, s , що $t > s$ та $\pi^t(j) = \pi^s(j)$. Діючи на обидві частини цієї рівності підстановкою π^{-1} достатньою кількістю разів, отримаємо зрештою $\pi^{t-s}(j) = j$. Виберемо тепер найменше натуральне число m , що має властивість

$\pi^m(j) = j$. За допомогою наведених вище аргументів тепер можна упевнитись у тому, що всі числа $j, \pi(j), \pi^2(j), \dots, \pi^{m-1}(j)$ є різними.

Нехай

$$\sigma = (j \ \pi(j) \ \pi^2(j) \ \dots \ \pi^{m-1}(j)), \ \rho = \sigma^{-1} \odot \pi,$$

тоді $\pi = \sigma \odot \rho$. Якщо $k \in \{j, \pi(j), \pi^2(j), \dots, \pi^{m-1}(j)\}$, то легко бачити, що $\rho(k) = k$. Це означає, що $\text{Supp}(\sigma) \cap \text{Supp}(\rho) = \emptyset$. Пропозиція 4.4 показує, що $\sigma \odot \rho = \rho \odot \sigma$.

Нехай тепер $k \in \text{Inv}(\pi)$. Оскільки $\text{Supp}(\sigma) \subseteq \text{Supp}(\pi)$, то $\text{Inv}(\pi) \subseteq \text{Inv}(\sigma)$, і отже $k \in \text{Inv}(\sigma)$. Вище вже відзначалось, що $\text{Inv}(\sigma) = \text{Inv}(\sigma^{-1})$, а це тягне за собою той факт, що $k \in \text{Inv}(\rho)$.

Таким чином, $\text{Inv}(\pi) \subseteq \text{Inv}(\rho)$, а оскільки $j \in \text{Inv}(\rho) \setminus \text{Inv}(\pi)$, $\text{Inv}(\rho) \neq \text{Inv}(\pi)$. Це означає, що $|\text{Supp}(\rho)| < |\text{Supp}(\pi)|$. За індуктивним припущенням ρ буде добутком розділених циклів. Оскільки $\text{Supp}(\sigma) \cap \text{Supp}(\rho) = \emptyset$, то і підстановка π є добутком розділених циклів.

Частина друга

2

5. МАТРИЦІ, ОПЕРАЦІЇ НАД МАТРИЦЯМИ

Матрицею називатимемо прямокутну таблицю, елементи якої — це деякі математичні об'єкти. З яких саме об'єктів складається матриця вказується додатково. Це можуть бути деякі сукупності чисел або ж елементів іншої природи, такі як багаточлени, функції, а пізніше і елементи деякого абстрактного поля, чи, навіть, кільця. Елементи матриці будемо позначати однією буквою з двома індексами, які вказують на місце елемента в матриці; перший індекс указує номер рядка, в якому знаходиться даний елемент, а другий індекс — номер місця елемента у рядку або, що те саме, номер стовпця, в якому знаходиться даний елемент. Таким чином, матриця розміру $k \times n$ записується у наступній формі

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n-1} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n-1} & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & a_{k3} & \dots & a_{kn-1} & a_{kn} \end{pmatrix} \quad \text{або} \quad \left\| \begin{array}{cccccc} a_{11} & a_{12} & a_{13} & \dots & a_{1n-1} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n-1} & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & a_{k3} & \dots & a_{kn-1} & a_{kn} \end{array} \right\|.$$

Використовуватимемо ще наступну скорочену форму запису матриці:

$$\| a_{ij} \|_{1 \leq i \leq k, 1 \leq j \leq n}.$$

Сукупність всіх матриць розміру $k \times n$, коефіцієнти яких належать до множини S , будемо позначати через $M_{k \times n}(S)$.

Матриця, утворена з елементів, які стоять на перетині декількох вибраних рядків та декількох вибраних стовпців матриці A , називається *підматрицею* або *субматрицею* матриці A . Якщо в матриці A вибрані рядки з номерами $i(1), i(2), \dots, i(k)$ та стовпці з номерами $j(1), j(2), \dots, j(m)$, то відповідною підматрицею буде

$$\begin{pmatrix} a_{i(1)j(1)} & a_{i(1)j(2)} & \cdots & a_{i(1)j(m)} \\ a_{i(2)j(1)} & a_{i(2)j(2)} & \cdots & a_{i(2)j(m)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i(k)j(1)} & a_{i(k)j(2)} & \cdots & a_{i(k)j(m)} \end{pmatrix}.$$

Зокрема, рядки та стовпці матриці можна розглядати як її підматриці.

Дві матриці $A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, $B = \|b_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$ з множини $M_{k \times n}(S)$ називаються *рівними*, якщо $a_{ij} = b_{ij}$ для кожної пари індексів i, j , $1 \leq i \leq k$, $1 \leq j \leq n$. Інакше кажучи, рівні матриці повинні мати однакові розміри, та їх елементи, що стоять на однакових місцях, повинні збігатися.

Якщо кількість рядків матриці дорівнює кількості її стовпців, то така матриця називається *квадратною*, а кількість її рядків (або стовпців) називають *порядком* цієї матриці. Зокрема, квадратна матриця порядку 1 — це просто один елемент. Сукупність всіх квадратних матриць порядку n , коефіцієнти яких належать до множини S , будемо позначати через $M_n(S)$.

Числова квадратна матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n}$ називається (*верхньо*) *трикутною*, якщо $a_{ij} = 0$ при $i > j$.

Трикутна матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n}$ називається *унітрикутною*, якщо $a_{ii} = 1$ для кожного i , $1 \leq i \leq n$.

Трикутна матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n}$ називається *нультрикутною*, якщо $a_{ii} = 0$ для кожного i , $1 \leq i \leq n$.

Числова квадратна матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n}$ називається *діагональною*, якщо $a_{ij} = 0$ для будь-яких $i \neq j$.

Розглянемо тепер деякі природні операції над матрицями з числовими елементами.

Нехай $A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, $B = \|b_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$ — дві матриці з множини $M_{k \times n}(R)$.

Сумою $A + B$ цих матриць будемо називати матрицю $\|c_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, елементи якої визначаються за правилом $c_{ij} = a_{ij} + b_{ij}$ для кожної пари індексів i, j , $1 \leq i \leq k$, $1 \leq j \leq n$.

Інакше кажучи, щоб додати дві матриці однакового розміру, потрібно скласти їх елементи, що стоять на однакових місцях. Зокрема, додавання матриць зводиться до додавання їх відповідних елементів, а тому воно успадковує всі основні властивості операції додавання чисел.

Додавання матриць комутативне:

$A + B = B + A$ для кожної пари матриць $A, B \in M_{k \times n}(R)$.

Додавання матриць асоціативне:

$(A + B) + C = A + (B + C)$ для кожної трійки матриць $A, B, C \in M_{k \times n}(R)$.

Відносно операції додавання матриць існує нульовий елемент, тобто така матриця O , що $A + O = A$ для кожної матриці $A \in M_{k \times n}(R)$.

Неважко помітити, що матриця з цією властивістю, єдина. Кожен елемент матриці O дорівнює 0 .

Для кожної матриці A існує протилежна матриця $-A$, тобто матриця, що має властивість $A + (-A) = O$. Для кожної матриці A протилежна матриця єдина і якщо $A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, то

$$-A = \|-a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}.$$

На множині $M_{k \times n}(R)$ можна ввести також операцію віднімання за правилом:

$$A - B = A + (-B) \text{ для кожної пари матриць } A, B \in M_{k \times n}(R).$$

На відміну від операції додавання операція множення матриці на матрицю визначається складніше. Спочатку задамо її для квадратних матриць, а потім зробимо деякі зауваження відносно множення прямокутних матриць.

Отже, нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$ — дві матриці з множини $M_n(R)$.

Добутком AB цих матриць будемо називати матрицю $\|c_{ij}\|_{1 \leq i, j \leq n}$, елементи якої визначаються за правилом

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{1 \leq k \leq n} a_{ik}b_{kj}$$

для кожної пари індексів i, j , $1 \leq i, j \leq n$.

Слід відзначити, що множення матриць не комутативне. В цьому можна пересвідчитись, розглянувши такий приклад:

$$\begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 14 & 10 \\ 18 & 11 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 19 & 18 \end{pmatrix}.$$

Матриці A, B , для яких $AB = BA$, називаються *переставними* (по-іншому кажуть, що ці матриці комутують).

Але іншою важливою властивістю — асоціативністю — множення матриць володіє.

5.1. Теорема. Для довільних матриць $A, B, C \in M_n(R)$ виконуються наступні рівності:

$$(1) (AB)C = A(BC).$$

$$(2) (A + B)C = AC + BC.$$

$$(3) A(B + C) = AB + AC.$$

(4) Існує така матриця $E \in M_n(R)$, що для кожної матриці $A \in M_n(R)$ виконується рівність $AE = EA = A$. Ця матриця E визначається єдиним чином.

Доведення. (1) Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, $C = \|c_{ij}\|_{1 \leq i, j \leq n}$. Покладемо

$$AB = \|d_{ij}\|_{1 \leq i, j \leq n}, (AB)C = \|u_{ij}\|_{1 \leq i, j \leq n},$$

$$BC = \|v_{ij}\|_{1 \leq i, j \leq n}, A(BC) = \|w_{ij}\|_{1 \leq i, j \leq n}.$$

Потрібно довести, що $u_{ij} = w_{ij}$ для довільних індексів i, j , $1 \leq i, j \leq n$. Маємо

$$\begin{aligned} u_{ij} &= \sum_{1 \leq k \leq n} d_{ik} c_{kj} = \sum_{1 \leq k \leq n} \left(\sum_{1 \leq m \leq n} a_{im} b_{mk} \right) c_{kj} = \sum_{1 \leq k \leq n} \sum_{1 \leq m \leq n} (a_{im} b_{mk}) c_{kj}, \\ w_{ij} &= \sum_{1 \leq m \leq n} a_{im} v_{mj} = \sum_{1 \leq m \leq n} a_{im} \left(\sum_{1 \leq k \leq n} b_{mk} c_{kj} \right) = \\ &= \sum_{1 \leq m \leq n} \sum_{1 \leq k \leq n} a_{im} (b_{mk} c_{kj}) = \sum_{1 \leq m \leq n} \sum_{1 \leq k \leq n} a_{im} (b_{mk} c_{kj}). \end{aligned}$$

(2) Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, $C = \|c_{ij}\|_{1 \leq i, j \leq n}$.
Покладемо

$$AC = \|d_{ij}\|_{1 \leq i, j \leq n}, \quad BC = \|u_{ij}\|_{1 \leq i, j \leq n}, \quad (A+B)C = \|v_{ij}\|_{1 \leq i, j \leq n}.$$

Потрібно довести, що $v_{ij} = d_{ij} + u_{ij}$ для довільних індексів i, j , $1 \leq i, j \leq n$. Маємо

$$v_{ij} = \sum_{1 \leq k \leq n} (a_{ik} + b_{ik}) c_{kj} = \sum_{1 \leq k \leq n} a_{ik} c_{kj} + \sum_{1 \leq k \leq n} b_{ik} c_{kj} = d_{ij} + u_{ij}.$$

Твердження (3) доводиться аналогічно.

(4) Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$. Визначимо символи δ_{ij} (символи Кронекера) за правилом:

$$\delta_{ij} = \begin{cases} 0, & \text{якщо } i \neq j, \\ 1, & \text{якщо } i = j. \end{cases}$$

Покладемо $E = \|\delta_{ij}\|_{1 \leq i, j \leq n}$. Інакше кажучи,

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Нехай $AE = \|x_{ij}\|_{1 \leq i, j \leq n}$, $EA = \|z_{ij}\|_{1 \leq i, j \leq n}$. Маємо

$$x_{ij} = \sum_{1 \leq k \leq n} a_{ik} \delta_{kj} = a_{ij} \delta_{jj} = a_{ij}.$$

$$z_{ij} = \sum_{1 \leq k \leq n} \delta_{ik} a_{kj} = \delta_{ii} a_{ij} = a_{ij}.$$

Це означає, що $AE = EA = A$.

Припустимо, що існує така інша матриця U , що $AU = UA = A$ для кожної матриці $A \in M_n(R)$. Тоді $EU = U$ та $EU = E$, так що $E = U$.

Матрицю E називають *одиничною матрицею*.

Нехай $A \in M_n(R)$. Матриця U називається оберненою до A , якщо $AU = UA = E$.

Слід відзначити, що не кожна матриця має обернену. Як приклад розглянемо матрицю

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

Помножимо її на довільну матрицю:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} \\ 0 & 0 \end{pmatrix}.$$

Таким чином, цей добуток не може бути одиничною матрицею, тобто вказана матриця не має оберненої.

Але якщо матриця A має обернену, то ця обернена матриця буде єдиною. Дійсно, нехай U, V — дві матриці, що мають властивості $AU = UA = E = VA = AV$. Розглянемо матрицю $V(AU)$. Маємо

$$V(AU) = VE = V \quad \text{та} \quad V(AU) = (VA)U = EU = U.$$

Отже $V = U$. Тому далі матрицю, обернену до A , позначатимемо через A^{-1} .

Критерії існування оберненої матриці пов'язані з поняттям визначника матриці і тому будуть розглянуті пізніше.

Множення матриць можна розширити і на прямокутні матриці. При цьому наведене вище визначення залишається. Інакше кажучи, добуток двох прямокутних матриць A та B є визначеним тільки у випадку, коли кількість стовпців матриці A дорівнює кількості рядків матриці B , кількість рядків добутку AB дорівнює кількості рядків матриці A , кількість стовпців добутку AB дорівнює кількості стовпців матриці B , причому, якщо $A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, $B = \|b_{ij}\|_{1 \leq i \leq n, 1 \leq j \leq t}$, то добуток AB цих матриць — це матриця $\|c_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq t}$ елементи якої визначаються за правилом

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{1 \leq m \leq n} a_{im}b_{mj}$$

для кожної пари індексів i, j , $1 \leq i, j \leq n$, $1 \leq j \leq t$.

Слід відзначити, що множення прямокутних матриць також буде асоціативним; доведення цього факту аналогічне.

Зауважимо, що матриці мають надзвичайно широкі та надзвичайно важливі застосування. Вони найперше виникають як зручний технічний апарат для скороченого запису різноманітних громіздких виразів, рівнянь, співвідношень, тощо. Наприклад, використавши матриці, систему лінійних рівнянь

$$\begin{cases} a_{11}x_1 & a_{12}x_2 & \dots & a_{1n}x_n = b_1 \\ a_{21}x_1 & a_{22} & \dots & a_{2n}x_n = b_2 \\ \dots & \dots & \dots & \dots \\ a_{k1}x_1 & a_{k2} & \dots & a_{kn}x_n = b_k \end{cases}$$

можна записати у вигляді матричного рівняння

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}.$$

Розглянемо тепер операцію множення матриці на число. Нехай $A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$ — матриця з множини $M_n(R)$, $\alpha \in R$.

Добутком числа α та матриці A називається матриця $\alpha A = \|c_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, коефіцієнти якої визначаються за правилом $c_{ij} = \alpha a_{ij}$ для кожної пари індексів i, j , $1 \leq i \leq k$, $1 \leq j \leq n$.

Інакше кажучи, щоб помножити число на матрицю, необхідно помножити кожен її елемент на це число. Перелічимо відразу властивості цієї операції:

$$\begin{aligned} (\alpha + \beta)A &= \alpha A + \beta A, \\ \alpha(A + B) &= \alpha A + \alpha B, \\ \alpha(\beta A) &= (\alpha\beta)A, \\ 1A &= A, \\ \alpha(AB) &= (\alpha A)B = A(\alpha B). \end{aligned}$$

Слід відзначити також, що операцію множення числа α на матрицю A можна звести до операції множення матриць. Справді, $\alpha A = (\alpha E)A$.

Підсумовуючи сказане, можемо виписати всі властивості операцій, які ми отримали.

$$\begin{aligned} A + B &= B + A, \\ A + (B + C) &= (A + B) + C, \\ A + O &= A, \\ A + (-A) &= O, \\ A(B + C) &= AB + AC, \\ (A + B)C &= AC + BC, \\ A(BC) &= (AB)C, \\ AE = EA &= A, \\ (\alpha + \beta)A &= \alpha A + \beta A, \\ \alpha(A + B) &= \alpha A + \alpha B, \\ \alpha(\beta A) &= (\alpha\beta)A, \\ 1A &= A, \\ \alpha(AB) &= (\alpha A)B = A(\alpha B). \end{aligned}$$

За допомогою вже введених до розгляду арифметичних операцій над матрицями можна задавати нові похідні операції на множині $M_n(R)$. Серед усього розмаїття таких похідних операцій особливо виділяються дві: *операція переходу до комутаторів* і *операція транспонування*. Перша з них зіставляє впорядкованій парі матриць A, B з $M_n(R)$ їх *комутатор* $[A, B] = AB - BA$.

Операція переходу до комутаторів антикомутативна, тобто

$$[A, B] = -[B, A]$$

і $[A, A] = O$. Ця операція не є асоціативною. Справді, легко переконатись, що

$$[[A, B], C] = [AB - BA, C] = ABC - BAC - CAB + CBA,$$

$$[A, [B, C]] = [A, BC - CB] = ABC - ACB - BCA + CBA.$$

Візьмемо тепер

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Тоді отримуємо

$$\begin{aligned} BAC + CAB &= \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} ACB + BCA &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Тепер вже видно, що $[[A, B], C] \neq [A, [B, C]]$.

Але для операції переходу до комутаторів має місце наступна рівність

$$[[A, B], C] + [[C, A], B] + [[B, C], A] = O \text{ (тотожність Якобі).}$$

Справді,

$$\begin{aligned} [[A, B], C] + [[C, A], B] + [[B, C], A] &= [AB - BA, C] + [CA - AC, B] + \\ &+ [BC - CB, A] = ABC - BAC - CAB + CBA + CAB - ACB - BCA + \\ &+ BAC + BCA - CBA - ABC + ACB = O. \end{aligned}$$

На завершення пояснимо, як задається друга із зазначених вище неарифметичних операцій над матрицями. Нехай $A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$ — матриця з множини $M_n(R)$.

Транспонованою матрицею до матриці A називатимемо матрицю $A^t = \|b_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}$, де $b_{ij} = a_{ji}$. Інакше кажучи, рядки матриці A^t — це стовпці матриці A , а стовпці матриці A^t — це рядки матриці A . Про матрицю A^t будемо ще говорити, що вона *отримана з матриці A за допомогою транспонування*. Наступна теорема відзначає часто вживані властивості операції транспонування матриць.

5.2. Теорема. *Операція транспонування має наступні властивості:*

- (1) $(A^t)^t = A$.
- (2) $(A + B)^t = A^t + B^t$.
- (3) $(AB)^t = B^t A^t$.
- (4) $(A^{-1})^t = (A^t)^{-1}$.
- (5) $(\alpha A)^t = \alpha A^t$.

Доведення. Перші два твердження майже очевидні. Доведемо останню рівність.

Нехай

$$A = \|a_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}, \quad B = \|b_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n}.$$

Покладемо

$$AB = \|c_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n},$$

$$A^t = \|u_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq k}, \quad B^t = \|v_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq n},$$

$$B^t A^t = \|w_{ij}\|_{1 \leq i \leq k, 1 \leq j \leq k}.$$

Тоді маємо

$$c_{ij} = \sum_{1 \leq m \leq n} a_{im} b_{mj},$$

$$w_{ij} = \sum_{1 \leq m \leq n} v_{im} u_{mj} = \sum_{1 \leq m \leq n} b_{mi} a_{jm} = \sum_{1 \leq m \leq n} a_{jm} b_{mi} = c_{ji}.$$

Це і означає, що $(AB)^t = B^t A^t$.

З властивості (3) та визначення оберненої матриці випливає (4). Дійсно, $A^{-1}A = AA^{-1} = E$. Застосовуючи (3), отримаємо

$$E = E^t = (A^{-1}A)^t = A^t (A^{-1})^t, \quad E = E^t = (AA^{-1})^t = (A^{-1})^t A^t.$$

Ці рівності і показують, що $(A^{-1})^t = (A^t)^{-1}$. Властивість (5) очевидна.

Матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ називається *симетричною*, якщо $A = A^t$, тобто $a_{ij} = a_{ji}$ для кожної пари індексів i, j , $1 \leq i, j \leq n$.

Матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ називається *кососиметричною*, якщо $a_{ij} = -a_{ji}$ для кожної пари індексів i, j , $1 \leq i, j \leq n$.

Зокрема, для елементів головної діагоналі кососиметричної матриці маємо $a_{ii} = -a_{ii}$, або $a_{ii} = 0$ при кожному i , $1 \leq i \leq n$. Якщо A — кососиметрична матриця і $A^t = \|b_{ij}\|_{1 \leq i, j \leq n}$, то $b_{ij} = a_{ji} = -a_{ij}$, тобто $A^t = -A$. На роль симетричних та кососиметричних матриць вказує наступна теорема.

5.3. Теорема. Кожна квадратна матриця A може бути зображена у вигляді $A = S + K$, де S — симетрична матриця, K — кососиметрична матриця і таке зображення єдине.

Доведення. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$. Покладемо

$$B = \|b_{ij}\|_{1 \leq i, j \leq n}, \text{ де } b_{ij} = a_{ij} + a_{ji},$$

$$C = \|c_{ij}\|_{1 \leq i, j \leq n}, \text{ де } c_{ij} = a_{ij} - a_{ji}, 1 \leq i, j \leq n.$$

$$\text{Маємо } b_{ji} = a_{ji} + a_{ij} = a_{ij} + a_{ji} = b_{ij},$$

$$c_{ji} = a_{ji} - a_{ij} = -(a_{ij} - a_{ji}) = -c_{ij}, 1 \leq i, j \leq n.$$

Інакше кажучи, B — симетрична матриця, C — кососиметрична матриця. Далі,

$$b_{ij} + c_{ij} = a_{ij} + a_{ji} + a_{ij} - a_{ji} = 2a_{ij},$$

отже $B + C = 2A$.

Тепер залишається взяти $S = 1/2 B$, $K = 1/2 C$. Припустимо, що $A = S_1 + K_1$, де S_1 — симетрична матриця, K_1 — кососиметрична матриця.

$$\text{Нехай } S_1 = \|u_{ij}\|_{1 \leq i, j \leq n}, K_1 = \|v_{ij}\|_{1 \leq i, j \leq n}.$$

Маємо

$$b_{ij} = a_{ij} + a_{ji} = u_{ij} + v_{ij} + u_{ji} + v_{ji} = u_{ij} + u_{ji} + v_{ij} - v_{ji} = 2u_{ij},$$

$$c_{ij} = a_{ij} - a_{ji} = u_{ij} + v_{ij} - (u_{ji} + v_{ji}) = u_{ij} - u_{ji} + v_{ij} + v_{ji} = 2v_{ij}.$$

$$\text{Це означає, що } S_1 = 1/2 B = S, K_1 = 1/2 C = K.$$

6. ВИЗНАЧНИКИ, ЇХ ЕЛЕМЕНТАРНІ ВЛАСТИВОСТІ

Нехай $M = \{a_1, a_2, \dots, a_n\}$ — скінченна множина чисел. Замість запису $\sum_{1 \leq i \leq n} a_i = a_1 + a_2 + \dots + a_n$ будемо користуватись також записом $\sum_{a \in M} a$. Цей символ позначає суму всіх елементів множини M . Скінченну множину можна індексувати не тільки за допомогою відрізка натурального ряду, а й за допомогою деяких інших скінченних множин, наприклад, $M = \{a_x | x \in X\}$. Тому для суми всіх елементів множини M можна застосувати також запис $\sum_{x \in X} a_x$. Якщо π — підстановка скінченної множини X , то $\{\pi(x) | x \in X\} = X$, а тому $M = \{a_{\pi(x)} | x \in X\}$. Звідси отримуємо рівність

$$\sum_{x \in X} a_x = \sum_{x \in X} a_{\pi(x)}.$$

З леми 4.1 тепер отримуємо наступне твердження:

6.1. Лема. Нехай M — скінченна множина, індексована за допомогою симетричної групи S_n . $M = \{a_\pi \mid \pi \in S_n\}$. Мають місце рівності:

$$(1) \sum_{\pi \in S_n} a_\pi = \sum_{\pi \in S_n} a_{\pi^{-1}}.$$

$$(2) \sum_{\pi \in S_n} a_\pi = \sum_{\pi \in S_n} a_{\pi \circ \sigma} = \sum_{\pi \in S_n} a_{\sigma \circ \pi},$$

де σ — деяка фіксована підстановка з S_n .

Нагадаємо поняття визначників матриць 2-го та 3-го порядку, щоб за аналогією ввести поняття визначника квадратної матриці будь-якого порядку. Маємо

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}; \quad (1)$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - \\ - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \quad (2)$$

З'ясуємо тепер, що спільного мають ці два поняття. Для першого випадку розглянемо симетричну групу S_2 . Вона складається з двох підстановок ε, α , де

$$\varepsilon = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \text{ причому } \text{sign } \varepsilon = 1, \text{sign } \alpha = -1.$$

Тому

$$a_{11}a_{22} - a_{12}a_{21} = \text{sign } \varepsilon a_{1\varepsilon(1)}a_{2\varepsilon(2)} - \text{sign } \alpha a_{1\alpha(1)}a_{2\alpha(2)}.$$

Розглянемо симетричну групу S_3 . Вона складається з шести підстановок $\varepsilon, \alpha, \beta, \gamma, \pi, \sigma$, де

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \\ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

причому

$$\text{sign } \varepsilon = \text{sign } \alpha = \text{sign } \beta = 1,$$

$$\text{sign } \gamma = \text{sign } \pi = \text{sign } \sigma = -1.$$

Тепер

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{1\varepsilon(1)}a_{2\varepsilon(2)}a_{3\varepsilon(3)} + a_{1\alpha(1)}a_{2\alpha(2)}a_{3\alpha(3)} + a_{1\beta(1)}a_{2\beta(2)}a_{3\beta(3)} - \\ - a_{1\gamma(1)}a_{2\gamma(2)}a_{3\gamma(3)} + a_{1\pi(1)}a_{2\pi(2)}a_{3\pi(3)} + a_{1\sigma(1)}a_{2\sigma(2)}a_{3\sigma(3)}.$$

Виходячи з двох розглянутих випадків, можна тепер по аналогії отримати визначення для визначника квадратної матриці довільного порядку n . Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Для кожної підстановки $\pi \in S_n$ утворюємо добуток

$$\text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

Сума $\det(A)$ всіх цих добутків називається визначником матриці A , тобто

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

Ми будемо також використовувати наступне більш розгорнуте позначення для визначника матриці A :

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}.$$

Відзначимо також, що визначник матриці порядку 1 — це саме число, з якого складається дана матриця.

З визначення видно, що використовувати його для знаходження визначників квадратних матриць навіть не досить високих порядків доволі утруднено (при $n = 4$ сума, що дає розклад визначника, має 24 члени, при $n = 5$ вона має вже 120 членів і т.д.). Тому розглянемо тепер деякі елементарні (але важливі) властивості визначників, які дають можливість досить просто знаходити їх. Точніше, будемо розглядати деякі перетворення матриць, які не змінюють їх визначників. За допомогою цих перетворень ми зможемо переходити від даної матриці до іншої, яка має той же визначник, але цей визначник можна вже просто підрахувати.

6.2. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$, $B = A'$.

Тоді $\det(A) = \det(B)$.

Доведення. Нехай $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, $b_{ij} = a_{ji}$, $1 \leq i, j \leq n$.

Маємо

$$\det(A) = \sum_{\pi \in S_n} d_{\pi},$$

де $d_{\pi} = \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$.

Далі

$$\begin{aligned} \det(B) &= \sum_{\pi \in S_n} \text{sign } \pi b_{1\pi(1)} b_{2\pi(2)} \dots b_{n\pi(n)} = \\ &= \sum_{\pi \in S_n} \text{sign } \pi a_{\pi(1)1} a_{\pi(2)2} \dots a_{\pi(n)n}. \end{aligned}$$

Розглянемо матрицю, стовпцями якої будуть індекси кожного множника довільного члена $\text{sign } \pi a_{\pi(1)1} a_{\pi(2)2} \dots a_{\pi(n)n}$ останньої суми:

$$\begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Очевидно, ця таблиця відповідає підстановці π^{-1} . Таким чином,

$$\begin{aligned} \text{sign } \pi a_{\pi(1)1} a_{\pi(2)2} \dots a_{\pi(n)n} &= \text{sign } \pi a_{1\pi^{-1}(1)} a_{2\pi^{-1}(2)} \dots a_{n\pi^{-1}(n)} = \\ &= \text{sign } \pi^{-1} a_{1\pi^{-1}(1)} a_{2\pi^{-1}(2)} \dots a_{n\pi^{-1}(n)} = d_{\pi^{-1}}, \end{aligned}$$

оскільки $\text{sign } \pi = \text{sign } \pi^{-1}$.

Отже,

$$\det(B) = \sum_{\pi \in S_n} d_{\pi^{-1}}.$$

З леми 6.1 отримуємо рівність

$$\sum_{\pi \in S_n} d_{\pi^{-1}} = \sum_{\pi \in S_n} d_{\pi} = \det(A).$$

Оскільки рядки матриці A^t — це стовпці матриці A , а стовпці матриці A^t — це рядки матриці A , то доведена вище властивість показує, що рядки й стовпці матриці рівноправні відносно властивостей визначників. Звідси випливає, що кожного твердження про визначники, що відноситься до рядків матриці, має місце його аналог і для стовпців. Тому подальші властивості ми будемо формулювати для рядків, маючи на увазі, що аналогічна властивість буде справедливою і для стовпців.

6.3. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ і $a_{kj} = b_j + c_j$ для деякого k , $1 \leq k \leq n$.

Нехай далі

$$U = \|u_{ij}\|_{1 \leq i, j \leq n}, \quad V = \|v_{ij}\|_{1 \leq i, j \leq n},$$

$$\text{де} \quad u_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq k, \\ b_j, & \text{якщо } i = k, \end{cases} \quad v_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq k, \\ c_j, & \text{якщо } i = k. \end{cases}$$

$$\text{Тоді} \quad \det(A) = \det(U) + \det(V).$$

Доведення. Маємо

$$\begin{aligned} \det(A) &= \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{k-1\pi(k-1)} a_{k\pi(k)} a_{k+1\pi(k+1)} \dots a_{n\pi(n)} = \\ &= \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{k-1\pi(k-1)} (b_{\pi(k)} + c_{\pi(k)}) a_{k+1\pi(k+1)} \dots a_{n\pi(n)} = \\ &= \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{k-1\pi(k-1)} b_{\pi(k)} a_{k+1\pi(k+1)} \dots a_{n\pi(n)} + \\ &+ \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{k-1\pi(k-1)} c_{\pi(k)} a_{k+1\pi(k+1)} \dots a_{n\pi(n)} = \end{aligned}$$

$$\begin{aligned}
&= \sum_{\pi \in S_n} \text{sign } \pi u_{1\pi(1)} u_{2\pi(2)} \cdots u_{n\pi(n)} + \sum_{\pi \in S_n} \text{sign } \pi v_{1\pi(1)} v_{2\pi(2)} \cdots v_{n\pi(n)} = \\
&= \det(U) + \det(V).
\end{aligned}$$

6.4. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ і $a_{kj} = \alpha b_j$ для деякого k , $1 \leq k \leq n$.

Нехай далі $U = \|u_{ij}\|_{1 \leq i, j \leq n}$, де $u_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq k, \\ b_j, & \text{якщо } i = k. \end{cases}$

Тоді $\det(A) = \alpha \det(U)$.

Доведення. Маємо

$$\begin{aligned}
\det(A) &= \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \cdots a_{k-1\pi(k-1)} a_{k\pi(k)} a_{k+1\pi(k+1)} \cdots a_{n\pi(n)} = \\
&= \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \cdots a_{k-1\pi(k-1)} (\alpha b_{\pi(k)}) a_{k+1\pi(k+1)} \cdots a_{n\pi(n)} = \\
&= \alpha \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \cdots a_{k-1\pi(k-1)} b_{\pi(k)} a_{k+1\pi(k+1)} \cdots a_{n\pi(n)} = \\
&= \alpha \sum_{\pi \in S_n} \text{sign } \pi u_{1\pi(1)} u_{2\pi(2)} \cdots u_{n\pi(n)} = \alpha \det(U).
\end{aligned}$$

6.5. Наслідок. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ і $a_{kj} = 0$ для деякого k , $1 \leq k \leq n$. Тоді $\det(A) = 0$.

6.6. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$, k, t — деякі числа, $1 \leq k < t \leq n$.

Нехай далі $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, де $b_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq k, t, \\ a_{ij}, & \text{якщо } i = k, \\ a_{kj}, & \text{якщо } i = t. \end{cases}$

Тоді $\det(B) = -\det(A)$.

Доведення. Маємо

$$\det(A) = \sum_{\pi \in S_n} d_{\pi},$$

де $d_{\pi} = \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}$.

Далі,

$$\det(B) = \sum_{\pi \in S_n} \pi u_{\pi},$$

$$\begin{aligned}
\text{де} \quad u_{\pi} &= b_{1\pi(1)} b_{2\pi(2)} \cdots b_{k-1\pi(k-1)} b_{k\pi(k)} b_{k+1\pi(k+1)} \cdots \\
&\cdots b_{t-1\pi(t-1)} b_{t\pi(t)} b_{t+1\pi(t+1)} \cdots b_{n\pi(n)} = a_{1\pi(1)} a_{2\pi(2)} \cdots \\
&\cdots a_{k-1\pi(k-1)} a_{k\pi(k)} a_{k+1\pi(k+1)} \cdots a_{t-1\pi(t-1)} a_{t\pi(t)} a_{t+1\pi(t+1)} \cdots a_{n\pi(n)}.
\end{aligned}$$

Розглянемо матрицю, стовпцями якої будуть індекси кожного множника довільного члена останньої суми:

$$\begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & \dots & t-1 & t & t+1 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(k-1) & \pi(k) & \pi(k+1) & \dots & \pi(t-1) & \pi(t) & \pi(t+1) & \dots & \pi(n) \end{pmatrix}.$$

Покажемо, що ця таблиця відповідає деякій підстановці $\vartheta(\pi)$. Розглянемо підстановку $\pi \odot \tau_{k,t}$. Нехай $i \neq k, t$, тоді

$$\pi \odot \tau_{k,t}(i) = \pi(\tau_{k,t}(i)) = \pi(i).$$

Далі

$$\pi \odot \tau_{k,t}(k) = \pi(\tau_{k,t}(k)) = \pi(t),$$

$$\pi \odot \tau_{k,t}(t) = \pi(\tau_{k,t}(t)) = \pi(k).$$

Це означає, що $\vartheta(\pi) = \pi \odot \tau_{k,t}$.

Оскільки $\text{sign } \pi \odot \tau_{k,t} = \text{sign } \pi \text{ sign } \tau_{k,t}$, а транспозиція є непарною підстановкою, то

$$\text{sign } \vartheta(\pi) = -\text{sign } \pi \quad \text{або} \quad \text{sign } \pi = -\text{sign } \vartheta(\pi).$$

Отже,

$$\text{sign } \pi b_{1\pi(1)} b_{2\pi(2)} \dots b_{n\pi(n)} = -\text{sign } \vartheta(\pi) a_{1\vartheta(\pi)(1)} a_{2\vartheta(\pi)(2)} \dots a_{n\vartheta(\pi)(n)} = -d_{\vartheta(\pi)}.$$

Тепер можемо отримати

$$\det(B) = \sum_{\pi \in S_n} (-d_{\vartheta(\pi)}) = - \sum_{\pi \in S_n} d_{\vartheta(\pi)}.$$

Оскільки $\vartheta(\pi) = \pi \odot \tau_{k,t}$, то з леми 6.1 випливає рівність

$$\det(B) = - \sum_{\pi \in S_n} d_{\vartheta(\pi)} = - \sum_{\pi \in S_n} d_{\pi} = -\det(A).$$

6.7. Наслідок. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$.

Якщо матриця A має два однакових рядки, то $\det(A) = 0$.

Доведення. Нехай рядки з номерами k, t співпадають. Поміняємо їх місцями. За попередньою властивістю визначник змінює знак. Але ж, поміняв однакові рядки, ми не змінили матрицю, а отже, і не змінили її визначник. Таким чином, $\det(A) = -\det(A)$. Звідси випливає, що $\det(A) = 0$.

6.8. Наслідок. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$, k, t — деякі числа, $1 \leq k < t \leq n$.

Нехай далі $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, де $b_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq k, \\ b_{kj} + \alpha a_{tj}, & \text{якщо } i = k \end{cases}$

для деякого числа α .

Тоді $\det(B) = \det(A)$.

Доведення. Нехай $U = \|u_{ij}\|_{1 \leq i, j \leq n}$,

де $u_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq k, \\ b_{tj}, & \text{якщо } i = k. \end{cases}$

З пропозицій 6.3, 6.4 отримаємо рівність

$$\det(B) = \det(A) + \alpha \det(U).$$

З наслідку 6.7 випливає, що $\det(U) = 0$, тому $\det(B) = \det(A)$.

Нехай маємо рядки

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

та числа $\alpha_1, \alpha_2, \dots, \alpha_m$. Рядок $(b_1, b_2, \dots, b_n)$, де

$$b_i = \alpha_1 a_{1i} + \alpha_2 a_{2i} + \dots + \alpha_m a_{mi}, \quad 1 \leq i \leq n,$$

будемо називати лінійною комбінацією даних рядків з коефіцієнтами $\alpha_1, \alpha_2, \dots, \alpha_m$ відповідно.

6.9. Наслідок. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Якщо до деякого рядка матриці A додати лінійну комбінацію деяких інших рядків цієї матриці, то визначник нової матриці дорівнює визначнику попередньої матриці.

6.10. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Якщо A — трикутна матриця, то $\det(A) = a_{11} a_{22} \dots a_{nn}$.

Доведення. Маємо

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

Нехай π — підстановка степеня n і $\pi \neq \epsilon$. Тоді знайдеться індекс m , для якого $\pi(m) \neq m$. Нехай k — найбільший індекс з властивістю $\pi(k) \neq k$. Оскільки

$$\pi(k+1) = k+1, \dots, \pi(n) = n,$$

то $\pi(k) \notin \{k, k+1, \dots, n\}$, а значить $k > \pi(k)$. Звідси випливає, що $a_{k\pi(k)} = 0$. Отже у сумі, що дає розклад $\det(A)$, ненульовим може бути тільки член, індексований тотожною підстановкою, тобто

$$\det(A) = a_{11} a_{22} \dots a_{nn}.$$

Користуючись властивостями, що доведені вище, ми отримуємо наступний метод знаходження визначників. Він фактично повторює метод Гауса. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Розглянемо зараз перетворення матриці, які не змінюють її визначника, або змінюють тільки його знак, та приводять матрицю до трикутного вигляду. Розглянемо елементи a_{i1} , $1 \leq i \leq n$. Якщо всі вони дорівнюють нулю,

матриця A має нульовий стовпець i за наслідком 6.5 її визначник дорівнює нулю. Таким чином знайдеться індекс k , для якого $a_{k1} \neq 0$. Можна вважати, що $a_{11} \neq 0$, якщо це не так, можна поміняти місцями 1-й та k -й рядки, у цьому випадку за пропозицією 6.6 визначник отриманої матриці відрізняється від $\det(A)$ тільки знаком. Перший рядок множимо на число $-a_{11}/a_{11}$ та додаємо до i -го рядка, $2 \leq i \leq n$. За наслідком 6.8 кожне таке перетворення не змінює визначника. Таким чином, ми отримали матрицю, у якій всі елементи першого стовпця, окрім першого, дорівнюють нулю. Розглядаємо тепер другий стовпець і застосовуємо до нього аналогічні перетворення і т.д. В результаті всіх таких перетворень ми приходимо до трикутної матриці, визначник якої можна знайти, користуючись пропозицією 6.10.

Як приклад, застосуємо доведені вище властивості для знаходження визначників кососиметричних матриць. Нехай A — кососиметрична матриця. Множимо кожний рядок на -1 і отримуємо матрицю $-A$. Оскільки $-A = A'$, то враховуючи пропозиції 6.2 та 6.4, отримуємо

$$\det(A) = \det(A') = \det(-A) = (-1)^n \det(A).$$

Звідси отримуємо, що якщо порядок кососиметричної матриці A — непарний, то $\det(A) = 0$.

7. МІНОРИ, АЛГЕБРИЧНІ ДОПОВНЕННЯ, ЇХ РОЛЬ

Існують методи знаходження визначників, які базуються на тому, що визначник матриці може бути виражений через визначники деяких її підматриць. Поняття, що вводиться нижче, будуть одним з основних для цього підходу.

Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. В матриці A вибираємо t рядків та t стовпців. Нехай це будуть рядки з номерами $k(1), k(2), \dots, k(t)$ та стовпці з номерами $j(1), j(2), \dots, j(t)$. Розглянемо підматрицю, яка утворена з коефіцієнтів, що стоять на перетині цих вибраних рядків та стовпців. *Визначник цієї підматриці називається мінором порядку t , що відповідає рядкам з номерами $k(1), k(2), \dots, k(t)$ та стовпцям з номерами $j(1), j(2), \dots, j(t)$.* Цей міnor будемо позначати через

$$\text{minor} \{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\}.$$

Викреслимо тепер виділені рядки та стовпці; отримуємо підматрицю порядку $n - t$. *Визначник цієї підматриці називається доповнюючим мінором до мінора порядку t , що відповідає рядкам з номерами $k(1), k(2), \dots, k(t)$ та стовпцям з номерами $j(1), j(2), \dots, j(t)$; він будемо позначатися через*

$$\text{com} \{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\}.$$

І, нарешті, алгебричним доповненням до мінору порядку t , що відповідає рядкам з номерами $k(1), k(2), \dots, k(t)$ та стовпцям з номерами $j(1), j(2), \dots, j(t)$, називається число

$$A_{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)} = (-1)^{k(1)+k(2)+\dots+k(t)+j(1)+j(2)+\dots+j(t)} \operatorname{com}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\}.$$

7.1. Теорема. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. В матриці A вибираємо t рядків та t стовпців. Розглянемо мінор, що відповідає цим рядкам та стовпцям. Це буде сума $t!$ членів, кожен з яких є добутком (взятим зі знаком «+» або «-») t елементів матриці A . Алгебричне доповнення до виділеного мінору буде сумою $(n-t)!$ членів, кожен з яких є добутком (взятим зі знаком «+» або «-») $(n-t)$ елементів матриці A . Перемножимо ці дві суми. В результаті отримаємо частину суми, що дає розклад визначника матриці A .

Д о в е д е н н я . Нехай виділеними будуть рядки з номерами $k(1), k(2), \dots, k(t)$ та стовпці з номерами $j(1), j(2), \dots, j(t)$. Припустимо спочатку, що

$$k(1) = 1, k(2) = 2, \dots, k(t) = t, j(1) = 1, j(2) = 2, \dots, j(t) = t.$$

У цьому випадку виділений мінор $\operatorname{minor}\{1, 2, \dots, t; 1, 2, \dots, t\} = \Delta$ буде визначником підматриці $B = \|b_{ij}\|_{1 \leq i, j \leq t}$, де $b_{ij} = a_{ij}$, $1 \leq i, j \leq t$, а алгебричне доповнення до нього $A_{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)} = \Xi$ збігається з доповнюючим мінором і буде визначником підматриці $C = \|c_{ij}\|_{1 \leq i, j \leq n-t}$, де $c_{ij} = a_{i+t, j+t}$, $1 \leq i, j \leq n-t$. Отже, маємо

$$\Delta = \det(B) = \sum_{\pi \in S_t} \operatorname{sign} \pi b_{1\pi(1)} b_{2\pi(2)} \dots b_{t\pi(t)};$$

$$\Xi = \det(C) = \sum_{\sigma \in S_{n-t}} \operatorname{sign} \sigma c_{1\sigma(1)} c_{2\sigma(2)} \dots c_{n-t\sigma(n-t)}.$$

Розглянемо їх добуток

$$\begin{aligned} \Delta \Xi &= \left(\sum_{\pi \in S_t} \operatorname{sign} \pi b_{1\pi(1)} b_{2\pi(2)} \dots b_{t\pi(t)} \right) \times \\ &\times \left(\sum_{\sigma \in S_{n-t}} \operatorname{sign} \sigma c_{1\sigma(1)} c_{2\sigma(2)} \dots c_{n-t\sigma(n-t)} \right) = \\ &= \sum_{\pi \in S_t} \sum_{\sigma \in S_{n-t}} \operatorname{sign} \pi \operatorname{sign} \sigma b_{1\pi(1)} b_{2\pi(2)} \dots b_{t\pi(t)} c_{1\sigma(1)} c_{2\sigma(2)} \dots c_{n-t\sigma(n-t)} = \\ &= \sum_{\pi \in S_t} \sum_{\sigma \in S_{n-t}} \operatorname{sign} \pi \operatorname{sign} \sigma a_{1\pi(1)} a_{2\pi(2)} \dots \\ &\dots a_{t\pi(t)} a_{t+1\pi(t)+\sigma(1)} a_{t\pi(t)+t+\sigma(2)} \dots a_{n\pi(t)+\sigma(n-t)}. \end{aligned}$$

Розглянемо перетворення $\rho = \rho(\pi, \sigma)$ множини $\{1, 2, \dots, n\}$,

яке наступним чином визначається за підстановками $\pi \in S_t$ та $\sigma \in S_{n-t}$. Покладемо

$$\rho(1) = \pi(1), \rho(2) = \pi(2), \dots, \rho(t) = \pi(t),$$

$$\rho(t+1) = t + \sigma(1), \rho(t+2) = t + \sigma(2), \dots, \rho(n) = t + \sigma(n-t).$$

Покажемо, що ρ буде підстановкою степеня n . Нехай k, m — довільні числа з множини $\{1, 2, \dots, n\}$, $k < m$. Якщо $m \leq t$, то $\rho(k) = \pi(k) \neq \pi(m) = \rho(m)$; у випадку, коли $m > t$, $k \leq t$ маємо $\rho(k) = \pi(k) \leq t < t + \sigma(m-t) = \rho(m)$; і, нарешті, якщо $k > t$, то $\rho(k) = t + \sigma(k-t) \neq t + \sigma(m-t) = \rho(m)$.

Отже ρ ін'єктивне. Звідси випливає, що

$$|\text{Im } \rho| = |\{1, 2, \dots, n\}| = n,$$

тобто $\text{Im } \rho = \{1, 2, \dots, n\}$ і, отже, $\rho \in S_n$.

Підрахуємо тепер парність підстановки ρ . Нехай пара чисел k, m , $1 \leq k < m \leq n$, утворює інверсію відносно ρ . Знову розглянемо всі можливі випадки.

Якщо $m \leq t$, то $\rho(k) = \pi(k) \neq \pi(m) = \rho(m)$, так що k, m утворюють інверсію відносно π . У випадку, коли $m > t$, $k \leq t$ маємо

$$\rho(k) = \pi(k) \leq t < t + \sigma(m-t) = \rho(m),$$

і інверсію не отримуємо. Нарешті, якщо $k > t$, то

$$\rho(k) = t + \sigma(k-t) \neq t + \sigma(m-t) = \rho(m),$$

так що $k-t, m-t$ утворюють інверсію відносно σ . Звідси випливає, що $i(\rho) = i(\pi) + i(\sigma)$, отже,

$$\text{sign } \rho = (-1)^{i(\rho)} = (-1)^{i(\pi) + i(\sigma)} = (-1)^{i(\pi)} (-1)^{i(\sigma)} = (\text{sign } \pi)(\text{sign } \sigma).$$

Отже, коли примусити π пробігати всі підстановки степеня t , а σ — всі підстановки степеня $n-t$, підстановка $\rho(\pi, \sigma)$ буде пробігати деяку підмножину S_n (це буде власна підмножина, оскільки її порядок дорівнює $(t!)((n-t)!) < n!$). Повертаючись до нашого добутку ΔE , можемо написати тепер

$$\begin{aligned} \Delta E &= \sum_{\pi \in S_t} \sum_{\sigma \in S_{n-t}} \text{sign } \pi \text{sign } \sigma a_{1\pi(1)} a_{2\pi(2)} \dots \\ &\dots a_{t\pi(t)} a_{t+1\ t+\sigma(1)} a_{t+2\ \pi(t)} a_{t+3\ t+\sigma(2)} \dots a_{nt\ \sigma(n-t)} = \\ &= \sum_{\substack{\pi \in S_t, \\ \sigma \in S_{n-t}}} \text{sign } \rho(\pi, \sigma) a_{1\rho(1)} a_{2\rho(2)} \dots a_{n\rho(n)} = \\ &= \sum_{\substack{\text{по деяким} \\ \text{підстановкам} \\ \rho \in S_n}} \text{sign } \rho a_{1\rho(1)} a_{2\rho(2)} \dots a_{n\rho(n)}. \end{aligned}$$

Отже, дійсно отримали частину суми, що дає розклад визначника матриці A .

Розглянемо тепер загальний випадок. Будемо вважати, що

$$k(1) < k(2) < \dots < k(t) \text{ та } j(1) < j(2) < \dots < j(t).$$

Згадаємо, що коли в матриці A поміняти місцями два рядки (стовпці), то за пропозицією 6.6 визначник нової матриці відрізняється від визначника старої тільки множником, що дорівнює -1 . Застосовуючи цю властивість, спробуємо, міняючи рядки та стовпці, добитися того, щоб потрібна нам підматриця розташувалася у верхньому лівому куті матриці A , і при цьому взаємне розташування всіх інших рядків та стовпців не змінилося. Для цього рядок з номером $k(1)$ міняємо місцями з $(k(1) - 1)$ -м, далі з $(k(1) - 2)$ -м і т.д., поки цей рядок не займе перше місце. Для цього потрібно застосувати $k(1) - 1$ вказаних перетворень. Далі будемо послідовно представляти рядок з номером $k(2)$ з рядками, що розташовані над ним, поки він не займе друге місце в матриці; для цього потрібно застосувати $k(2) - 2$ перетворень. Аналогічно будемо чинити з іншими виділеними рядками, поки вони не займуть перші t місць у матриці. В результаті потрібно було зробити

$$\begin{aligned} & (k(1) - 1) + (k(2) - 2) + \dots + (k(t) - t) = \\ & = (k(1) + k(2) + \dots + k(t)) - (1 + 2 + \dots + t) \end{aligned}$$

перетворень рядків. Аналогічну операцію виконаємо і з виділеними стовпцями. Для цього потрібно буде зробити

$$\begin{aligned} & (j(1) - 1) + (j(2) - 2) + \dots + (j(t) - t) = \\ & = (j(1) + j(2) + \dots + j(t)) - (1 + 2 + \dots + t) \end{aligned}$$

перетворень стовпців.

В результаті отримали нову матрицю D , в якій виділені раніше рядки та стовпці утворюють підматрицю порядку t , що розташована у лівому верхньому куті, при цьому взаємне розташування всіх інших рядків та стовпців не змінилося, тобто якщо викреслити перші t рядків та стовпців, то отримаємо підматрицю, визначник якої і буде доповнюючим мінором до мінору матриці A , розташованому у рядках з номерами $k(1), k(2), \dots, k(t)$ та стовпцях з номерами $j(1), j(2), \dots, j(t)$.

За пропозицією 6.6

$$\begin{aligned} \det(D) &= (-1)^{(k(1)+k(2)+\dots+k(t))-(1+2+\dots+t)+(j(1)+j(2)+\dots+j(t))-(1+2+\dots+t)} \det(A) = \\ &= (-1)^{k(1)+k(2)+\dots+k(t)+j(1)+j(2)+\dots+j(t)} \det(A). \end{aligned}$$

$$\text{Звідси } \det(A) = (-1)^{k(1)+k(2)+\dots+k(t)+j(1)+j(2)+\dots+j(t)} \det(D).$$

Мінор Δ_D матриці D , що відповідає рядкам з номерами $1, 2, \dots, t$ та стовпцям з номерами $1, 2, \dots, t$, дорівнює мінору матриці A , що відповідає рядкам з номерами $k(1), k(2), \dots, k(t)$

та стовпцям з номерами $j(1), j(2), \dots, j(t)$, а його доповнюючий мінор Ξ_D дорівнює

$$\text{com}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\}.$$

Вище було доведено, що добуток

$$\Delta_D \Xi_D = \text{minor}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\} \times \\ \times \text{com}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\}$$

буде частиною суми, що дає розклад визначника матриці D . Враховуючи рівність

$$\det(A) = (-1)^{k(1)+k(2)+\dots+k(t)+j(1)+j(2)+\dots+j(t)} \det(D)$$

та той факт, що

$$A_{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)} = \\ = (-1)^{k(1)+k(2)+\dots+k(t)+j(1)+j(2)+\dots+j(t)} \text{com}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\},$$

отримаємо, що добуток

$$\text{minor}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\} A_{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)}$$

буде частиною суми, що дає розклад визначника матриці A .

Застосуємо доведену зараз теорему для отримання нових методів обчислення визначників матриць.

7.2. Теорема (розклад визначника за рядком чи стовпцем). Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. В матриці A вибираємо рядок (відповідно стовпець) з номером t . Кожний елемент a_{tj} (відповідно a_{ij}) цього рядка (що розглядається як мінор 1-го порядку) (відповідно стовпця) множимо на його алгебричне доповнення A_{tj} (відповідно A_{ij}). Тоді

$$\det(A) = \sum_{1 \leq j \leq n} a_{tj} A_{tj}$$

$$(\text{відповідно } \det(A) = \sum_{1 \leq j \leq n} a_{jt} A_{jt}).$$

Доведення. Зважаючи на пропозицію 6.2, можна розглянути тільки випадок, коли в матриці виділено рядок.

Нехай

$$P_{tj} = \{\pi \in S_n \mid \pi(t) = j\}.$$

Як і в теоремі 4.2 можна довести, що $|P_{tj}| = (n-1)!$, $P_{tj} \cap P_{tm} = \emptyset$, якщо $j \neq m$ та $S_n = \bigcup_{1 \leq j \leq n} P_{tj}$. Звідси випливає рівність

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)} = \\ = \sum_{1 \leq j \leq n} \sum_{\pi \in P_{tj}} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

За теоремою 7.1 добуток $a_{tj}A_{tj}$ дорівнює деякій частині суми, що дає розклад визначника матриці A . Нехай $\text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$ належить до цієї частини. Оскільки кожен член цієї частини має множником a_{tj} , то $\pi(t) = j$. Алгебричне доповнення відрізняється від визначника матриці порядку n тільки множником $(-1)^{t+j}$, а тому розклад $a_{tj}A_{tj}$ містить рівно $(n-1)!$ членів. Звідси випливає рівність

$$a_{tj}A_{tj} = \sum_{\pi \in P_{tj}} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

а тому

$$\det(A) = \sum_{1 \leq j \leq n} a_{tj}A_{tj}.$$

7.3. Наслідок. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Має місце наступна рівність

$$\sum_{1 \leq j \leq n} a_{tj}A_{tj} = \delta_{tm} \det(A),$$

$$(\text{відповідно } \sum_{1 \leq j \leq n} a_{tj}A_{jm} = \delta_{tm} \det(A)), \quad 1 \leq t, m \leq n.$$

Доведення. Нехай $(c_1, c_2, \dots, c_n)$ — довільний набір n чисел. Замінімо в матриці A рядок з номером t даним набором чисел та позначимо отриману матрицю через B .

$$\text{Нехай } B = \|b_{ij}\|_{1 \leq i, j \leq n}, \text{ тобто } b_{ij} = \begin{cases} a_{ij}, & \text{якщо } i \neq t, \\ c_j, & \text{якщо } i = t. \end{cases}$$

З теореми 7.2 отримуємо рівність

$$\det(B) = \sum_{1 \leq j \leq n} b_{tj}B_{tj}.$$

Очевидно, алгебричне доповнення B_{tj} до елемента b_{tj} в матриці B збігається з A_{tj} (щоб його отримати, ми викреслюємо рядок з номером t , тобто викреслюється те, чим відрізняється матриця B від матриці A). Враховуючи визначення елементів b_{ij} , отримуємо рівність

$$\det(B) = \sum_{1 \leq j \leq n} c_j A_{tj}.$$

Тепер покладемо $c_j = a_{mj}$, $1 \leq j \leq n$. Якщо $m = t$, то $B = A$ і за теоремою 7.2 $\sum_{1 \leq j \leq n} a_{tj}A_{tj} = \det(A)$. Якщо ж $m \neq t$, то матриця B має два однакових рядки. Наслідок 6.7 показує, що в цьому випадку її визначник дорівнює нулю, тобто $\sum_{1 \leq j \leq n} a_{tj}A_{mj} = 0$. За допомогою символів Кронекера можемо об'єднати ці дві рівності у одну:

$$\sum_{1 \leq j \leq n} a_{tj}A_{mj} = \delta_{tm} \det(A).$$

Як приклад застосування теореми 7.2, знайдемо визначник наступної матриці

$$A_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_{n-1}^2 & a_n^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_{n-1}^{n-1} & a_n^{n-1} \end{pmatrix}.$$

Визначник матриці такого типу називається *визначником Ван-дермонда*. Розглянемо спочатку випадок $n = 2$. Маємо

$$\det(A_2) = \begin{vmatrix} 1 & 1 \\ a_1 & a_2 \end{vmatrix} = a_2 - a_1.$$

Виникає наступна індуктивна гіпотеза: $\det(A_n) = \prod_{1 \leq k < l \leq n} (a_l - a_k)$.

Припустимо, що ця формула є вірною для всіх A_m , де $m < n$. Застосуємо до матриці A_n наступні перетворення. Множимо $(n-1)$ -й рядок на число $(-a_1)$ та додаємо до n -го рядка. Далі $(n-2)$ -й рядок множимо на число $(-a_1)$ та додаємо до $(n-1)$ -го рядка і т.д. І, нарешті, 1-й рядок множимо на число $(-a_1)$ та додаємо до 2-го рядка.

В результаті всіх цих перетворень отримуємо наступну матрицю

$$B_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & a_2 - a_1 & a_3 - a_1 & \dots & a_{n-1} - a_1 & a_n - a_1 \\ 0 & a_2^2 - a_1 a_2 & a_3^2 - a_1 a_3 & \dots & a_{n-1}^2 - a_1 a_{n-1} & a_n^2 - a_1 a_n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a_2^{n-1} - a_1 a_2^{n-2} & a_3^{n-1} - a_1 a_3^{n-2} & \dots & a_{n-1}^{n-1} - a_1 a_{n-1}^{n-2} & a_n^{n-1} - a_1 a_n^{n-2} \end{pmatrix}.$$

За наслідком 6.8 $\det(B_n) = \det(A_n)$. Розкладаючи тепер визначник матриці B_n за першим стовпцем, використовуючи теорему 7.2, маємо

$$\det(B_n) = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) \begin{vmatrix} 1 & 1 & \dots & 1 & 1 \\ a_2 & a_3 & \dots & a_{n-1} & a_n \\ a_2^2 & a_3^2 & \dots & a_{n-1}^2 & a_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ a_2^{n-1} & a_3^{n-1} & \dots & a_{n-1}^{n-1} & a_n^{n-1} \end{vmatrix}.$$

Застосовуючи індуктивну гіпотезу, отримуємо нарешті,

$$\begin{aligned} \det(A_n) &= \det(B_n) = \\ &= (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) \prod_{2 \leq k < l \leq n} (a_l - a_k) = \prod_{1 \leq k < l \leq n} (a_l - a_k). \end{aligned}$$

Теорема 7.2 допускає наступне узагальнення.

7.4. Теорема (теорема Лапласа).

Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. В матриці A вибираємо t рядків (відповідно t стовпців). Кожен мінор порядку t , що відповідає вибраним рядкам (відповідно стовпцям), множимо на його алгебричне доповнення. Тоді сума всіх цих добутків дорівнює $\det(A)$.

Д о в е д е н н я . Зважаючи на пропозицію 6.2, можна розглянути тільки випадок, коли вибираються рядки. Нехай виділеними будуть рядки з номерами $k(1), k(2), \dots, k(t)$. Згадаємо що

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

Розглянемо довільний член $\text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$ цієї суми. Розглянемо окремо добуток тих елементів, перші індекси яких належать до виділених рядків, тобто добуток $a_{k(1)\pi(k(1))} a_{k(2)\pi(k(2))} \dots a_{k(t)\pi(k(t))}$. Цей добуток (зі знаком «+» або «-») належить, очевидно, до розкладу

$$\text{minor}\{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))\}.$$

Очевидно також, що добуток усіх інших елементів $a_{j\pi(j)}$, $j \notin \{k(1), \dots, k(t)\}$ (знову ж таки зі знаком «+» або «-») належить до розкладу

$$\text{com}\{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))\}.$$

Зважаючи на теорему 7.1, отримуємо звідси, що член $\text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$ належить до розкладу

$$\text{minor}\{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))\}$$

та

$$A_{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))}.$$

Таким чином, всякий член суми, що дає розклад $\det(A)$, входить до розкладу добутку деякого мінора, який відповідає вибраним рядкам, на його алгебричне доповнення. Розклад

$$\text{minor}\{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))\}$$

містить $t!$ членів, а розклад

$$A_{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))}$$

містить $(n - t)!$ членів. Отже, розклад добутку

$$\text{minor}\{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))\}$$

та

$$A_{k(1), k(2), \dots, k(t); \pi(k(1)), \pi(k(2)), \dots, \pi(k(t))}$$

містить $t!(n-t)!$ членів. Покажемо тепер, що розклади добутоків двох різних мінорів, які відповідають вибраним рядкам, на їх алгебричні доповнення не містять однакових членів. Дійсно, нехай

$$\{j(1), j(2), \dots, j(t)\} \neq \{s(1), s(2), \dots, s(t)\}$$

та нехай $\text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$ належить до розкладу добутку

$$\text{minor}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\} A_{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)},$$

а $\text{sign } \sigma a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$ належить до розкладу добутку

$$\text{minor}\{k(1), k(2), \dots, k(t); s(1), s(2), \dots, s(t)\} A_{k(1), k(2), \dots, k(t); s(1), s(2), \dots, s(t)}.$$

Це означає, зокрема, що

$$\{\pi(k(1)), \pi(k(2)), \dots, \pi(k(t))\} = \{j(1), j(2), \dots, j(t)\} \neq$$

$$\neq \{s(1), s(2), \dots, s(t)\} = \{\sigma(k(1)), \sigma(k(2)), \dots, \sigma(k(t))\}.$$

Далі, загальна кількість мінорів порядку t , що відповідають вибраним рядкам, дорівнює числу сполучень з n по t , тобто числу $(n!)/(t!(n-t)!)$. Таким чином, сума добутоків усіх мінорів порядку t , що відповідають вибраним рядкам, на їх алгебричні доповнення дають нам $(t!(n-t)!)(n!)/(t!(n-t)!)=n!$ членів з розкладу $\det(A)$. Оскільки розклад $\det(A)$ містить рівно $n!$ членів, то звідси і отримуємо, що сума добутоків усіх мінорів порядку t , що відповідають вибраним рядкам, на їх алгебричні доповнення дорівнює $\det(A)$.

Теорема Лапласа дозволяє зводити обчислення визначників матриць до обчислення визначників матриць менших порядків. Але ж цих менших матриць може бути дуже й дуже багато, тому теорему Лапласа доцільно застосовувати тільки для матриць, в яких можна виділити рядки, що мають велику кількість нулів.

Наприклад, нехай

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1t} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2t} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{t1} & a_{t2} & \dots & a_{tt} & 0 & \dots & 0 \\ a_{t+11} & a_{t+12} & \dots & a_{t+1t} & a_{t+1t+1} & \dots & a_{t+1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nt} & a_{nt+1} & \dots & a_{nn} \end{pmatrix}.$$

Скорочуючи, можна зобразити матрицю A у вигляді

$$\begin{pmatrix} B & O \\ C & D \end{pmatrix},$$

де

$$B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1t} \\ a_{21} & a_{22} & \dots & a_{2t} \\ \dots & \dots & \dots & \dots \\ a_{t1} & a_{t2} & \dots & a_{tt} \end{pmatrix}, \quad C = \begin{pmatrix} a_{t+11} & a_{t+12} & \dots & a_{t+1t} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nt} \end{pmatrix},$$

$$D = \begin{pmatrix} a_{t+1t+1} & a_{t+1t+2} & \dots & a_{t+1n} \\ \dots & \dots & \dots & \dots \\ a_{nt+1} & a_{nt+2} & \dots & a_{nn} \end{pmatrix}.$$

O — нульова матриця розміру $t \times (n - t)$.

Кожен мінор $\text{minor}\{k(1), k(2), \dots, k(t); j(1), j(2), \dots, j(t)\}$, де $\{j(1), j(2), \dots, j(t)\} \neq \{1, 2, \dots, t\}$, буде визначником матриці, що має нульовий стовпець, а тому дорівнює нулю за наслідком 6.5. Отже, з теореми 7.4 отримуємо рівність

$$\det(A) = \det(B) \det(D).$$

8. ВЛАСТИВОСТІ ОПЕРАЦІЇ МНОЖЕННЯ МАТРИЦЬ

Розглянемо зараз подальші властивості операції множення матриць і перш за все питання про умови існування оберненої матриці. Але спочатку розглянемо наступну теорему, яка відіграє важливу роль не тільки для вирішення цього питання.

8.1. Теорема. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Тоді $\det(AB) = \det(A) \det(B)$.

Доведення. Нехай $AB = C = \|c_{ij}\|_{1 \leq i, j \leq n}$. Розглянемо наступну допоміжну матрицю D порядку $2n$:

$$D = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & \dots & 0 \\ -1 & 0 & \dots & b_{11} & b_{12} & \dots & b_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix},$$

або, використовуючи більш короткий запис,

$$D = \begin{pmatrix} A & O \\ -E & B \end{pmatrix}.$$

Зважаючи на аргументи, які були приведені у кінці попереднього параграфа, маємо $\det(D) = \det(A) \det(B)$.

Застосуємо зараз перетворення стовпців, що не змінюють визначника матриці, для того, щоб заповнити правий нижній кут матриці D нулями. Для цього до $(n+1)$ -го стовпця матриці D додаємо її перший стовпець, помножений на число b_{11} , потім другий, помножений на b_{21} , і т.д. і, нарешті, n -й стовпець, помножений на b_{n1} . Далі до $(n+2)$ -го стовпця матриці D додаємо її перший стовпець, помножений на число b_{12} , потім другий, помножений на b_{22} , і т.д. і нарешті, n -й стовпець, помножений на b_{n2} . Загалом, до $(n+k)$ -го стовпця матриці D додаємо лінійну комбінацію перших n стовпців з коефіцієнтами помноженими на число $b_{1k}, b_{2k}, \dots, b_{nk}$ відповідно.

Отриману матрицю позначимо через H , так що

$$H = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & h_{11} & h_{12} & \dots & h_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} & h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & h_{n1} & h_{n2} & \dots & h_{nn} \\ -1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

За наслідком 6.8 $\det(H) = \det(D)$. Знайдемо тепер елементи h_{ij} . Згадуючи послідовність зроблених перетворень, отримуємо

$$h_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = c_{ij}, \quad 1 \leq i, j \leq n.$$

Інакше кажучи, правий верхній кут матриці H займає матриця AB , тобто

$$H = \begin{pmatrix} A & AB \\ -E & O \end{pmatrix}.$$

Знову застосовуючи аргументи, які були приведені у кінці попереднього параграфа, маємо

$$\det(H) = \text{minor} \{1, 2, \dots, n; n+1, n+2, \dots, 2n\} A_{1, 2, \dots, n; n+1, n+2, \dots, 2n}.$$

Далі

$$\text{minor} \{1, 2, \dots, n; n+1, n+2, \dots, 2n\} = \det(AB),$$

$$A_{1, 2, \dots, n; n+1, n+2, \dots, 2n} = (-1)^{1+2+\dots+n+(n+1)+\dots+2n} (-1)^n = 1,$$

оскільки показник степеня при (-1) дорівнює

$$2n^2 + n + n = 2n^2 + 2n.$$

Таким чином, $\det(H) = \det(AB)$.

Отже маємо

$$\det(A) \det(B) = \det(D) = \det(H) = \det(AB).$$

Використаємо зараз цю теорему для вивчення питання про існування оберненої матриці. Дійсно, якщо для матриці A існує обернена, то з теореми 8.1 одержуємо

$$1 = \det(E) = \det(A A^{-1}) = \det(A) \det(A^{-1}).$$

Матриця $A \in M_n(R)$ називається невинродженою, якщо $\det(A) \neq 0$.

8.2. Теорема. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Матриця A тоді і тільки має обернену, коли вона невинроджена. Більш того, якщо $A^{-1} = \|b_{ij}\|_{1 \leq i, j \leq n}$, то $b_{ij} = A_{ji}/\det(A)$, $1 \leq i, j \leq n$.

Д о в е д е н н я . Ми вже відзначали, що якщо матриця A має обернену, то вона мусить бути невинродженою. Навпаки, нехай $\det(A) \neq 0$. Використаємо для знаходження оберненої матриці наслідок 7.3.

Нехай $b_{ij} = A_{ji}/\det(A)$, $1 \leq i, j \leq n$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$.

Розглянемо добутки $AB = \|u_{ij}\|_{1 \leq i, j \leq n}$ та $BA = \|v_{ij}\|_{1 \leq i, j \leq n}$.
Маємо

$$u_{ij} = \sum_{1 \leq k \leq n} a_{ik} b_{kj} = \sum_{1 \leq k \leq n} a_{ik} (A_{jk}/\det(A)) = (1/\det(A)) \delta_{ij} \det(A) = \delta_{ij},$$

$$v_{ij} = \sum_{1 \leq k \leq n} b_{ik} a_{kj} = \sum_{1 \leq k \leq n} (A_{ki}/\det(A)) a_{kj} = (1/\det(A)) \delta_{ji} \det(A) = \delta_{ij},$$

$$1 \leq i, j \leq n.$$

Це означає, що $AB = BA = E$, тобто $B = A^{-1}$.

Позначимо через $GL_n(R)$ (відповідно $GL_n(Q)$) підмножину всіх невинроджених матриць з $M_n(R)$ (відповідно з $M_n(Q)$).

Зараз розглянемо подальші властивості операції множення матриць. Виділимо зараз деякі важливі типи спеціальних матриць.

Позначимо через $E_{km} = \|u_{ij}^{(km)}\|_{1 \leq i, j \leq n}$, яка визначається за наступним правилом:

$$u_{ij}^{(km)} = 1, \text{ якщо } (i, j) = (k, m),$$

$$u_{ij}^{(km)} = 0, \text{ якщо } (i, j) \neq (k, m).$$

Інакше кажучи,

$$H = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix} \rightarrow k\text{-й рядок}$$

↓

$m\text{-й стовпець}$

Матриця E_{km} буде називатися базовою матрицею.

Обґрунтуванням для такої назви є наступна обставина. Якщо $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, то, очевидно,

$$A = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{ij}.$$

Знайдемо перш за все добуток базових матриць. Нехай

$$E_{km} E_{rs} = \|w_{ij}\|_{1 \leq i, j \leq n},$$

тоді

$$w_{ij} = \sum_{1 \leq t \leq n} u_{it}^{(km)} u_{tj}^{(rs)}.$$

Якщо $i \neq k$, то $u_{it}^{(km)} = 0$ для кожного t , так що $w_{ij} = 0$. Нехай $i = k$, тоді маємо $w_{kj} = u_{km}^{(km)} u_{mj}^{(rs)} = u_{mj}^{(rs)}$. Зокрема, якщо $m \neq r$, то $w_{kj} = 0$. Якщо ж $m = r$, то

$$w_{ks} = u_{ms}^{(rs)} = u_{rs}^{(rs)} = 1, \text{ а } w_{kj} = 0 \text{ для } j \neq s.$$

Таким чином, ми отримали наступне просте правило множення базових матриць:

$$E_{km} E_{rs} = \begin{cases} E_{ks}, & \text{якщо } m = r, \\ 0, & \text{якщо } m \neq r. \end{cases}$$

Скористаємось ним зараз же.

8.3. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Тоді

$$AE_{km} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & a_{1k} & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & a_{2k} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & a_{nk} & 0 & \dots & 0 \end{pmatrix},$$

↓

$k\text{-й стовпець}$

$$E_{km}A = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \\ a_{m1} & a_{m2} & \dots & a_{mn} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \rightarrow k\text{-й рядок}$$

Д о в е д е н н я . Ми вже відзначали, що $A = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{ij}$.
Тоді

$$\begin{aligned} AE_{km} &= \left(\sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{ij} \right) E_{km} = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{ij} E_{km} = \\ &= \sum_{1 \leq i \leq n} a_{ik} E_{ik} E_{km} = \sum_{1 \leq i \leq n} a_{ik} E_{im} = a_{1k} E_{1m} + a_{2k} E_{2m} + \dots + a_{nk} E_{nm}. \end{aligned}$$

$$\begin{aligned} E_{km}A &= E_{km} \left(\sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{ij} \right) = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{km} E_{ij} = \\ &= \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq n} a_{ij} E_{km} E_{ij} = \sum_{1 \leq j \leq n} a_{mj} E_{km} E_{mj} = \sum_{1 \leq j \leq n} a_{mj} E_{kj} = \\ &= a_{m1} E_{k1} + a_{m2} E_{k2} + \dots + a_{mn} E_{kn}. \end{aligned}$$

Інакше кажучи, якщо помножити матрицю A на базову матрицю E_{km} справа, то отримаємо матрицю, m -й стовпець якої — це k -й стовпець матриці A , а всі інші стовпці — нульові. Якщо помножити матрицю A на базову матрицю E_{km} зліва, то отримаємо матрицю, k -й рядок якої — це m -й рядок матриці A , а всі інші рядки — нульові.

Ми вже раніше відзначали, що множення матриць не є комутативним. Більш того, зараз ми переконаємось, що комутативність — це дуже рідке явище у множині матриць.

Нехай S — деяка підмножина $M_n(R)$. Централізатором підмножини S будемо називати сукупність всіх тих матриць, кожна з яких переставна з будь-якою матрицею з множини S . Централізатор усієї множини $M_n(R)$ називається центром алгебри матриць, будемо позначати його через $\zeta(M_n(R))$.

Одинична матриця E переставна з будь-якою матрицею, тобто вона належить до центра. Матриці αE також належать до центра, дійсно

$$A(\alpha E) = \alpha(AE) = \alpha(EA) = (\alpha E)A.$$

Матриця αE називається скалярною.

Покладемо

$$RE = \{\alpha E \mid \alpha \in R\} \text{ (відповідно } QE = \{\alpha E \mid \alpha \in Q\}).$$

Отже, множина скалярних матриць належить до центра алгебри матриць. Кожна скалярна матриця є діагональною. Але не кожна діагональна матриця належить до центра, як показує наступний результат.

8.4. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $D = \|d_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$, та D — діагональна матриця. Множення матриці A на матрицю D зліва (відповідно справа) рівносильне множенню рядків (відповідно стовпців) матриці A на елементи d_{11} , d_{22} , ..., d_{nn} відповідно.

Доведення. Якщо $DA = C = \|c_{ij}\|_{1 \leq i, j \leq n}$, то маємо

$$c_{ij} = \sum_{1 \leq k \leq n} d_{ik} a_{kj} = d_{ii} a_{ij}.$$

Аналогічно для множення справа.

Ми можемо описати центр алгебри матриць.

8.5. Теорема. $\zeta(M_n(R)) = RE$.

Доведення. Раніше ми вже показали, що центр містить у собі множину скалярних матриць. Навпаки, нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in \zeta(M_n(R))$. Матриця A переставна з кожною матрицею, зокрема, вона переставна з кожною базовою матрицею: $AE_{km} = E_{km}A$ для кожної пари індексів k, m , $1 \leq k, m \leq n$.

Покладемо $AE_{km} = \|u_{ij}\|_{1 \leq i, j \leq n}$, $E_{km}A = \|v_{ij}\|_{1 \leq i, j \leq n}$. Припустимо, що $k \neq m$. З пропозиції 8.3 отримуємо, що $u_{jm} = a_{jk}$, а $v_{jm} = 0$ при $j \neq k$. Отже, якщо $j \neq k$, то $a_{jk} = 0$, тобто матриця A повинна бути діагональною.

Застосовуючи тепер пропозицію 8.4, отримуємо, що і всі елементи головної діагоналі матриці A повинні бути рівними, так що A — скалярна матриця.

Розглянемо тепер інші спеціальні матриці, множення на які рівносильне розглянутим вище перетворенням матриць.

Покладемо $t_{km}(\alpha) = E + \alpha E_{km}$, $k \neq m$, $\alpha \in R$. Матрицю $t_{km}(\alpha)$ будемо називати трансекцією. Вона є трикутною і $\det(t_{km}(\alpha)) = 1$. Зокрема, з теореми 8.2 випливає, що трансекція має обернену матрицю. Розглянемо для цього добуток двох трансекцій:

$$\begin{aligned} t_{km}(\alpha)t_{rs}(\beta) &= (E + \alpha E_{km})(E + \beta E_{rs}) = \\ &= E + \alpha E_{km} + \beta E_{rs} + \alpha\beta E_{km}E_{rs}. \end{aligned}$$

Звідси випливає, зокрема, що

$$t_{km}(\alpha)t_{km}(-\alpha) = E,$$

тобто

$$(t_{k\ m}(\alpha))^{-1} = t_{k\ m}(-\alpha).$$

8.6. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Тоді

$$At_{km}(\alpha) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m-1} & a_{1m} + \alpha a_{1k} & a_{1m+1} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2m-1} & a_{2m} + \alpha a_{2k} & a_{2m+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm-1} & a_{nm} + \alpha a_{nk} & a_{nm+1} & \dots & a_{nn} \end{pmatrix},$$

$$t_{km}(\alpha)A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{k-11} & a_{k-12} & \dots & a_{k-1n} \\ a_{k1} + \alpha a_{m1} & a_{k2} + \alpha a_{m2} & \dots & a_{kn} + \alpha a_{mn} \\ a_{k+11} & a_{k+12} & \dots & a_{k+1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Д о в е д е н н я . Це твердження випливає з визначення трансвекції та пропозиції 8.3.

8.7. Теорема. Кожна матриця $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ може бути представлена у вигляді добутку деяких трансвекцій та діагональної матриці.

Д о в е д е н н я . З попередньої пропозиції випливає, що множення матриці A зліва на трансвекцію $t_{k\ m}(\alpha)$ призводить до матриці, всі рядки якої, за виключенням k -го, ті самі, що і у матриці A , а k -й рядок є сумою k -го рядка матриці A та її m -го рядка, помноженого на число α . Перетворення такого типу ми вже застосовували у розділі 6 для того, щоб перейти від матриці A до верхньо-трикутної матриці, яка має той же самий визначник.

Якщо $a_{12} = 0$, але існує такий номер k , що $a_{1k} \neq 0$, то додаючи то другого стовпця k -й стовпець, отримаємо матрицю, коефіцієнт якої з номером (1, 2) буде ненульовим. Цього можна досягти, застосовавши множення на відповідну трансвекцію.

Якщо ж весь перший рядок матриці A є нульовим, то вибираємо рядок, який містить ненульові коефіцієнти. Додаючи його до першого рядка, отримаємо матрицю, перший рядок якої містить ненульові коефіцієнти. Цього можна досягти, застосовавши множення на відповідну транспозицію. Отже можна припустити, що $a_{12} \neq 0$. Додаючи до першого стовпця його другий, помножений на число $(1 - a_{11})/a_{12}$, отримаємо матрицю, коефіцієнт якої з номером (1, 1) буде одиничним.

Тепер застосуємо ті перетворення, які ми вже застосовували у розділі 6 для того, щоб перейти від матриці A до верхньотрикутної матриці, яка має той же самий визначник. Таким чином, помножив матрицю A на відповідні трансвекції зліва, ми перейдемо від матриці A до деякої верхньотрикутної матриці.

Інакше кажучи, існують такі трансвекції $t_{k(1)m(1)}(\alpha_1), \dots, t_{k(i)m(i)}(\alpha_i)$, що $t_{k(i)m(i)}(\alpha_i) \dots t_{k(1)m(1)}(\alpha_1)A$ — верхньотрикутна матриця.

За допомогою аналогічних перетворень, застосованих до стовпців, можна тепер перейти від отриманої матриці до діагональної матриці D . Але, як показує пропозиція 8.6, кожне таке перетворення стовпців рівносильне множенню матриці справа на деяку трансвекцію.

Отже, існують такі трансвекції $t_{q(1)r(1)}(\beta_1), \dots, t_{q(s)r(s)}(\beta_s)$, що

$$t_{k(i)m(i)}(\alpha_i) \dots t_{k(1)m(1)}(\alpha_1) A t_{q(s)r(s)}(\beta_s) \dots t_{q(1)r(1)}(\beta_1) = D —$$

діагональна матриця.

Ми вже відзначали, що $(t_{km}(\alpha))^{-1} = t_{km}(-\alpha)$, тому з отриманої рівності випливає

$$A = t_{k(1)m(1)}(-\alpha_1), \dots, t_{k(i)m(i)}(-\alpha_i) D t_{q(1)r(1)}(-\beta_1), \dots, t_{q(s)r(s)}(-\beta_s).$$

Ми використовували ще перетворення, в результаті яких у матриці міняються місцями два рядка або стовпця. Ці перетворення також рівносильні множенню матриці зліва або справа на наступну спеціальну матрицю. Покладемо

$$g_{km} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \begin{matrix} \rightarrow k\text{-й рядок} \\ \\ \\ \rightarrow m\text{-й рядок} \end{matrix}$$

$\downarrow \qquad \qquad \qquad \downarrow$
 $k\text{-й стовпець} \quad m\text{-й стовпець}$

8.8. Пропозиція. Нехай $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$. Тоді

$$As_{km} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{k-11} & a_{k-12} & \dots & a_{k-1n} \\ a_{m1} & a_{m2} & \dots & a_{mn} \\ a_{k+11} & a_{k+12} & \dots & a_{k+1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m-11} & a_{m-12} & \dots & a_{m-1n} \\ a_{k1} & a_{k2} & \dots & a_{kn} \\ a_{m+11} & a_{m+12} & \dots & a_{m+1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$$s_{km}A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k-1} & a_{1m} & a_{1k+1} & \dots & a_{1m-1} & a_{1k} & a_{1m+1} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2k-1} & a_{2m} & a_{2k+1} & \dots & a_{2m-1} & a_{2k} & a_{2m+1} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nk-1} & a_{nm} & a_{nk+1} & \dots & a_{nm-1} & a_{nk} & a_{nm+1} & \dots & a_{nn} \end{pmatrix}$$

Д о в е д е н н я . Покладемо $s_{km} = \|s_{ij}^{(km)}\|_{1 \leq i, j \leq n}$, тобто

$$s_{ij}^{(km)} = \begin{cases} 1, \text{ якщо } i = j \neq k, m; \\ 1, \text{ якщо } (i, j) = (k, m) \text{ або } (i, j) = (m, k); \\ 0, \text{ в усіх інших випадках.} \end{cases}$$

$$As_{km} = \|v_{ij}\|_{1 \leq i, j \leq n}, \quad s_{km}A = \|w_{ij}\|_{1 \leq i, j \leq n}.$$

Тепер будемо мати

$$v_{ij} = \sum_{1 \leq t \leq n} a_{it} s_{tj}^{(km)}.$$

Якщо $j \neq k, m$, то $v_{ij} = a_{ij} s_{jj}^{(km)} = a_{ij}$. Нехай $j = k$, тоді

$$v_{ik} = a_{im} s_{mk}^{(km)} = a_{im}.$$

При $j = m$ маємо

$$v_{im} = a_{ik} s_{km}^{(km)} = a_{ik}.$$

Аналогічно розглядається і добуток $s_{km}A$.

Частина третя

9. БІНАРНІ АЛГЕБРИЧНІ ОПЕРАЦІЇ, ЇХ ВЛАСТИВОСТІ

В математиці дуже мало понять, які були б більш первісні, ніж поняття бінарної алгебричної операції. Ми вже маємо досить багатий набір конкретних алгебричних операцій, досить багато знаємо про їх властивості. Тепер ми маємо можливість осмислити цей конкретний матеріал з більш загальних позицій. Те загальне, що мають розглянуті вже операції, можна виділити у наступному визначенні.

Нехай M — множина. Бінарною алгебричною операцією (або законом композиції) на множині M будемо називати відображення

$$f: M \times M \longrightarrow M$$

декартова квадрата множини M у цю ж множину. Таким чином, кожній упорядкованій парі (a, b) елементів множини M ставиться у відповідність однозначно визначений елемент $f(a, b)$ тієї ж множини M . Елемент $f(a, b)$ називається композицією елементів a і b відносно даної операції.

Для запису композиції елементів a і b частіше всього виписують a та b у відповідному порядку, відділяючи їх спеціальним характеристичним знаком даної операції, наприклад, $a + b$. З позначень знаків бінарних алгебричних операцій, які використовуються найбільш часто, вкажемо «+» та «·». Закон, що позначається знаком «+», називається частіше всього додаванням, а відповідна композиція елементів $a + b$ називається їх сумою; у цьому випадку говорять також про адитивне позначення бінарної алгебричної операції. Закон, що позначається знаком «·», називається частіше всього множенням, а відповідна композиція елементів $a \cdot b$ називається їх добутком; у цьому випадку говорять також про мультиплікативне позначення бінарної алгебричної операції. В останньому випадку часто крапка опускається, тобто замість $a \cdot b$ пишуть просто ab . Слід

пам'ятати, що у більшості випадків ці позначення досить умовні. Розглянемо тепер деякі приклади бінарних алгебричних операцій.

- 1) Додавання на множинах цілих, раціональних та дійсних чисел.
- 2) Множення на множинах цілих, раціональних та дійсних чисел.
- 3) Нехай M — множина. $P(M)$ — множина всіх перетворень множини M , тоді композиція $f \odot g$ дає приклад бінарної алгебричної операції на множині $P(M)$.
- 4) Нехай M — множина, $B(M)$ — його булеан. Відображення $(X, Y) \longrightarrow X \cap Y$, $(X, Y) \longrightarrow X \cup Y$, $(X, Y) \longrightarrow X \setminus Y$, $(X, Y) \longrightarrow X \Delta Y$, $X, Y \subseteq M$, дають приклади бінарних алгебричних операцій на множині $B(M)$.
- 5) Додавання, множення та комутування на множині матриць $M_n(R)$.
- 6) Додавання та множення дійсних функцій (тобто перетворень множини R).
- 7) Відображення $(n, k) \longrightarrow n^k$, $n, k \in N$, дає приклад бінарної алгебричної операції на множині натуральних чисел.
- 8) Відображення $(n, k) \longrightarrow \text{НСД}(n, k)$, $(n, k) \longrightarrow \text{НСК}(n, k)$, $n, k \in Z$, дають приклади бінарних алгебричних операцій на множині цілих чисел (при цьому ми вважаємо, що $\text{НСД}(n, k)$, $\text{НСК}(n, k) \geq 0$).
- 9) Додавання та векторне множення у просторі R^3 .

Розглянемо деякі важливі властивості бінарних алгебричних операцій. При цьому будемо користуватись мультиплікативною формою запису операції і робити ілюстрації для адитивної форми запису.

Операція на множині M називається комутативною, якщо $ab = ba$ для кожної пари елементів $a, b \in M$.

Для адитивної форми запису це виглядає так: $a + b = b + a$.

Комутативними будуть операції додавання та множення на множинах цілих, раціональних та дійсних чисел; операції $\cap$, $\cup$ та Δ на булеані $B(M)$; додавання матриць; додавання та множення дійсних функцій; операції НСД, НСК на Z ; додавання векторів у просторі R^3 .

Якщо маємо три елементи $a, b, c \in M$, то з них можливо утворити наступні два добутки (якщо не змінювати порядок їх слідування): $a(bc)$ та $(ab)c$.

Операція на множині M називається асоціативною, якщо

$$(ab)c = a(bc)$$

для кожної трійки елементів $a, b, c \in M$.

У адитивному запису: $(a + b) + c = a + (b + c)$.

Для чотирьох елементів a, b, c, d добутків уже значно більше: $((ab)c)d$, $(ab)(cd)$, $(a(bc))d$, $a(b(cd))$, $a((bc)d)$. Інакше кажучи, кожному добутку елементів a, b, c, d відповідає деяке розташування дужок між ними. Якщо операція асоціативна, то отримуємо, наприклад, $((ab)c)d = (ab)(cd)$. І така рівність має місце і в більш загальному випадку, як показує наступна теорема.

9.1. Теорема. Якщо бінарна операція на множині M є асоціативною, то результат її послідовного застосування до кожного скінченного набору елементів множини M не залежить від розташування дужок між ними (порядок слідування елементів не змінюється!).

Доведення. Розглянемо довільний скінченний набір елементів $a_1, a_2, \dots, a_n$ множини M . Скористаємось індукцією за числом n . Якщо $n = 1, 2$, то доводити нічого, для $n = 3$ твердження випливає з закону асоціативності. Припустимо тепер, що $n > 3$ та твердження вже має місце для скінченних наборів, кількість елементів у яких менша ніж n . Покажемо, що кожний добуток елементів $a_1, a_2, \dots, a_n$ (у даному порядку слідування) співпадає з деяким фіксованим добутком. У цій якості виділимо так званий *лівономований добуток*:

$$(\dots (((a_1 a_2) a_3) a_4) \dots) a_{n-1}) a_n.$$

Тепер розглянемо довільний добуток елементів $a_1, a_2, \dots, a_n$ (у даному порядку слідування). При цьому будемо виписувати тільки зовнішні дужки, оскільки для добутків, що складаються з меншої ніж n кількості елементів, твердження теореми є вірним і тому внутрішнє конкретне розташування дужок не має значення.

Отже, розглянемо добуток $(a_1 \dots a_t)(a_{t+1} \dots a_n)$. Мають місце наступні два випадки: $t + 1 = n$ та $t + 1 < n$.

У першому випадку кожний добуток елементів $a_1, a_2, \dots, a_{n-1}$ (у даному порядку слідування) співпадає за індуктивною гіпотезою з їх лівономованим добутком, а тому, помножив справа на елемент a_n , отримуємо лівономований добуток елементів $a_1, a_2, \dots, a_n$ (у даному порядку слідування). Розглянемо тепер другий випадок. Застосовуючи закон асоціативності, будемо мати

$$\begin{aligned} (a_1 \dots a_t)(a_{t+1} \dots a_n) &= (a_1 \dots a_t)((a_{t+1} \dots a_{n-1}) a_n) = \\ &= ((a_1 \dots a_t)(a_{t+1} \dots a_{n-1})) a_n = (\dots (((a_1 a_2) a_3) a_4) \dots) a_{n-1}) a_n. \end{aligned}$$

З теореми 9.1 випливає, що кожне розташування дужок при знаходженні добутку елементів $a_1, a_2, \dots, a_n$ (у даному порядку слідування) приводить до одного й того ж результату. Тому далі взагалі не будемо писати ніяких дужок і записувати добуток елементів $a_1, a_2, \dots, a_n$ (у даному порядку слідування) просто як $a_1 a_2 \dots a_n$, зважаючи на ту обставину, що у кожній конкретній ситуації можливо розташувати дужки так, як це потрібно для даної конкретної ситуації.

Для скороченого запису добутку елементів $a_1, a_2, \dots, a_n$ (у даному порядку слідування) будемо використовувати також наступне позначення:

$$a_1, a_2, \dots, a_n = \prod_{1 \leq i \leq n} a_i.$$

У випадку, коли $a_1, a_2, \dots, a_n = a$, добуток $a_1 a_2 \dots a_n$ позначають через a^n і називають n -м степенем елемента a .

9.2. Наслідок. Якщо бінарна операція на множині M є асоціативною, то для кожного елемента $a \in M$ та довільних $n, m \in N$ мають місце рівності

$$a^n a^m = a^{n+m}, (a^n)^m = a^{nm}.$$

У випадку, коли використовується адитивний запис, для бінарної операції замість $\prod_{1 \leq i \leq n} a_i$ використовується уже звичний запис $\sum_{1 \leq i \leq n} a_i$, замість степеня елемента говорять про його кратне:

$$na = \underbrace{a + \dots + a}_n.$$

Твердження наслідку 9.1 для адитивного запису виглядає так:

$$na + ma = (n + m)a, m(na) = (mn)a.$$

Елементи a, b називаються переставними або комутуючими, якщо $ab = ba$.

Для переставних елементів має місце рівність $(ab)^n = a^n b^n$ при довільному $n \in N$. Дійсно,

$$(ab)^2 = abab = a(ba)b = a(ab)b = (aa)(bb) = a^2 b^2,$$

а далі індукцією за числом n :

$$\begin{aligned} (ab)^n &= (ab)^{n-1}(ab) = (a^{n-1}b^{n-1})ab = a^{n-1}(b^{n-1}a)b = a^{n-1}(b^{n-2}(ba))b = \\ &= a^{n-1}b^{n-2}(ab)b = a^{n-1}(b^{n-2}a)b^2 = \dots = a^{n-1}ab^{n-1} = a^n b^n. \end{aligned}$$

Використовуючи аналогічні аргументи, можна довести і більш загальне твердження.

9.3. Пропозиція. Нехай на множині M задана бінарна асоціативна операція. Якщо $a_1, a_2, \dots, a_n$ — такі елементи множини M , що $a_i a_j = a_j a_i$, $i, j, 1 \leq i, j \leq n$, то

$$(a_1 a_2 \dots a_n)^m = a_1^m a_2^m \dots a_n^m$$

для довільного $m \in N$.

У адитивному запису ця рівність виглядає так:

$$m(a_1 + a_2 + \dots + a_n) = ma_1 + ma_2 + \dots + ma_n.$$

Нехай на множині M задана бінарна операція. Елемент $z \in M$ називається центральним, якщо він переставний з кожним елементом множини M . Сукупність всіх центральних елементів називається центром M і буде позначатися через $\zeta(M)$.

Непуста множина S , на якій задана бінарна асоціативна операція, називається напівгрупою. Напівгрупа називається комутативною, якщо її операція ще й комутативна.

Наведемо зараз приклади напівгруп.

Множини цілих, раціональних та дійсних чисел відносно операції додавання утворюють комутативну напівгрупу.

Множини цілих, раціональних та дійсних чисел відносно операції множення утворюють комутативну напівгрупу.

Нехай M — множина. Множина $P(M)$ всіх перетворень множини M буде напівгрупою відносно композиції $f \circ g$ перетворень за теоремою 3.1. Як ми бачили раніше, ця напівгрупа не є комутативною.

Нехай M — множина. Булеан $B(M)$ цієї множини буде комутативною напівгрупою відносно операцій $(X, Y) \longrightarrow X \cap Y$, $(X, Y) \longrightarrow X \cup Y$, $(X, Y) \longrightarrow X \setminus Y$, $(X, Y) \longrightarrow XY$, $X, Y \subseteq M$, за теоремою 1.1.

Множина квадратних матриць $M_n(R)$ буде комутативною напівгрупою відносно операції додавання та напівгрупою відносно операції множення матриць за теоремою 5.1.

Множина всіх дійсних функцій (тобто перетворень множини R) буде комутативною напівгрупою відносно звичайних операцій додавання та множення дійсних функцій.

Множина всіх цілих чисел буде комутативною напівгрупою відносно операцій $(n, k) \longrightarrow \text{НСД}(n, k)$, $(n, k) \longrightarrow \text{НСК}(n, k)$, $n, k \in \mathbb{Z}$.

Векторний простір R^3 буде комутативною напівгрупою відносно операції додавання векторів.

Наведемо також ще один важливий приклад.

Нехай M — непуста множина, яку будемо називати *алфавітом*, а елементи цієї множини будемо називати *буквами*. Через F_M позначимо множину всіх скінченних наборів елементів множини M . Визначимо операцію на F_M за наступним правилом:

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_m) = (a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m).$$

Ця операція, яка називається ще конкатенацією, очевидно асоціативна. Таким чином, відносно цієї операції F_M стає напівгрупою. F_M називають *вільною напівгрупою над алфавітом M* . Ми можемо отождествити набір, що складається з одного елемента, з самим цим елементом, і отримати більш звичайний запис набору $(a_1, a_2, \dots, a_n)$ у вигляді добутку $a_1 a_2 \dots a_n$. У цьому більш звичному вигляді і записують елементи вільної напівгрупи F_M . Елемент $w = a_1 a_2 \dots a_n$ вільної напівгрупи F_M природно називати *словом*, а число n — *довжиною* цього слова. При цьому два слова $a_1 a_2 \dots a_n$ та $b_1 b_2 \dots b_m$ тоді і тільки тоді будуть рівними, коли $n = m$ та $a_t = b_t$ для кожного $1 \leq t \leq m$.

Нехай на множині M задана бінарна операція. Елемент $e \in M$ називається *нейтральним елементом відносно даної операції*, якщо

$$ae = ea = a$$

для кожного елемента a множини M .

Нейтральний елемент, якщо він існує, буде єдиним. Якщо операція на множині M записується мультиплікативно, то частіше використовується термін *єдиничний елемент*; якщо операція записується адитивно, то говорять про *нульовий елемент*, у цьому випадку будемо позначати його через 0_M , так що визначення нульового елемента виглядає наступним чином: $a + 0_M = 0_M + a = a$ для кожного елемента $a \in M$.

Відносно операції додавання на множинах цілих, раціональних та дійсних чисел нульовим елементом буде число 0.

Відносно операції множення на множинах цілих, раціональних та дійсних чисел одиничним елементом буде число 1.

Нехай M — множина. $P(M)$ — множина всіх перетворень множини M . Композиція $f \circ g$ має одиничний елемент, ним буде тотожна підстановка ϵ_M .

Нехай M — множина, $B(M)$ — його булеан. Операції $\cap$, $\cup$, Δ також мають нейтральні елементи. Для операції $\cap$ ним буде множина M , а два двох інших операцій нейтральним елементом буде пуста множина.

Відносно операції додавання на множині матриць $M_n(R)$ нульовим елементом буде нульова матриця O , відносно операції множення матриць одиничним елементом буде матриця E .

Відносно операції додавання дійсних функцій нульовим елементом буде функція, що дорівнює 0 для кожного значення аргументу; відносно операції множення дійсних функцій одиничним елементом буде функція, що дорівнює 1 для кожного значення аргументу.

Відносно операції $(n, k) \longrightarrow \text{НСД}(n, k)$ на множині цілих чисел нейтральним елементом буде число 1. Операція $(n, k) \longrightarrow \text{НСК}(n, k)$, $n, k \in \mathbb{Z}$, не має нейтрального елемента.

У просторі R^3 відносно операції додавання нульовим елементом буде нульовий вектор.

Напівгрупа, що має одиничний елемент, називається напівгрупою з одиницею.

Нехай на множині M задана бінарна операція. Підмножина S множини M називається сталою відносно операції, якщо для кожної пари елементів $a, b \in S$ їх композиція ab також належить до S .

Це означає, що звуження бінарної операції, заданої на множині M , на її підмножину S буде бінарною операцією на підмножині S . Наприклад, підмножина всіх парних чисел буде сталою підмножиною $\mathbb{Z}$ відносно операції додавання, в той час, як множина всіх непарних чисел не буде сталою відносно цієї операції.

9.4. Пропозиція. *Нехай на множині M задана бінарна операція. Якщо S — система сталих підмножин множини M , то перетин $\cap S$ підмножин цієї системи також буде підмножиною, сталою відносно даної операції.*

Це твердження очевидне.

Слід відзначити, що об'єднання сталих підмножин не буде сталою підмножиною. Наприклад, підмножина $2\mathbb{Z}$ всіх парних цілих чисел та підмножина $3\mathbb{Z}$ всіх цілих чисел кратних 3 будуть сталими відносно операції додавання, а їх об'єднання не містить числа $5 = 2 + 3$ і отже не буде сталою підмножиною.

Нехай C — довільна підмножина множини M , S — система сталих відносно операції підмножин, кожне з яких містить C . Тоді перетин $\cap S$ буде найменшою сталою підмножиною, яка містить у собі C . Ця підмножина називається сталою підмножиною, породженою підмножиною C .

Нехай на множині M задана бінарна операція, яка має одиничний елемент e . Елемент a множини M має обернений, якщо існує такий елемент x (він і називається оберненим до a), що $ax = xa = e$.

Якщо операція асоціативна, то обернений до a елемент буде єдиним. Дійсно, якщо y — елемент, що також має властивість $ay = ya = e$, то

$$y = ey = (xa)y = x(ay) = xe = x.$$

Тому далі єдиний обернений до a елемент будемо позначати через a^{-1} . З самого означення видно, що $(a^{-1})^{-1} = a$.

Якщо операція записується адитивно, то замість елемента, оберненого до a , будемо говорити про елемент, протилежний до a , цей елемент будемо позначати через $-a$; отже визначення протилежного елемента виглядає так:

$$a + (-a) = (-a) + a = 0_M.$$

9.5. Пропозиція. *Нехай на множині M задана бінарна асоціативна операція, яка має одиничний елемент e . Якщо елементи $a_1, a_2, \dots, a_n$ мають обернені у множині M , то їх добуток $a_1 a_2 \dots a_n$ також має обернений і*

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}.$$

Дійсно, маємо

$$\begin{aligned} (a_1 a_2 \dots a_n)(a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}) &= (a_1 a_2 \dots a_{n-1}) (a_n a_n^{-1})(a_{n-1}^{-1} \dots a_1^{-1}) = \\ &= (a_1 a_2 \dots a_{n-1})(a_{n-1}^{-1} \dots a_1^{-1}) = \dots = e. \end{aligned}$$

9.6. Наслідок. *Нехай P — напівгрупа з одиницею. Тоді підмножина $U(P)$ всіх тих елементів, що мають обернені, буде сталою.*

Наявність одиничного елемента та елемента, оберненого до a , дозволяє визначити всі цілі степені цього елемента. Покладемо

$$a^0 = e, \quad a^{-n} = (a^{-1})^n, \quad n \in \mathbb{N}.$$

У адитивному запису це виглядає так:

$$0a = 0_M, \quad (-n)a = n(-a).$$

9.7. Пропозиція. *Якщо бінарна операція на множині M є асоціативною, то для кожного елемента $a \in M$ та довільних $n, m \in \mathbb{Z}$ мають місце рівності*

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

Д о в е д е н н я . Якщо $n, m > 0$, то рівності вже доведені у наслідку 9.2. Якщо хоча б одне з цих чисел дорівнює нулю, то рівності тривіальні. Нехай $n, m < 0$, тоді

$$a^n a^m = (a^{-1})^{-n} (a^{-1})^{-m} = (a^{-1})^{-n+(-m)} = (a^{-1})^{-(n+m)} = a^{n+m},$$

$$(a^n)^m = ((a^n)^{-1})^{-m} = (((a^{-1})^{-n})^{-1})^{-m} = ((a^{-1})^n)^{-m} = \\ = ((a^{-n}))^{-m} = a^{(-n)(-m)} = a^{nm}.$$

Нехай тепер $n > 0$, $m < 0$, $n > -m$, тоді

$$a^n a^m = \underbrace{a \dots a}_n \underbrace{(a^{-1}) \dots (a^{-1})}_m = \underbrace{a \dots a}_{n - (-m)} = a^{n+m}.$$

Якщо $n < 0$, $m < 0$, $n < -m$, тоді

$$a^n a^m = \underbrace{a \dots a}_n \underbrace{(a^{-1}) \dots (a^{-1})}_{-m} = \underbrace{(a^{-1}) \dots (a^{-1})}_{(-m) - n} = (a^{-1})^{-(n+m)} = a^{n+m}.$$

Розглянемо тепер другу рівність. Нехай тепер $n > 0$, $m < 0$, тоді

$$(a^n)^m = ((a^n)^{-1})^{-m} = ((a^{-1})^n)^{-m} = ((a^{-1})^{n(-m)}) = (a^{-1})^{-nm} = a^{(-nm)} = a^{nm}.$$

Якщо $n < 0$, $m > 0$, то

$$(a^n)^m = (((a^{-1})^{-n})^m = (a^{-1})^{(-n)m} = (a^{-1})^{-nm} = a^{(-nm)} = a^{nm}.$$

Нехай M , S — множини, на яких задані бінарні алгебричні операції, що позначаються символами $\square$ та $\star$ відповідно, та нехай $f: M \longrightarrow S$ — відображення. Це відображення називають гомоморфізмом, якщо

$$f(x \square y) = f(x) \star f(y)$$

для довільних елементів $x, y \in M$.

Про відображення f говорять ще, що воно зберігає операції або узгоджено з операціями.

Ін'єктивний гомоморфізм називається мономорфізмом, сюр'єктивний гомоморфізм називається епіморфізмом, і бієктивний гомоморфізм називається ізоморфізмом.

Якщо $f: M \longrightarrow S$ — ізоморфізм, то з теореми 3.3 випливає існування оберненого відображення $f^{-1}: S \longrightarrow M$. Якщо u, v — довільні елементи множини S , то $u = f(x)$, $v = f(y)$ для деяких елементів $x, y \in M$. Тепер

$$f^{-1}(u \star v) = f^{-1}(f(x) \star f(y)) = f^{-1}(f(x \square y)) = x \square y = f^{-1}(u) \square f^{-1}(v).$$

Це означає, що відображення $f^{-1}: S \longrightarrow M$ також буде ізоморфізмом.

Множини M , S , на яких задані бінарні алгебричні операції, називаються ізоморфними, якщо існує ізоморфізм однієї з них на іншу; цей факт будемо позначати так $M \cong S$.

Якщо M — множина, на якій задано бінарну алгебричну операцію, то її вивчення має дві сторони. Перша відповідає на питання

які об'єкти є елементами множини M , а друга вивчає властивості операції на цих об'єктах.

Відповідно до цього і вивчення M можна проводити з різних точок зору. Можна вивчати зв'язки між індивідуальними властивостями елементів та їх підмножин і їх властивостями по відношенню до операції. Такий підхід є присутнім при вивченні конкретних множин, таких, наприклад, як груп підстановок, груп перетворень площини та простору, груп симетрій і т.і.

Однак можна вивчати і ті властивості, що цілком визначаються через властивості операцій. Цей підхід є характерним для загальної алгебри, він і приводить до важливого поняття ізоморфізму. Він виник досить давно, але входив у алгебру дуже повільно. Ще Р. Декарт говорив про суттєву спільність математичних дисциплін: "Хоча їх об'єкти різні, вони залишаються узгодженими між собою в тому, що розглядають в цих об'єктах тільки різні співвідношення або пропорції, які в них знаходяться".

Уточнюючи цю узгодженість, Г. Лейбніц вводить у розгляд загальне поняття ізоморфії (він називає це "подібність") і можливість ототожнювати ізоморфні співвідношення або операції. Він наводить приклад ізоморфізму, який став класичним. Це відображення $x \rightarrow \log x$ множини всіх додатних дійсних чисел з операцією множення на множину всіх дійсних чисел з операцією додавання.

Поняття ізоморфізму було знайомо Е. Галуа для груп підстановок. Але у загальному вигляді це поняття з'являється у теорії груп у середині XIX століття. Елементи множин M, S , що відповідають один одному при ізоморфізмі, мають однакові властивості відносно операцій. Загальна алгебра вивчає лише ті властивості, які зберігаються при ізоморфізмах.

10. ГРУПИ

У попередньому розділі ми вже привели всі поняття, необхідні для того, щоб дати одне з фундаментальних понять алгебри — поняття групи.

Напівгрупа з одиницею G , кожний елемент якої має обернений, називається групою. Інакше кажучи, група — це множина G , на якій задана бінарна алгебрична операція $(x, y) \mapsto xy$, $x, y \in G$, яка задовольняє наступним умовам (аксіомам групи):

(G 1) операція асоціативна, тобто $x(yz) = (xy)z$ для всіх елементів $x, y, z \in G$;

(G 2) G має одиничний елемент e , тобто елемент, що має властивість $xe = ex = x$ для кожного $x \in G$;

(G 3) кожен елемент $x \in G$ має обернений, тобто такий елемент x^{-1} , що $xx^{-1} = x^{-1}x = e$.

Якщо операція в групі комутативна, то група називається абелевою (на честь норвезького математика Абеля). Як правило, у абелевій групі використовується адитивний запис операції, так, що аксіоми абелевої групи виглядають наступним чином:

(AG 1) операція комутативна, тобто $x + y = y + x$ для всіх елементів $x, y \in G$;

(AG 2) операція асоціативна, тобто $x + (y + z) = (x + y) + z$ для всіх елементів $x, y, z \in G$;

(AG 3) G має нульовий елемент 0_G , тобто елемент, що має властивість $x + 0_G = x$ для кожного $x \in G$;

(AG 4) кожен елемент $x \in G$ має протилежний, тобто такий елемент $-x$, що $x + (-x) = 0_G$.

Самий термін “група” належить видатному французькому математику Еваристу Галуа. Серія досліджень, що приводить до поняття групи, це “теорія підстановок”, яка розвинулась з робіт Лагранжа, Вандермонда, Гаусса, Руффіні, Коші, присвячених знаходженню коренів алгебричних рівнянь. В цих дослідженнях були отримані перші результати теорії груп.

Але реальним засновником теорії груп вважається Галуа, який звів вивчення алгебричних рівнянь до вивчення пов'язаних із ними груп підстановок, він перший увів поняття нормальної підгрупи та зрозумів його важливість, він розглянув групи, що мають спеціальні властивості, йому належить ідея “лінійного представлення” груп, і цей факт показує, що він підійшов до поняття ізоморфізму.

Геніальні роботи Галуа довгий час залишались незрозумілими, розповсюдження його ідей проходило значно пізніше його трагічної загибелі у роботах Ж. Серре та “Трактати про підстановки” К. Жордана. Досягнення теорії Галуа стимулювали інтенсивне вивчення скінченних груп підстановок, і на першому етапі розвиток теорії груп проходив спочатку у рамках теорії скінченних груп підстановок. Визначення “абстрактних” груп було дано А. Келі у середині XIX століття.

Однак навіть дослідження скінченних абстрактних груп досить довгий час сприймалися як частина теорії підстановок. І лише наприкінці XIX століття почався усвідомлений розвиток автономної теорії груп. Під впливом геометрії, топології, теорії диференціальних рівнянь виникла необхідність вивчення нескінченних груп перетворень. Відомий німецький геометр Ф. Клейн зв'язує геометрії з відповідними групами перетворень.

Ідея групи та пов'язані з нею ідеї інваріантності й симетрії усвідомлювались досить довгий час. Усюди, де суттєву роль грає симетрія якогось об'єкта (алгебричного або диференціального рівняння, кристалічної решітки або геометричної фігури і т.і.), виникає група перетворень (рухів, замін змінних, підстановок, індексів), що зберігають цей об'єкт. Групи виступають тут як міра симетрії і використовуються для класифікації цих об'єктів.

Це пояснює, чому теорія груп має надзвичайний успіх у геометрії, аналізі, теоретичній фізиці.

Визначення групи можна ослабити.

10.1. Теорема. *Напівгрупа G тоді і тільки тоді буде групою, коли вона має праву одиницю, тобто такий елемент e_r , що $xe_r = x$ для кожного елемента $x \in G$, та коли для кожного елемента $x \in G$ існує правий обернений, тобто елемент x_r із властивістю $xx_r = e_r$.*

Д о в е д е н н я . Якщо G — група, то її одиничний елемент буде і правою одиницею, а елемент, обернений до x , буде і правим оберненим. Навпаки, нехай напівгрупа G задовольняє умовам даної теореми. Покажемо, що права одиниця буде одночасно і лівою одиницею. Маємо

$$e_r xx_r = e_r e_r = e_r = xx_r$$

Помножимо тепер обидві частини рівності $e_r xx_r = xx_r$ на правий обернений до x_r , і будемо мати $e_r xe_r = xe_r$, тобто $e_r x = x$. Отже e_r — ліва одиниця. Нехай u — довільна права одиниця, v — довільна ліва одиниця, тоді $v = vu = u$. Це означає, що e_r — єдина права, та ліва одиниця в G .

З рівності $xx_r = e_r$ отримуємо $x_r xx_r = x_r e_r = x_r$. Для елемента x_r існує правий обернений. Множимо обидві частини останньої рівності справа на цей елемент і отримуємо $x_r xe = xx_r = e$, тобто $x_r = x^{-1}$.

10.2. Теорема. *Напівгрупа G тоді і тільки тоді буде групою, коли для довільних елементів $a, b \in G$ рівняння $ax = b$ та $xa = b$ мають розв'язки.*

Д о в е д е н н я . Якщо G — група, то рівняння $ax = b$ має розв'язок $x = a^{-1}b$, а рівняння $xa = b$ має розв'язок $x = ba^{-1}$. Навпаки, нехай G — напівгрупа, в якій указані рівняння мають розв'язки. Зокрема, рівняння $ax = a$ має розв'язок, який позначимо через e . Нехай b — довільний елемент G , позначимо через c розв'язок рівняння $xa = b$. Маємо тоді

$$be = (ca)e = c(ae) = ca = b,$$

тобто e — права одиниця для G . Правим оберненим для довільного елемента $a \in G$ буде розв'язок рівняння $xa = e$, і ми можемо застосувати теорему 10.1.

Група G називається *скінченною*, якщо множина її елементів *скінченна*. Як і для множин, кількість елементів скінченної групи G будемо позначати через $|G|$ і називати порядком групи G . Група, що не є скінченною, називається *нескінченною*.

10.3. Теорема. *Скінченна напівгрупа G тоді і тільки тоді буде групою, коли для довільних елементів $a, b, c \in G$ із рівнянь $ab = ac$ та $ba = ca$ завжди випливає $b = c$.*

Д о в е д е н н я . Якщо G — група, то елемент a має обернений, тому з рівняння $ab = ac$ (відповідно $ba = ca$) випливає

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c$$

(відповідно $b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = ce = c$).

Навпаки, нехай $G = \{g_1, \dots, g_n\}$. З умов теореми випливає, що всі елементи $ag_1, \dots, ag_n$ будуть попарно різними. Це означає, що $G = \{ag_1, \dots, ag_n\}$, зокрема, $b \in \{ag_1, \dots, ag_n\}$. У свою чергу це означає, що рівняння $ax = b$ має розв'язок у групі G . Аналогічно доводиться, що і рівняння $xa = b$ має розв'язок у групі G . Тепер можна застосувати теорему 10.2.

Раніше, ніж розглянути приклади груп, розглянемо важливе поняття підгрупи, а потім розглянемо разом і приклади груп і приклади їх підгруп.

Нехай G — група. Стала підмножина H групи G називається її підгрупою, якщо H буде групою відносно звуження на H операції, заданої у G . Той факт, що H — підгрупа G будемо позначати так: $H \leq G$.

10.4. Теорема (критерій підгрупи). Непуста підмножина H групи G тоді і тільки тоді буде підгрупою, коли виконуються наступні умови:

(SG 1) якщо $x, y \in H$, то $xy \in H$;

(SG 2) якщо $x \in H$, то і $x^{-1} \in H$.

Доведення. Якщо H — підгрупа, то умова (SG 1) випливає з означення. Нехай e_H — одиничний елемент H , тоді для довільного елемента $x \in H$ будемо мати $xe_H = x$ (зокрема, можна покласти $x = e_H$). Елемент x має обернений у групі G , тому з останнього рівняння отримаємо

$$x^{-1}xe_H = x^{-1}x = e.$$

Таким чином $e \in H$. Оскільки одиничні елементи G та H співпадають, то елемент, обернений до x в H буде оберненим до x у G . Зокрема має місце й умова (SG 2).

Навпаки, нехай підмножина H задовольняє умови (SG 1), (SG 2). З умови (SG 1) отримуємо, що H — стала підмножина G . Зокрема звуження на H операції, заданої у G , буде бінарною операцією на H . Ця операція асоціативна, оскільки асоціативною є операція в усій групі G . Якщо $x \in H$, то згідно (SG 2) і $x^{-1} \in H$. За умовою (SG 1) $e = xx^{-1} \in H$, зокрема, e буде одиничним елементом і для H . Нарешті, остання аксіома групи випливає з умови (SG 2).

10.5. Наслідок. Непуста підмножина H групи G тоді і тільки тоді буде підгрупою, коли виконується наступна умова:

(SG 3) якщо $x, y \in H$, то $xy^{-1} \in H$.

Доведення. Покажемо, що умова (SG 3) рівносильна умовам (SG 1) та (SG 2). Очевидно (SG 3) випливає з обох умов (SG 1), (SG 2). Нехай має місце (SG 3). Якщо $x \in H$, то $e = xx^{-1} \in H$. Далі $x^{-1} = ex^{-1} \in H$, так що (SG 2) має місце.

Нарешті, нехай $y \in H$. Уже було доведено, що $y^{-1} \in H$, а тому $xy = x(y^{-1})^{-1} \in H$, отже i (SG 1) має місце.

Нехай G — абелева група з адитивною операцією. На G можна визначити операцію віднімання за наступним правилом: $x - y = x + (-y)$. Наслідок 10.5 для цього випадку виглядає так:

Непуста підмножина H адитивної абелевої групи G тоді і тільки тоді буде підгрупою, коли виконується наступна умова:
(SG 3) якщо $x, y \in H$, то $x - y \in H$.

10.6. Наслідок. *Нехай G — група, H — її підгрупа. Підмножина $K \subseteq H$ тоді і тільки тоді буде підгрупою групи G , коли вона є підгрупою H .*

10.7. Наслідок. *Нехай G — група, S — система підгруп групи G . Перетин $\cap S$ підгруп цієї системи також буде підгрупою G .*

Доведення. Нехай $S = \cap S$, $x, y \in S$. Нехай U — довільна підгрупа із системи S , тоді $xy^{-1} \in U$, і отже xy^{-1} належить перетину всіх таких підгруп, тобто S . Залишилось застосувати наслідок 10.5.

Нехай G — група, H — її підгрупа, M — її деяка підмножина. Покладемо

$$C_H(M) = \{x \in H \mid xg = gx \text{ для кожного } g \in M\}.$$

Підмножина $C_H(M)$ називається централізатором підмножини M у підгрупі H .

Якщо $M = \{a\}$, то замість $C_H(\{a\})$ будемо використовувати коротший запис $C_H(a)$. Слід відзначити, що $Z(G) = C_G(G)$.

10.8. Наслідок. *Нехай G — група, H — її підгрупа, M — підмножина. Централізатор $C_H(M)$ буде підгрупою групи G . Зокрема, центр $z(G)$ також буде підгрупою G .*

Доведення. Нехай $x, y \in C_H(M)$, $g \in M$. Застосовуючи асоціативний закон, отримуємо $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$, звідки $xy \in C_H(M)$. Далі, якщо обидві частини рівності $xg = gx$ помножити зліва на x^{-1} , то приходимо до рівності $x^{-1}xg = g = x^{-1}gx$. Знову множення обох частин цієї рівності на x^{-1} вже справа приводить до $gx^{-1} = x^{-1}g$, що доводить співвідношення $x^{-1} \in C_H(M)$. Залишилось застосувати теорему 10.4.

Слід відзначити, що об'єднання підгруп не буде підгрупою. Воно не завжди буде сталою підмножиною, як це можна було побачити у попередньому параграфі.

Нехай M — множина. Система L її підмножин називається локальною, якщо для кожної пари підмножин $H, K \in L$ існує така підмножина $L \in L$, що $H, K \subseteq L$.

Спеціальним типом локальних систем є лінійно впорядковані

системи підгруп. Система L підмножин множини M називається лінійно впорядкованою, якщо для кожної пари підмножин $H, K \in L$ має місце одне з включень $H \subseteq K$ або $K \subseteq H$.

10.9. Наслідок. Нехай G — група, L — локальна система підгруп групи G . Тоді об'єднання $\cup L$ підгруп цієї системи також буде підгрупою G .

Доведення. Нехай $V = \cup L$, $x, y \in V$. Існують такі підгрупи H, K з системи L , що $x \in H$, $y \in K$. Виберемо тепер підгрупу $L \in L$, яка містить у собі обидві підгрупи H, K . Таким чином, $x, y \in L$. Оскільки L — підгрупа, $xy^{-1} \in L$ за наслідком 10.5, і отже $xy^{-1} \in V$.

Залишилось знову застосувати наслідок 10.5.

10.10. Наслідок. Нехай G — група, L — лінійно впорядкована система підгруп групи G . Тоді об'єднання $\cup L$ підгруп цієї системи також буде підгрупою G .

10.11. Наслідок. Нехай G — група, $H_1 \leq H_2 \leq \dots \leq H_n \leq \dots$ — зростаюча система підгруп групи G . Тоді об'єднання $\cup_{n \in \mathbb{N}} H_n$ підгруп цієї системи також буде підгрупою G .

Нехай M — підмножина групи G , S — система всіх тих підгруп, які містять у собі M . Тоді перетин $\langle M \rangle = \cap S$ буде за наслідком 10.7 підгрупою групи G . Цей перетин називають підгрупою, породженою підмножиною M , а множина M називається системою породжуючих елементів для підгрупи $\langle M \rangle$. Зокрема, якщо $\langle M \rangle = G$, то будемо говорити, що M породжує всю групу G . Група G називається скінченно породженою, якщо вона породжується деякою своєю скінченною підмножиною.

Якщо H — підгрупа групи G , що містить у собі підмножину M , то H містить у собі і підгрупу $\langle M \rangle$, у цьому сенсі $\langle M \rangle$ — найменша з підгруп, які містять у собі підмножину M . Ясно, що якщо M — підгрупа групи G , то $\langle M \rangle = M$. Разом із цим ми маємо наступне корисне твердження.

10.12. Пропозиція. Нехай G — група, H — її підгрупа. Якщо $M \subseteq H$, то $\langle M \rangle \leq H$.

Нехай x — елемент групи G , H — довільна підгрупа, до якої належить елемент x . З теореми 10.4 за допомогою звичайної індукції отримаємо співвідношення $x^n, e = x^0, x^{-n} \in H$ для будь-якого $n \in \mathbb{N}$, тобто $\{x^n \mid n \in \mathbb{Z}\} \subseteq H$. З іншого боку, із пропозиції 9.7 отримуємо рівність $x^n x^{-m} = x^{n-m}$, яка показує, що $\{x^n \mid n \in \mathbb{Z}\}$ — підгрупа групи G (див. наслідок 10.5). Це означає, що $\{x^n \mid n \in \mathbb{Z}\} = \langle x \rangle$ — підгрупа, породжена підмножиною $\{x\}$, або підгрупа, породжена елементом x . Цю підгрупу будемо називати також циклічною. Елемент y з властивістю $\langle y \rangle = \langle x \rangle$ називається породжуючим елементом для підгрупи $\langle x \rangle$. Згодом ми побачимо, що циклічна підгрупа може мати більше одного породжуючого елемента. Група називається циклічною, якщо вона співпадає з однією зі своїх циклічних підгруп.

Розглянемо детальніше підгрупу $\langle x \rangle$. Можливі два випадки.

(I) $x^n \neq x^m$, якщо $n \neq m$.

У цьому випадку підгрупа $\langle x \rangle$ є нескінченною. Будемо говорити, що елемент x має нескінченний порядок.

(II) Існують такі цілі числа n, m , що $n \neq m$, але $x^n = x^m$. Одне з чисел n, m більше за інше. Нехай $n > m$. З рівності $x^n = x^m$ отримуємо $x^{n-m} = e$. Отже серед додатних степеней елемента x деякі дорівнюють одиничному елементу. Нехай t — найменше додатне число, для якого $x^t = e$. Довільне ціле число n поділимо на t (природно з остачею): $n = tq + r$, де $0 \leq r < t$. Маємо

$$x^n = x^{tq+r} = x^{tq}x^r = (x^t)^qx^r = x^r.$$

За допомогою попередніх аргументів можна довести, що всі елементи $e = x^0, x = x^1, x^2, \dots, x^{t-1}$ різні. Звідси випливає, що

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\} = \{x^0, x^1, x^2, \dots, x^{t-1}\}.$$

У цьому випадку будемо говорити, що елемент x має скінченний порядок. Порядком елемента x називається найменше ненульове натуральне число t , яке має властивість $x^t = e$. Позначення: $|x| = t$. Із самого означення випливає рівність $|x| = |\langle x \rangle|$. Слід підкреслити, що $|e| = 1$.

Група називається періодичною, якщо кожен її елемент має скінченний порядок.

Будемо говорити, що група не має скруту або вільна від скруту, якщо кожен її неединичний елемент має нескінченний порядок.

Група називається мішаною, якщо вона має як неединичні елементи скінченного порядку, так і неединичні елементи нескінченного порядку.

Розглянемо тепер більш детально питання про породжуючі елементи циклічних груп.

10.13. Теорема. Нехай $G = \langle g \rangle$ — циклічна група, $y \in G$.

(1) Якщо G — нескінченна група, то рівність $\langle y \rangle = G$ має місце тоді і тільки тоді, коли або $y = g$, або $y = g^{-1}$.

(2) Якщо група G скінченна та $|G| = t$, то рівність $\langle y \rangle = G$ має місце тоді і тільки тоді, коли $y = g^m$, де $\text{НСД}(m, t) = 1$.

Д о в е д е н н я . Нехай спочатку $G = \langle g \rangle$ — нескінченна циклічна група, y — її інший породжуючий елемент. Оскільки $y \in \langle g \rangle$, то $y = g^m$ для деякого $m \in \mathbb{Z}$. З іншого боку, $\langle y \rangle = G$, зокрема, $g \in \langle y \rangle$, а тому і $g = y^d$, де $d \in \mathbb{Z}$. Отже, маємо $g = y^d = (g^m)^d = g^{md}$. Множимо тепер обидві частини цієї рівності на елемент g^{-1} і отримаємо $g^{md-1} = e$. Оскільки $\langle g \rangle$ — нескінченна циклічна група, це означає, що $md - 1 = 0$, тобто $m, d \in \{1, -1\}$. Таким чином для елемента y маємо тільки дві можливості: $y = g$ або $y = g^{-1}$. Розглянемо тепер випадок, коли група G — скінченна. Знову маємо $g^{md-1} = e$, але в цьому

випадку це означає, що $md - 1 = kt$ для деякого $k \in \mathbb{Z}$. Звідси $md + kt = 1$, а отже, $\text{НСД}(m, t) = 1$. Навпаки, нехай $\text{НСД}(m, t) = 1$. Існують такі цілі числа d, k , що $md + tk = 1$. Тоді

$$g = g^1 = g^{md+tk} = g^{md}g^{tk} = (g^m)^d(g^t)^k = y^d e^k = y^d.$$

Зокрема, $g \in \langle y \rangle$, і за пропозицією 10.12 $\langle g \rangle \leq \langle y \rangle$. Та ж пропозиція 10.12 дає і протилежне включення $\langle y \rangle \leq \langle g \rangle$, отже $\langle y \rangle = \langle g \rangle$.

10.14. Теорема. Нехай $G = \langle g \rangle$ — циклічна група, H — її підгрупа. Тоді H також буде циклічною.

Доведення. Оскільки H — підгрупа, то $e \in H$. Якщо $H = \{e\}$, то $H = \langle e \rangle$, зокрема, H — циклічна. Припустимо тепер, що H містить неединичні елементи. Усі елементи групи G вичерпуються цілими степенями елемента g , тому існує таке ціле число m , що $1 \neq g^m \in H$. Якщо $m < 0$, то, за умовою (SG 2), також $(g^m)^{-1} = g^{-m} \in H$. Це означає, що підгрупа H обов'язково містить додатні неединичні степені елемента g . Нехай $\Xi = \{k > 0 \mid 1 \neq g^k \in H\}$. У множині Ξ вибираємо найменший елемент d . Зокрема, $g^d \in H$, і за пропозицією 10.12 $\langle g^d \rangle \leq H$. Якщо x — довільний елемент підгрупи H , то $x = g^n$ для деякого $n \in \mathbb{Z}$. Поділимо n на d (природно з остачею): $n = dq + r$, де $0 \leq r < d$. Звідси

$$x = g^n = g^{dq+r} = (g^d)^q(g^r) \quad \text{і} \quad g^r = x(g^d)^{-q}.$$

За умовою (SG 3) $g^r \in H$, а тому $r \in \Xi$. З вибору числа d випливає, що $r = 0$, отже $x = g^n = (g^d)^q$. Це означає, що $H \leq \langle g^d \rangle$. Ми вже довели, що протилежне включення також має місце, отже $H = \langle g^d \rangle$.

Узагальнимо тепер розглянуту ситуацію.

10.15. Теорема. Нехай G — група, M — її підмножина. Підгрупа $\langle M \rangle$ складається з елементів, що мають вигляд $x_1 x_2 \dots x_n$, де $x_j \in M$ або $x_j^{-1} \in M$, $1 \leq j \leq n$, і тільки з них.

Доведення. Нехай Y — множина всіх елементів, що мають вигляд $x_1 x_2 \dots x_n$, де $x_j \in M$ або $x_j^{-1} \in M$, $1 \leq j \leq n$. З теореми 10.4 випливає, що $Y \subseteq \langle M \rangle$. З іншого боку, із самого означення випливає включення $M \subseteq Y$. Покажемо, що Y задовольняє умову (SG 3), із наслідку 10.5 буде випливати тоді, що Y — підгрупа.

Отже, нехай $g_1, g_2 \in Y$, тоді $g_1 = x_1 x_2 \dots x_n$, $g_2 = x_{n+1} x_{n+2} \dots x_m$, де $x_j \in M$ або $x_j^{-1} \in M$, $1 \leq j \leq m$. Маємо

$$g_1(g_2)^{-1} = (x_1 x_2 \dots x_n)(x_{n+1} x_{n+2} \dots x_m)^{-1} = x_1 x_2 \dots x_n x_m^{-1} \dots x_{n+1}^{-1} \in Y.$$

Отже, Y — підгрупа, що містить у собі підмножину M . Це означає, що $\langle M \rangle \leq Y$. Оскільки і протилежне включення має місце, то $\langle M \rangle = Y$.

На закінчення розглянемо корисну конструкцію декартового (прямого) добутку скінченної множини груп. Нехай $G_1, \dots, G_n$ — групи, $D = G_1 \times \dots \times G_n$ — їх декартовий добуток як множин. На множині D визначимо операцію множення за правилом

$$(g_1, \dots, g_n)(x_1, \dots, x_n) = (g_1x_1, \dots, g_nx_n), \text{ де } g_j, x_j \in G_j, 1 \leq j \leq n.$$

Оскільки g_j, x_j — елементи однієї і тієї ж групи G_j , то їх добуток визначений у цій групі G_j , $1 \leq j \leq n$, так, що ми отримали дійсно операцію на D . Ця операція, асоціативна:

$$\begin{aligned} ((g_1, \dots, g_n)(x_1, \dots, x_n))(y_1, \dots, y_n) &= ((y_1y_1)y_1, \dots, (g_nx_n)y_n) = \\ &= (g_1(x_1y_1), \dots, g_n(x_ny_n)) = (g_1, \dots, g_n)((x_1, \dots, x_n)(y_1, \dots, y_n)). \end{aligned}$$

Якщо e_j — одиничний елемент групи G_j , $1 \leq j \leq n$, то набір $(e_1, \dots, e_n)$ буде, очевидно, одиничним елементом для D . Нарешті, також очевидно, що

$$(g_1, \dots, g_n)^{-1} = (g_1^{-1}, \dots, g_n^{-1}).$$

Таким чином, всі аксіоми групи для D виконані. Тому далі, коли мова зайде про декартовий добуток груп, ми будемо розуміти під цим тільки що побудовану групу. Ця група називається також прямим добутком груп $G_1, \dots, G_n$ (слід відзначити, що поняття прямого та декартового добутку груп у загальному випадку відрізняються один від одного, але для випадку скінченної множини груп вони співпадають). Якщо всі групи $G_1, \dots, G_n$ — абелеві, то і їх декартовий добуток буде абелевою групою:

$$\begin{aligned} (g_1, \dots, g_n)(x_1, \dots, x_n) &= (g_1x_1, \dots, g_nx_n) = (x_1g_1, \dots, x_ng_n) = \\ &= (x_1, \dots, x_n)(g_1, \dots, g_n). \end{aligned}$$

Якщо у кожній з груп $G_1, \dots, G_n$ операція записується адитивно, то адитивний запис використовується і для позначення групової операції у їх декартовому добутку:

$$(g_1, \dots, g_n) + (x_1, \dots, x_n) = (g_1 + x_1, \dots, g_n + x_n).$$

11. ПРИКЛАДИ ГРУП ТА ПІДГРУП

Числові групи. Множина R всіх дійсних чисел буде групою відносно операції додавання. Ця група буде вільною від скруту. Множина Q всіх раціональних чисел та множина Z всіх цілих чисел будуть її підгрупами. Група Z дає нам приклад нескінченної циклічної групи, вона породжується числом 1. Для кожного $n \geq 0$ підмножина $nZ = \{nk \mid k \in Z\}$ буде підгрупою Z . Дійсно, $nk - nt = n(k - t)$, тобто nZ

задовольняє умову (SG 3) і отже за наслідком 10.5 $n\mathbb{Z}$ буде підгрупою $\mathbb{Z}$. З теореми 10.13 випливає, що довільна підгрупа Z співпадає з однією з підмножин $n\mathbb{Z}$, $n \geq 0$, і інших підгруп Z не має.

Нехай p — просте число, $Q_p = \{m/(p^k) \mid m, k \in \mathbb{Z}\}$. Дріб, що має вигляд $m/(p^k)$, називається p -ічним. Очевидна рівність

$$m/(p^k) - r/(p^s) = (mp^s - rp^k)/(p^{k+s})$$

показує, що Q_p задовольняє умову (SG 3), отже за наслідком 10.5 Q_p буде підгрупою $\mathbb{Q}$. Її називають (адитивною) групою p -ічних дробів.

Множина $\mathbb{R} \setminus \{0\} = \mathbb{R}^\times$ усіх ненульових дійсних чисел буде групою відносно операції множення. Множини $\mathbb{Q} \setminus \{0\} = \mathbb{Q}^\times$ усіх ненульових раціональних чисел та множина $\{1, -1\}$ будуть її підгрупами, більш того, остання дає нам приклад скінченної циклічної групи. Відзначимо, що єдиними елементами групи $\mathbb{R}^\times$, які мають скінченний порядок, є 1 та -1 .

Булеан множини. Нехай A — довільна множина, $B(A)$ — булеан множини A . З теореми 1.1 випливає, що $B(A)$ буде групою відносно операції Δ (нагадаємо, що $C \Delta B = (C \setminus B) \cup (B \setminus C)$). Ця група буде абелевою, а з рівності $B \Delta Y = \emptyset$ отримуємо, що кожний елемент цієї групи має порядок 2.

Група інвертованих елементів напівгрупи. Багато важливих прикладів груп виникають у надрах напівгруп. Нехай S — напівгрупа з одиницею. Елемент $x \in S$ називається *інвертованим*, якщо він має в S обернений елемент. Множину всіх інвертованих елементів напівгрупи S позначимо через $U(S)$. З наслідку 9.6 випливає, що $U(S)$ — стала підмножина S . Інакше кажучи, звуження бінарної операції, що задана в S на $U(S)$ буде бінарною операцією на ній. Ця бінарна операція асоціативна, оскільки асоціативність має місце для всіх елементів із S . Єдиничний елемент належить до $U(S)$ за самим визначенням, і також за самим визначенням, кожний елемент із $U(S)$ має обернений, який також належить до $U(S)$. Таким чином, всі аксіоми (G1) — (G3) виконані для $U(S)$.

$U(S)$ ми будемо називати групою інвертованих елементів напівгрупи S .

У розділі 9 ми вже відзначали, що множина $P(A)$ усіх перетворень множини A буде напівгрупою з одиницею. Зокрема, оскільки $U(P(A)) = S(A)$, то множина $S(A)$ буде групою відносно операції множення функцій. Її називають *групою підстановок множини A* . Для групи S_n існує спеціальна назва: симетрична група степеня n . У розділі 8 ми відзначали, що $U(M_n(R)) = GL_n(R)$, зокрема множина $GL_n(R)$ всіх невідроджених квадратних матриць порядку n із дійсними коефіцієнтами буде групою відносно операції множення матриць. Її називають *загальною лінійною групою степеня n над R* . Підмножина $GL_n(\mathbb{Q})$ буде підгрупою в $GL_n(R)$. Дійсно, з визначення операції множення матриць випливає, що добуток двох матриць із раціональними коефіцієнтами має тільки раціональні коефіцієнти. Якщо $A \in GL_n(\mathbb{Q})$, то з теореми 8.2 випливає, що $A^{-1} \in GL_n(\mathbb{Q})$. Таким чином, $GL_n(\mathbb{Q})$ задовольняє умови (SG 1) — (SG 2), отже за теоремою 10.4 $GL_n(\mathbb{Q})$ буде підгрупою $GL_n(R)$.

Групи підстановок та перетворень. Нехай A — довільна множина. Ми вже відзначали, що множина $S(A)$ усіх підстановок A буде групою. Розглянемо зараз важливі приклади підгруп цієї групи.

Стабілізатор підмножини. Нехай B — підмножина A ,

$$\text{St}(B) = \{\pi \in S(A) \mid \pi(b) = b \text{ для кожного елемента } b \in B\}.$$

Якщо $\pi, \sigma \in \text{St}(B)$, то для кожного елемента $b \in B$ маємо

$$\pi \odot \sigma(b) = \pi(\sigma(b)) = \pi(b) = b,$$

тобто $\pi \odot \sigma \in \text{St}(B)$, а також

$$b = \varepsilon_A(b) = (\pi^{-1} \odot \pi)(b) = (\pi^{-1}(\pi(b))) = \pi^{-1}(b),$$

тобто і $\pi^{-1} \in \text{St}(B)$.

Таким чином, підмножина $\text{St}(B)$ задовольняє обидві умови (SG 1), (SG 2) і за теоремою 10.4 буде підгрупою $S(A)$. Зокрема, підгрупою буде $\text{St}(a)$ для кожного елемента $a \in A$. Відзначимо також очевидну рівність $\text{St}(B) = \bigcap_{b \in B} \text{St}(b)$.

Нехай тепер $\text{Inv}(B) = \{\pi \in S(A) \mid \pi(B) = B\}$. Якщо $\pi, \sigma \in \text{Inv}(B)$, $b \in B$, то $\sigma(b) = b_1 \in B$, так що маємо

$$\pi \odot \sigma(b) = \pi(\sigma(b)) = \pi(b_1) = b_2 \in B,$$

тобто $\pi \odot \sigma \in \text{Inv}(B)$. Оскільки $\pi(B) = B$, то існує такий елемент $b_3 \in B$, що $b = \pi(b_3)$, а тоді

$$b_3 = \varepsilon_A(b_3) = (\pi^{-1} \odot \pi)(b_3) = (\pi^{-1}(\pi(b_3))) = \pi^{-1}(b),$$

тобто і $\pi^{-1} \in \text{Inv}(B)$.

Таким чином, підмножина $\text{Inv}(B)$ задовольняє обидві умови (SG 1), (SG 2) і за теоремою 10.4 буде підгрупою $S(A)$. Слід відзначити, що $\text{St}(B) \leq \text{Inv}(B)$, в той час як $\text{Inv}(a) = \text{St}(a)$ для кожного елемента $a \in A$.

Фінітарні підстановки. Нехай $\pi \in S(A)$. Підмножина

$$\text{Supp } \pi = \{\pi \in A \mid \pi(a) \neq a\}$$

називається *носієм* підстановки π , а її доповнення $A \setminus \text{Supp } \pi$ — *множиною нерухомих точок* підстановки π . Підстановка π називається *фінітарною*, якщо її носій $\text{Supp } \pi$ є скінченним. Позначимо через $FS(A)$ підмножину всіх фінітарних підстановок множини A . Якщо $\pi, \sigma \in FS(A)$ і $b \in A \setminus (\text{Supp } \pi \cup \text{Supp } \sigma)$, то

$$\pi \odot \sigma(b) = \pi(\sigma(b)) = \pi(b) = b,$$

тобто $\text{Supp } (\pi \odot \sigma) \subseteq \text{Supp } \pi \cup \text{Supp } \sigma$, зокрема, $\text{Supp } (\pi \odot \sigma)$ скінченний, отже $\pi \odot \sigma \in FS(A)$. Далі, нехай $b \in A \setminus \text{Supp } \pi$, тоді

$$b = \varepsilon_A(b) = (\pi^{-1} \odot \pi)(b) = (\pi^{-1}(\pi(b))) = \pi^{-1}(b).$$

Це означає, що $\text{Supp } \pi^{-1} \subseteq \text{Supp } \pi$. Оскільки $\pi = (\pi^{-1})^{-1}$, то і $\text{Supp } \pi \subseteq \text{Supp } \pi^{-1}$, а тому $\text{Supp } \pi^{-1} = \text{Supp } \pi$. Зокрема, підмножина

Supp π^{-1} скінченна, отже і $\pi^{-1} \in FS(A)$. Таким чином, підмножина $FS(A)$ задовольняє обидві умови (SG 1), (SG 2) і за теоремою 10.4 буде підгрупою $S(A)$. $FS(A)$ називають *групою фінітарних підстановок* множини A .

Групи симетрій. Нехай $E = R^n$, через $d(x, y)$ будемо позначати відстань між точками x, y простору E . Відображення $f \in S(E)$ будемо називати *ізометрією* простору E , якщо f зберігає відстані між точками простору E , тобто $d(f(x), f(y)) = d(x, y)$ для кожної пари точок x, y простору E . Сукупність всіх ізометрій простору E позначимо через $\text{Isom}(E)$. Якщо $f, g \in \text{Isom}(E)$, $x, y \in E$, то

$$d(f \circ g(x), f \circ g(y)) = d(f(g(x)), f(g(y))) = d(g(x), g(y)) = d(x, y),$$

тобто $f \circ g \in \text{Isom}(E)$.

Далі

$$d(x, y) = d(f(f^{-1}(x)), f(f^{-1}(y))) = d(f^{-1}(x), f^{-1}(y)),$$

тобто і $f^{-1} \in \text{Isom}(E)$.

Таким чином, підмножина $\text{Isom}(E)$ задовольняє обидві умови (SG 1), (SG 2) і за теоремою 10.4 буде підгрупою $S(E)$.

Нехай тепер M — підмножина простору E , покладемо

$$\text{Sym}(M) = \text{Isom}(E) \cap \text{Inv}(B),$$

інакше кажучи, $\text{Sym}(M)$ складається з тих ізометрій простору E , які переводять підмножину M у себе. З наслідку 10.7 випливає, що $\text{Sym}(M)$ — підгрупа $\text{Isom}(E)$. Її називають *групою симетрій* підмножини M . Образно кажучи, група $\text{Sym}(M)$ вимірює ступінь симетричності фігури M . Наприклад, той факт, що рівнобедрений трикутник є більш симетричним, ніж нерівнобедрений, можна виміряти тим, що група симетрій нерівнобедреного трикутника (як підмножини простору R^2 — дійсної площини) складається лише з однієї тотожної підстановки, в той час як група симетрій рівнобедреного трикутника складається з тотожної підстановки та відбиття відносно осі симетрії рівнобедреного трикутника. Якщо ж розглянути групу симетрій рівностороннього трикутника, то вона складається уже із шести ізометрій: тотожної підстановки, поворотів на кути 120° та 240° навкруги центра трикутника та трьох відбиттів відносно трьох осей симетрій рівностороннього трикутника. У цьому сенсі рівносторонній трикутник буде більш симетричним, ніж рівнобедрений.

Симетрією молекули називається ізометрія простору, яка переводить кожен атом молекули у атом того ж типу і зберігає всі валентні зв'язки між атомами. Наприклад, молекула фосфору складається з чотирьох атомів, що розташовані у вершинах правильного тетраедра, і її група симетрій співпадає з групою симетрій правильного тетраедра.

Досить велику симетрію мають кристали, тому група симетрій кристала буде їх важливою характеристикою. Тут під симетрією кристала розуміється така ізометрія простору, яка зберігає розташування атомів кристала і всі зв'язки між ними, переміщуючи кожен атом в атом того ж самого елемента.

Також важливою фізичною характеристикою є симетрія фізичних законів. Під нею розуміють ті перетворення координат, при яких закон зберігається. Так, закони механіки повинні зберігатись при переході від однієї інерціальної системи координат до іншої. Відповідні перетворення координат мають у механіці Галілея—Ньютона наступний вигляд (для руху по прямій):

$$x' = x - vt, \quad t' = t,$$

а в механіці спеціального принципу відносності:

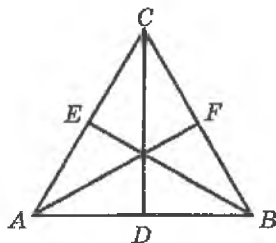
$$x' = \frac{x - vt}{\sqrt{1 - (v/c)^2}}, \quad t' = \frac{t - x(v/c)^2}{\sqrt{1 - (v/c)^2}},$$

де c — швидкість світла у пустоті. Група симетрій у першому випадку називається *групою Галілея—Ньютона*, а у другому випадку — *групою Лоренца*.

Групи симетрій скінченних об'єктів можна зв'язати з підгрупами групи підстановок скінченного степеня. Розглянемо це детальніше на наступних прикладах.

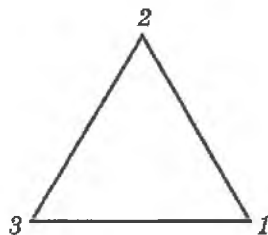
Нехай P_3 — правильний трикутник. Кожній вершині трикутника приписуємо деякий номер. Оскільки кожна симетрія переміщує вершини трикутника, то отримуємо деяку підстановку степеня 3.

Вершині A приписуємо номер 1, вершині B — номер 2, а вершині C — номер 3.



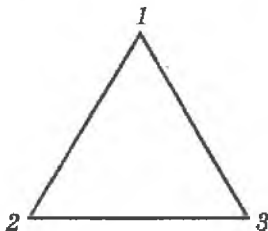
Тотожному перетворенню площини відповідає тотожна підстановка

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$



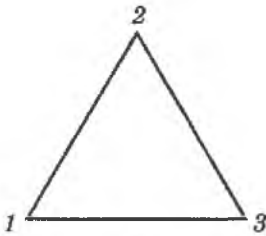
Повороту площини відносно центра трикутника на 120° відповідає підстановка

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$



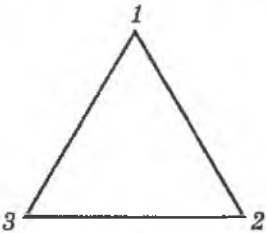
Повороту площини відносно центра трикутника на 240° відповідає підстановка

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$



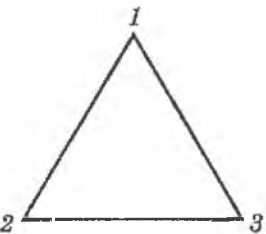
Відбиттю відносно осі AF трикутника відповідає підстановка

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$



Відбиттю відносно осі BE трикутника відповідає підстановка

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$



Відбиттю відносно осі CD трикутника відповідає підстановка

$$\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Таким чином, група симетрій правильного трикутника — це група S_3 .

Групу симетрій правильного чотирикутника не будемо розглядати так детально. Відзначимо, що вона складається з тотожної підстановки e , поворотів площини відносно центра чотирикутника на кути 90° , 180° , 270° , яким відповідають підстановки

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

з двох відбиттів відносно діагоналей чотирикутника, яким відповідають підстановки

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

з двох відбиттів відносно прямих, що проходять через середини протилежних сторін чотирикутника, яким відповідають підстановки

$$\pi_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \pi_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Запишемо тепер таблицю множення для групи $\text{Sym}(P_4)$ у вигляді матриці. У першому рядку і у першому стовпці запишемо всі

елементи групи, а на перетині рядка, що починається з елемента x , та стовпця, що починається з елемента y , будемо записувати елемент xy .

Таку таблицю називають ще *таблицею Келі групи*.

	ϵ	π_1	π_2	π_3	π_4	π_5	π_6	π_7
ϵ	ϵ	π_1	π_2	π_3	π_4	π_5	π_6	π_7
π_1	π_1	π_2	π_3	ϵ	π_7	π_6	π_4	π_5
π_2	π_2	π_3	ϵ	π_1	π_5	π_4	π_7	π_6
π_3	π_3	ϵ	π_1	π_2	π_6	π_7	π_5	π_4
π_4	π_4	π_6	π_5	π_7	ϵ	π_2	π_1	π_3
π_5	π_5	π_7	π_4	π_6	π_2	ϵ	π_3	π_1
π_6	π_6	π_5	π_7	π_4	π_3	π_1	ϵ	π_2
π_7	π_7	π_4	π_6	π_5	π_1	π_3	π_2	ϵ

Зробимо невеликий аналіз. Елемент $\sigma = \pi_1$ має порядок 4, а $\pi_2 = \sigma^2$, $\pi_3 = \sigma^3$. Покладемо також $\tau = \pi_4$, тоді $\tau^2 = \epsilon$ і з таблиці Келі можна побачити, що $\text{Sym}(P_4) = \langle \sigma, \tau \rangle$. Елементи σ, τ не переставні: $\tau\sigma = \sigma^3\tau$. Групу, яку ми зараз отримали, називають *групою діедра*.

Ми обмежились тут найбільш типовими прикладами груп симетрій. За більш детальною інформацією можна звернутися до книжок [1], [2].

Лінійні групи. Лінійними групами (точніше скінченно-вимірними лінійними групами) називають групу $GL_n(R)$ та її підгрупи. Зараз і розглянемо деякі важливі її підгрупи. Ми вже відзначали, що множина $GL_n(Q)$ всіх не вироджених квадратних матриць порядку n із раціональними коефіцієнтами буде підгрупою $GL_n(R)$. Покладемо

$$GL_n(Z) = \{A \in M_n(Z) \mid \det(A) \in \{1, -1\}\}.$$

З визначення операції множення матриць випливає, що добуток двох матриць із цілими коефіцієнтами має цілі коефіцієнти. Якщо $A \in GL_n(Z)$, то з теореми 8.2 випливає, що $A^{-1} \in GL_n(Z)$. Таким чином, $GL_n(Z)$ задовольняє умови (SG 1)—(SG 2), отже за теоремою 10.4 $GL_n(Z)$ буде підгрупою $GL_n(R)$.

Покладемо тепер

$$SL_n(R) = \{A \in M_n(R) \mid \det(A) = 1\}.$$

Нехай $A, B \in SL_n(R)$, згідно з теоремою 8.1 $\det(AB) = \det(A)\det(B) = 1$, що означає включення $AB \in SL_n(R)$. Далі з тієї ж теореми отримуємо також, що

$$1 = \det(E) = \det(AA^{-1}) = \det(A)\det(A^{-1}),$$

а тому і $\det(A^{-1}) = 1$, тобто $A^{-1} \in SL_n(R)$. Таким чином, $SL_n(R)$ задовольняє умови (SG 1)—(SG 2), отже за теоремою 10.4 $SL_n(R)$ буде

підгрупою $GL_n(R)$. Її називають *спеціальною лінійною групою степеня n над R* . Аналогічно визначаються підгрупи $SL_n(Q)$ та $SL_n(Z)$.

Позначимо тепер через $T_n(R)$ множину всіх невинероджених трикутних (точніше верхньо-трикутних) матриць порядку n із дійсними коефіцієнтами. Нехай знову $A, B \in T_n(R)$, $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, $C = AB = \|c_{ij}\|_{1 \leq i, j \leq n}$, та нехай $i > j$. Оскільки A та B — трикутні матриці, $a_{ij} = b_{ij} = 0$. Маємо тепер

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{i,i-1}b_{i-1,j} + a_{ii}b_{ij} + a_{i,i+1}b_{i+1,j} + \dots + a_{in}b_{nj}.$$

Оскільки

$$a_{i1} = a_{i2} = \dots = a_{i,i-1} = 0 \quad \text{і} \quad b_{ij} = b_{i+1,j} = \dots = b_{nj} = 0,$$

то також $c_{ij} = 0$. Це означає, що $AB \in T_n(R)$.

Слід відзначити також рівність

$$c_{ij} = a_{i1}b_{1i} + a_{i2}b_{2i} + \dots + a_{i,i-1}b_{i-1,i} + \\ + a_{ii}b_{ii} + a_{i,i+1}b_{i+1,i} + \dots + a_{in}b_{ni} = a_{ii}b_{ii}.$$

Розглянемо тепер матрицю A^{-1} . Позначимо її коефіцієнти через x_{ij} , $1 \leq i, j \leq n$. Теорема 8.2 дає нам коефіцієнти $x_{ij} = A_{ji} / \det(A)$, $1 \leq i, j \leq n$. У свою чергу, $A_{ji} = (-1)^{j+i} \det(S_{ji})$, де $S_{ji} = \|y_{km}\|_{1 \leq k, m \leq n-1}$ — підматриця матриці A , отримана викресленням із неї j -го рядка та i -го стовпця. Нехай $i > j$, розглянемо довільний k -й стовпець матриці S_{ji} . Якщо $k < j$, то k -й стовпець матриці S_{ji} складається з елементів

$$y_{1k} = a_{1k}, \dots, y_{k-1,k} = a_{k-1,k}, y_{kk} = a_{kk}, y_{kk} = 0, y_{k+1,k} = 0, \dots, y_{n-1,k} = 0.$$

Якщо $j = k$, то k -й стовпець матриці складається з елементів

$$y_{1k} = a_{1k}, \dots, y_{k-1,k} = a_{k-1,k}, y_{kk} = 0, y_{k+1,k} = 0, \dots, y_{nk} = 0.$$

Якщо $i > k > j$, то k -й стовпець матриці складається з елементів

$$y_{1k} = a_{1k}, \dots, y_{j-1,k} = a_{j-1,k}, y_{jk} = a_{j+1,k}, \dots, y_{k-1,k} = a_{kk}, y_{kk} = 0, \dots, y_{n-1,k} = 0.$$

Якщо $k \geq i$, то k -й стовпець матриці складається з елементів

$$y_{1k} = a_{1,k+1}, \dots, y_{j-1,k} = a_{j-1,k+1}, y_{jk} = a_{j+1,k+1}, \dots, y_{k-1,k} = a_{kk+1}, \\ y_{kk} = a_{k+1,k+1}, y_{k+1,k} = 0, \dots, y_{n-1,k} = 0.$$

Звідси видно, що матриця S_{ji} трикутна. Якщо $j < n-1$, $y_{jj} = 0$, а тому з пропозиції 6.10 отримуємо, що $A_{ji} = (-1)^{j+i} \det(S_{ji}) = 0$. Якщо $j = n-1$, то $i = n$; у цьому випадку всі елементи останнього рядка матриці дорівнюють нулю і наслідок 6.5 показує, що $A_{ji} = (-1)^{j+i} \det(S_{ji}) = 0$. Таким чином, якщо $i > j$, то $x_{ij} = A_{ji} / \det(A) = 0$. Це означає, що $A^{-1} \in T_n(R)$. Таким чином, $T_n(R)$ задовольняє умови (SG 1)—(SG 2), отже за теоремою 10.4 вона буде підгрупою $GL_n(R)$. Покладемо $T_n(Q) = GL_n(Q) \cap T_n(R)$ та $T_n(Z) = GL_n(Z) \cap T_n(R)$.

Позначимо через $UT_n(R)$ множину всіх унітрикутних матриць порядку n із дійсними коефіцієнтами. Якщо $A, B \in UT_n(R)$, $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, $C = AB = \|c_{ij}\|_{1 \leq i, j \leq n}$, то, як ми тільки що довели, C — трикутна матриця. Ми також довели рівність $c_{ii} = a_{ii}b_{ii}$, із якої випливає, що $c_{ii} = 1$ для кожного i , $1 \leq i \leq n$. З цієї рівності також отримуємо, що матриця, обернена до унітрикутної, сама буде унітрикутною.

Таким чином, $UT_n(R)$ задовольняє умови (SG 1)—(SG 2), отже за теоремою 10.4 вона буде підгрупою $GL_n(R)$. Покладемо $UT_n(Q) = GL_n(Q) \cap UT_n(R)$ та $UT_n(Z) = GL_n(Z) \cap UT_n(R)$.

Позначимо через $D_n(R)$ множину всіх невинуватених діагональних матриць порядку n із дійсними коефіцієнтами. Якщо $A, B \in D_n(R)$, $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$, $C = AB = \|c_{ij}\|_{1 \leq i, j \leq n}$, то, застосовуючи попередні аргументи, неважко довести, що C — діагональна матриця. Більш того $c_{ii} = a_{ii}b_{ii}$ для кожного i , $1 \leq i \leq n$. Зокрема, $AB = BA$. З цієї рівності також отримуємо, що матриця, обернена до діагональної, сама буде діагональною.

Таким чином, $D_n(R)$ задовольняє умови (SG 1)—(SG 2), отже за теоремою 10.4 вона буде абелевою підгрупою $GL_n(R)$. Покладемо $D_n(Q) = GL_n(Q) \cap D_n(R)$ та $D_n(Z) = GL_n(Z) \cap D_n(R)$. Зокрема, якщо $A \in D_n(Z)$, то $a_{ii} \in \{1, -1\}$ для кожного i , $1 \leq i \leq n$. Звідси випливає, що $D_n(Z)$ — скінченна абелева група і $|D_n(Z)| = 2^n$.

Матрицю $A \in M_n(R)$ називається *ортогональною*, якщо $AA^t = E$, тобто $A^{-1} = A^t$. Беручи до уваги пропозицію 6.2 та теорему 8.1, з рівності $AA^t = E$ отримуємо

$$1 = \det(E) = \det(AA^t) = \det(A)\det(A^t) = (\det(A))^2,$$

зокрема, ортогональна матриця завжди не вироджена.

Позначимо через $O_n(R)$ підмножину $M_n(R)$, що складається з усіх ортогональних матриць. Нехай $A, B \in O_n(R)$, тоді, за теоремою 5.2

$$(AB)^t = B^t A^t = B^{-1} A^{-1} = (AB)^{-1}, \text{ та } (A^{-1})^t = (A^t)^t = A = (A^{-1})^{-1}.$$

Інакше кажучи, $AB \in O_n(R)$, $A^{-1} \in O_n(R)$, а це, враховуючи теорему 10.4, означає, що $O_n(R)$ — підгрупа $GL_n(R)$.

12. ВІДНОШЕННЯ ЕКВІВАЛЕНТНОСТІ НА МНОЖИНАХ. РОЗКЛАД ГРУПИ В ОБ'ЄДНАННЯ СУМІЖНИХ КЛАСІВ

Ми вже відзначали раніше, що поняття відповідності й її часткового випадку — поняття відношення є одним з самих загальних понять математики. Конкретні важливі типи відношень визначаються тими чи іншими властивостями. Розглянемо зараз одне з важливих відношень — відношення еквівалентності.

Нагадаємо, що *бінарне відношення на множині A* — це підмножина Φ декартового добутку $A \times A$. Якщо $\alpha = (x, y) \in \Phi$, то будемо

говорити, що елементи x, y (у вказаному порядку) відповідають один одному при Φ . Замість запису $(x, y) \in \Phi$ будемо використовувати також і інший запис $x\Phi y$.

Бінарні відношення таким чином є множинами, а тому їх вивчення це є по суті вивчення підмножин декартового добутку $A \times A$. Зокрема можна говорити про включення одного бінарного відношення у інше, про об'єднання чи перетин бінарних відношень і т.і.

Випишемо зараз найбільш важливі властивості бінарних відношень.

Рефлексивність. Бінарне відношення Φ називається рефлексивним, якщо для кожного елемента $a \in A$ має місце $(a, a) \in \Phi$ (або має місце $a\Phi a$ для кожного $a \in A$).

Транзитивність. Бінарне відношення Φ називається транзитивним, якщо з включень $(a, b), (b, c) \in \Phi$ завжди випливає $(a, c) \in \Phi$, $a, b, c \in A$ (або з $a\Phi b$ та $b\Phi c$ випливає $a\Phi c$).

Симетричність. Бінарне відношення Φ називається симетричним, якщо з включення $(a, b) \in \Phi$ завжди випливає $(b, a) \in \Phi$, $a, b \in A$ (або з $a\Phi b$ випливає $b\Phi a$).

Антисиметричність. Бінарне відношення Φ називається антисиметричним, якщо з включень $(a, b), (b, a) \in \Phi$ завжди випливає $a = b$, $a, b \in A$ (або з $a\Phi b$ та $b\Phi a$ випливає $a = b$).

Відношення еквівалентності виникають із різних розбиттів множини A .

Система S підмножин множини A називається покриттям A , якщо $A = \cup S$. Покриття S називається розбиттями множини A , якщо кожні дві різні підмножини із системи S мають пустий перетин.

Нехай S — розбиття множини A . Розглянемо бінарне відношення $\Xi(S)$ на множині A , що задається за наступним правилом:

$(x, y) \in \Xi(S)$ тоді і тільки тоді, коли елементи x та y належать до однієї множини S з системи S .

Укажемо зараз властивості відношення $\Xi(S)$.

Оскільки $A = \cup S$, то для кожного елемента $x \in A$ існує підмножина $S \in S$, до якої належить елемент x . Зокрема, $(x, x) \in \Xi(S)$. Це означає, що відношення $\Xi(S)$ рефлексивне.

Відношення $\Xi(S)$ симетричне, це очевидно.

Нарешті, нехай $(x, y), (y, z) \in \Xi(S)$. Це означає, що існують такі підмножини $S, R \in S$, що $x, y \in R$ та $y, z \in S$. Зокрема, $y \in S \cap R$, і з означення розбиття отримуємо рівність $S = R$. Таким чином, елементи x, z належать до підмножини S , яка є елементом розбиття S . Інакше кажучи, відношення $\Xi(S)$ є транзитивним.

Бінарне відношення Ξ на множині A називається відношенням еквівалентності або просто еквівалентністю, якщо воно рефлексивне, симетричне, транзитивне.

Нехай Ξ — відношення еквівалентності на множині A , $x \in A$. Підмножину $[x]_{\Xi} = \{y \in A \mid (x, y) \in \Xi\}$ будемо називати класом еквівалентності елемента x .

Слід зразу відзначити, що клас еквівалентності визначається кожним своїм елементом. Дійсно, нехай $y \in [x]_{\Xi}$. Якщо $z \in [y]_{\Xi}$, то $(y, z) \in \Xi$. Разом із $(x, y) \in \Xi$ це дає, враховуючи транзитивність Ξ співвідношення $(x, z) \in \Xi$, тобто $z \in [x]_{\Xi}$. Інакше кажучи, $[y]_{\Xi} \subseteq [x]_{\Xi}$. Повторюючи ті ж самі аргументи, можна довести, що і $[x]_{\Xi} \subseteq [y]_{\Xi}$, тобто $[y]_{\Xi} = [x]_{\Xi}$.

Оскільки $(x, x) \in \Xi$, то $x \in [x]_{\Xi}$. Звідси випливає, що сукупність всіх класів еквівалентності утворює покриття множини A . Розглянемо перетин двох класів еквівалентності $[x]_{\Xi}$ та $[y]_{\Xi}$ і припустимо, що цей перетин непустий. Нехай $z \in [x]_{\Xi} \cap [y]_{\Xi}$. Тоді, як ми вже відзначали вище, $[z]_{\Xi} = [x]_{\Xi}$ та $[z]_{\Xi} = [y]_{\Xi}$, тобто $[y]_{\Xi} = [x]_{\Xi}$. Звідси випливає, що різні класи еквівалентності мають пустий перетин, а тому система всіх класів еквівалентності утворює розбиття $P(\Xi)$ множини A .

12.1. Теорема. Нехай A — множина.

Відображення $\rho: \Xi \rightarrow P(\Xi)$ буде бієкцією множини всіх відношень еквівалентності, заданих на A , на множину всіх розбиттів множини A .

Д о в е д е н н я . Нехай Ξ, Θ — два різних відношення еквівалентності на множині A . Тоді існує пара (x, y) , $x, y \in A$, яка належить до одного з цих відношень і не належить до іншого. Нехай для визначеності $(x, y) \in \Xi \setminus \Theta$. Оскільки $(x, y) \in \Xi$, то $y \in [x]_{\Xi}$, і оскільки $(x, y) \notin \Theta$, то $y \notin [x]_{\Theta}$.

Припустимо, що $P(\Xi) = P(\Theta)$, тоді знайдеться такий елемент $z \in A$, що $[z]_{\Theta} = [x]_{\Xi}$. Зокрема, $x \in [z]_{\Theta}$. Ми вже відзначали, що клас еквівалентності визначається кожним своїм елементом, тобто $[z]_{\Theta} = [x]_{\Theta}$. Отже $[x]_{\Theta} = [x]_{\Xi}$, і ми отримали протиріччя, оскільки $y \notin [x]_{\Theta}$. Це протиріччя показує, що $P(\Xi) \neq P(\Theta)$, тобто відображення ρ ін'єктивне.

Нехай S — довільне розбиття множини A . За цим розбиттям вище ми побудували відношення $\Xi(S)$, яке є відношенням еквівалентності. Якщо x — довільний елемент множини A , то $x \in S$ для деякої підмножини $S \in S$. З визначення відношення $\Xi(S)$ випливає, що кожен елемент підмножини S належить до класу еквівалентності елемента x .

Навпаки, нехай y — такий елемент A , що $(x, y) \in \Xi(S)$. Це означає, що існує така підмножина $Q \in S$, що $x, y \in Q$. У цьому випадку $x \in S \cap Q$, і з означення розбиття отримуємо рівність $Q = S$. Зокрема, $y \in S$. Отже клас еквівалентності елемента x відносно $\Xi(S)$ збігається з елементом розбиття S . Звідси й отримуємо рівність $P(\Xi) = S$. Інакше кажучи, відображення ρ буде також і сюр'єктивним, а тому і бієктивним.

Наведемо тепер приклади відношень еквівалентності. Поза математикою відношення еквівалентності виникають всякий раз, коли потрібно проводити класифікацію об'єктів тієї чи іншої природи. Так, наприклад, множину всіх людей можна розбити на нації, держави і т.і.; множину всіх тварин на види і т.д.

Якщо A — довільна множина, то можна розглянути два крайніх випадки: $\Xi = A \times A$ та $\Xi = \{(x, x) \mid x \in A\}$ (діагональ декартового добу-

ку $A \times A$). Усі інші відношення еквівалентності розташовані між цими двома крайніми позиціями.

В геометрії прикладом відношення еквівалентності є відношення паралельності, що визначене на множині всіх прямих площини або простору або на множині всіх площин простору.

Інший приклад: на множині $P = \{(x, y) \mid x > 0, y > 0\}$ розглянемо множину всіх гіпербол $G_a = \{(x, y) \mid xy = a\}$. Очевидно, що система $\{G_a \mid a > 0\}$ дає розбиття множини P , так, що дійсно приходимо до відношення еквівалентності.

Нехай M — множина всіх фундаментальних послідовностей $s = (x_n)_{n \in \mathbb{N}}$, що складаються з раціональних чисел. Розглянемо відношення ζ на множині M , яке визначається за таким правилом: $(s, r) \in \zeta$ тоді і тільки тоді, коли

$$\lim_{n \rightarrow \infty} (x_n - y_n) = 0,$$

тут $r = (y_n)_{n \in \mathbb{N}}$. Неважко упевнитись у тому, що ζ — відношення еквівалентності.

Нехай $M = [0, 1]$, визначимо відношення R за таким правилом: $(x, y) \in R$ тоді і тільки тоді, коли $x - y$ — раціональне число. Легко бачити, що R також буде відношенням еквівалентності.

Наведемо ще один важливий арифметичний приклад.

Два цілих числа a, b називаються конгруентними за модулем m , якщо $a - b$ ділиться на m ; цей факт ми будемо позначати так: $a \equiv b \pmod{m}$.

Неважко упевнитись в тому, що відношення конгруентності буде відношенням еквівалентності. Пізніше ми більш детально розглянемо властивості відношення конгруентності.

Цей приклад має таке важливе узагальнення.

Нехай G — група, H — її підгрупа. Визначимо відношення Σ_H за наступним правилом. Для елементів $x, y \in G$ включення $(x, y) \in \Sigma_H$ має місце тоді і тільки тоді, коли $xy^{-1} \in H$.

Відношення Σ_H рефлексивне: $xx^{-1} = e \in H$, тобто $(x, x) \in \Sigma_H$.

Відношення Σ_H симетричне: якщо $xy^{-1} \in H$, то оскільки H — підгрупа, вона містить також і елемент $(xy^{-1})^{-1} = (y^{-1})^{-1}x^{-1} = yx^{-1}$, тобто $(y, x) \in \Sigma_H$.

Відношення Σ_H транзитивне: якщо $xy^{-1}, yz^{-1} \in H$, то оскільки H — підгрупа, вона містить також і добуток цих елементів: $(xy^{-1})(yz^{-1}) = xz^{-1}$, тобто $(x, z) \in \Sigma_H$.

Таким чином, Σ_H — відношення еквівалентності.

З'ясуємо тепер, з яких елементів складається клас еквівалентності елемента x за відношенням Σ_H . Нехай $(x, y) \in \Sigma_H$, тоді $xy^{-1} = h \in H$. Множимо обидві частини рівності $xy^{-1} = h$ спочатку справа на y , а потім зліва на h^{-1} , отримаємо $y = h^{-1}x$.

Покладемо тепер

$$Hx = \{ux \mid u \in H\}.$$

Підмножина Hx називається правим суміжним класом (елемента x) групи G за підгрупою H .

Таким чином, кожний елемент, еквівалентний x (відносно Σ_H), належить до Hx . Навпаки, якщо $z \in Hx$, то $z = ux$ для деякого елемента $u \in H$. Маємо тепер $xz^{-1} = x(ux)^{-1} = xx^{-1}u^{-1} = u^{-1} \in H$, а це означає, що $(x, z) \in \Sigma_H$. Отже, класи еквівалентності за відношенням Σ_H — це праві суміжні класи за підгрупою H і тільки вони. Звідси випливає, що правий суміжний клас Hx визначається кожним своїм елементом (представником цього суміжного класу): якщо $y \in Hx$, то $Hu = Hx$; два правих суміжних класи або співпадають або мають пустий перетин, і група буде об'єднанням всіх правих суміжних класів. Інакше кажучи, система всіх правих суміжних класів за підгрупою H буде розбиттям групи. Якщо $H = \langle e \rangle$, то $xH = \{x\}$ для кожного елемента $x \in G$ так, що отримуємо найбільше розбиття групи G , яке складається з усіх одноелементних підмножин; якщо ж $H = G$, то отримуємо найменше розбиття, що складається з однієї множини — самої групи G .

Аналогічно, нехай тепер

$$xH = \{xu \mid u \in H\}.$$

Підмножина xH називається лівим суміжним класом (елемента x) групи G за підгрупою H .

Ліві суміжні класи — це точно класи еквівалентності за відношенням Λ_H , що визначається за наступним правилом:

Для елементів $x, y \in G$ включення $(x, y) \in \Lambda_H$ має місце тоді і тільки тоді, коли $y^{-1}x \in H$.

Тому кожний лівий суміжний клас xH визначається кожним своїм елементом: якщо $y \in xH$, то $yH = xH$; два лівих суміжних класи або співпадають або мають пустий перетин, і група буде об'єднанням всіх лівих суміжних класів. Інакше кажучи, система всіх лівих суміжних класів за підгрупою H також буде розбиттям групи.

Відзначимо, що з такими розбиттями в групах ми вже зустрічались. У теоремі 4.2 ми розглядали у групі S_n підмножини $P_i = \{\pi \in S_n \mid \pi(n) = i\}$ і показали, що $P_i \cap P_j = \emptyset$, якщо $i \neq j$ та

$$S_n = \bigcup_{1 \leq i \leq n} P_i = P_1 \cup P_2 \cup \dots \cup P_n.$$

Оскільки $P_n = \text{St}(n)$, то P_n — підгрупа S_n . Також ми показали фактично, що $P_i = \tau_{i,n} \odot P_n$.

Між розбиттями на ліві та праві суміжні класи існує такий зв'язок.

12.2. Пропозиція. Нехай G — група, H — її підгрупа. Відображення $v: Hx \rightarrow x^{-1}H$ буде бієкцією множини всіх правих суміжних класів за підгрупою H на множину всіх лівих суміжних класів за підгрупою H .

Доведення. Спочатку слід показати, що v — дійсно відображення, тобто, що воно не залежить від вибору представника суміжного класу. Нехай y — інший представник суміжного класу Hx , тоді $y = ux$ для деякого елемента $u \in H$.

За пропозицією 9.5 $y^{-1} = x^{-1}u^{-1}$, а тому $y^{-1} \in x^{-1}H$, отже $y^{-1}H = x^{-1}H$. Далі, відображення n — ін'єктивне: припустимо, що $x^{-1}H = v(Hx) = v(Hy) = y^{-1}H$. Тоді $y^{-1} = x^{-1}v$ для деякого елемента $v \in H$, а тому $y = v^{-1}x \in Hx$. Це означає, що $Hx = Hy$.

Відображення v — сюр'єктивне: розглянемо довільний лівий суміжний клас zH . Маємо $v(Hz^{-1}) = (z^{-1})^{-1}H = zH$. Таким чином, v — бієктивне відображення.

Нехай G — група, H — її підгрупа. У кожному лівому (відповідно правому) суміжному класі групи G за підгрупою H виберемо по одному представнику і об'єднаємо їх у підмножину $l \cap (G, H)$ (відповідно $r \cap (G, H)$), яку будемо називати повною множиною представників лівих (відповідно правих) суміжних класів групи G за підгрупою H або лівою (відповідно правою) трансверсаллю підгрупи H у групі G . Таким чином,

$$G = \bigcup_{x \in l \cap (G, H)} xH \quad (\text{відповідно } G = \bigcup_{x \in r \cap (G, H)} xH)$$

і рівність $xH = yH$ (відповідно $Hx = Hy$) для $x, y \in l \cap (G, H)$ (відповідно $x, y \in r \cap (G, H)$) означає, що $x = y$.

Нехай G — група, H — її підгрупа. Якщо множина всіх правих суміжних класів групи G за підгрупою H є скінченною, то говорять, що підгрупа H має в групі G скінченний індекс, а кількість всіх (різних) правих суміжних класів називається індексом підгрупи H в групі G . З пропозиції 12.2 випливає, що це число дорівнює кількості всіх (різних) лівих суміжних класів групи G за підгрупою H , тобто індекс підгрупи H в групі G може бути визначений також як кількість всіх (різних) лівих суміжних класів групи G за підгрупою H . Індекс підгрупи H у групі G будемо позначати через $|G : H|$. Інакше кажучи,

$$|G : H| = |r \cap (G, H)| = |l \cap (G, H)|.$$

У випадку, коли $H = G$, маємо $|G : H| = 1$, і навпаки. Якщо група G — скінченна і $H = \langle e \rangle$, то $|G : H| = |G|$.

Будемо говорити, що підгрупа H має в групі G нескінченний індекс, якщо множина всіх (правих) суміжних класів групи G за підгрупою H нескінченна.

12.3. Теорема. Нехай G — група, H, K — такі її підгрупи, що $K \leq H$. Нехай $T = l \cap (G, H)$, $U = l \cap (H, K)$. Тоді підмножина $R = \{tu \mid x \in T, u \in U\}$ буде повною множиною представників (лівих) суміжних класів групи G за підгрупою K .

Д о в е д е н н я . Маємо

$$G = \bigcup_{t \in T} tH, \quad H = \bigcup_{u \in U} uK.$$

Якщо x — довільний елемент групи G , то $x \in tH$ для деякого $t \in T$. Інакше кажучи, $x = th$, де $h \in H$. Знайдеться такий елемент $u \in U$, що $h \in uK$, тобто $h = uv$ для деякого $v \in K$. Отже $x = tuv$. Звідси випливає рівність

$$G = \bigcup_{t \in T, u \in U} tuK.$$

Нехай тепер $tuK = zwK$, де $t, z \in T$, $u, w \in U$. Зокрема, $tu = zwv$ для деякого елемента $v \in K$. Оскільки $u, w, v \in H$, то звідси випливає, що суміжні класи tH та zH мають непустий перетин, а значить співпадають. З визначення множини T випливає тепер рівність $t = z$. Множимо тепер обидві частини рівності $tu = zwv$ зліва на елемент t^{-1} і отримаємо $u = wv$. Це означає, що $u \in wK$, а оскільки u належить також і до суміжного класу uK , то суміжні класи uK та wK мають непустий перетин, а значить співпадають. З визначення множини U випливає тепер рівність $u = w$.

Інакше кажучи, рівність $tuK = zwK$ можлива тільки у випадку, коли $t = z$ і $u = w$. Разом з рівністю $G = \bigcup_{u \in R} uK$ це означає, що підмножина R буде повною множиною представників (лівих) суміжних класів групи G за підгрупою K .

12.4. Наслідок. *Нехай G — група, H, K — такі її підгрупи, що $K \leq H$. Підгрупа K тоді і тільки тоді має скінченний індекс у G , коли скінченними будуть індекси $|G : H|$ та $|H : K|$. У цьому випадку має місце рівність $|G : K| = |G : H| |H : K|$.*

12.5. Наслідок (теорема Лагранжа). *Нехай G — скінченна група, H — її підгрупа. Тоді $|G| = |G : H| |H|$. Інакше кажучи, порядок підгрупи скінченної групи завжди буде дільником порядку всієї групи.*

Дійсно, покладемо у цьому випадку $K = \langle e \rangle$, тоді $|H : K| = |H|$.

12.6. Наслідок. *Порядок елемента скінченної групи буде дільником порядку всієї групи.*

Дійсно, порядок елемента співпадає з порядком циклічної підгрупи, яку породжує цей елемент.

12.7. Наслідок. *Нехай G — скінченна група. Якщо $|G|$ — просте число, то G — циклічна група.*

Дійсно, нехай $e \neq g \in G$. Тоді підгрупа $\langle g \rangle$ має хоча б один неединичний елемент, а тому $|\langle g \rangle| > 1$. Оскільки $|G|$ — просте число, з теореми Лагранжа випливає рівність $|\langle g \rangle| = |G|$, із якої отримуємо, що $\langle g \rangle = G$.

12.8. Наслідок. *Нехай G — група, H, K — її підгрупи. Якщо індекси $|G : H|$ та $|G : K|$ скінченні, то скінченним буде також індекс $|G : H \cap K|$. Більш того, $|G : H \cap K| \leq |G : H| |G : K|$.*

Доведення. Нехай $L = H \cap K$, $T = l \tau(H, L)$, $x, y \in T$, $x \neq y$. Припустимо, що $xK = yK$, тоді $x^{-1}y \in K$. Оскільки $x, y \in H$, то $x^{-1}y \in H \cap K = L$, а тому $xL = yL$. З вибору елементів x, y випливає рівність $x = y$. Отримане протиріччя показує, що

суміжні класи xK та yK будуть різними. З того факту, що індекс $|G : K|$ скінченний, випливає, що скінченним буде індекс $|H : L|$, більш того $|H : L| \leq |G : K|$. З наслідку 12.4 отримуємо тоді

$$|G : H \cap K| = |G : H| |H : H \cap K| \leq |G : H| |G : K|.$$

12.9. Наслідок (теорема Пуанкаре). *Перетин скінченної множини підгруп, кожна з яких має скінченний індекс, буде підгрупою скінченного індексу.*

Скористаємось тепер наведеними вище результатами, щоб отримати більш детальну інформацію про підгрупи циклічних груп. Раніше ми вже довели теорему 10.14, яка показує, що кожна підгрупа циклічної групи сама буде циклічною.

12.10. Теорема. *Нехай $G = \langle g \rangle$ — циклічна група, H — її підгрупа.*

(1) *Якщо G — нескінченна, $H = \langle g^n \rangle$ і $n \neq 0$, то H також нескінченна, $|G : H| = n$; якщо $n = 0$, то індекс $|G : H|$ — нескінченний.*

(2) *Якщо G має скінченний порядок r , то $|H|$ — дільник числа r . Навпаки, для кожного дільника d числа r існує одна і тільки одна підгрупа порядку d , яка співпадає з $\langle g^{r/d} \rangle$.*

Д о в е д е н н я . (1) Нехай x — довільний елемент групи G , тоді $x = g^k$ для деякого $k \in \mathbb{Z}$. Ділимо k на n : $k = nq + s$, де $0 \leq s < n$. Маємо

$$g^k = g^{nq+s} = (g^n)^q g^s \in g^s H.$$

Звідси випливає рівність

$$G = \bigcup_{0 \leq s < n} g^s H.$$

Припустимо тепер, що $g^s H = g^t H$, де $0 \leq s \leq t < n$. Маємо тоді $g^t = g^s u$ для деякого $u \in H$, а оскільки $u = g^{nm}$ для деякого $m \in \mathbb{Z}$, то

$$g^t = g^s g^{nm} = g^{s+nm}.$$

З того факту, що G — нескінченна циклічна група, отримуємо рівність $t = s + nm$, а з вибору чисел s, t випливає тепер $m = 0$, тобто $s = t$. Таким чином, всі суміжні класи $g^s H$, де $0 \leq s < n$, різні, а це означає, що $|G : H| = n$.

Нехай тепер $|G| = r < \infty$. З теореми Лагранжа (наслідок 12.5) отримуємо, що $|H|$ є дільником числа r . Навпаки, нехай d — дільник числа r : $r = db$. Якщо припустити, що $|g^b| = u < d$, то $g^{bu} = e$ і $bu < bd = r$, що суперечить рівності $|g| = r$. Отже $|g^b| = d$. Нехай $\langle g^b \rangle$ — інша підгрупа порядку d . Тоді $g^{bd} = e$, отже bd ділиться на r , а тому b ділиться на d . У свою чергу звідси випливає включення $\langle g^b \rangle \leq \langle g^d \rangle$. Але ж $d = |\langle g^b \rangle|$ і $d = |\langle g^d \rangle|$, так що $\langle g^b \rangle = \langle g^d \rangle$.

12.11. Наслідок. Група G тоді і тільки тоді має тільки дві підгрупи (тобто $\langle e \rangle$ та G), коли $|G|$ — просте число.

Доведення. Нехай g — неединичний елемент групи G , тоді $\langle g \rangle = G$, зокрема, група G — циклічна. Якщо припустити, що $|g|$ — нескінченний, то $\langle e \rangle \neq \langle g^2 \rangle \neq \langle g \rangle$. Це протиріччя показує, що $|g|$ — скінченний. Враховуючи теорему 12.10, отримуємо, що він мусить бути простим числом.

З теореми 12.10 випливає, що кожна неединична підгрупа нескінченної циклічної групи має скінченний індекс. В роботі [3] Ю. Г. Федоров довів, що і навпаки, якщо в нескінченній групі G кожна неединична підгрупа має скінченний індекс, то G — циклічна група.

13. НОРМАЛЬНІ ПІДГРУПИ. ФАКТОР-ГРУПИ

У попередньому розділі ми розглянули розбиття групи, що складаються з правих та лівих суміжних класів за деякою підгрупою. Природно виникає питання: чи будуть ці два розбиття (за однією і тією ж самою підгрупою) суттєво різними, чи вони можуть співпадати? Інакше кажучи, чи будуть еквівалентності Σ_H та Λ_H різними? Або точніше: для яких підгруп H еквівалентності Σ_H та Λ_H (а значить і розбиття на праві та ліві суміжні класи за підгрупою H) співпадають, а для яких вони різні? Зразу видно, що для абелевих груп має місце співпадання. Але на простому прикладі групи S_3 можна упевнитись у тому, що обидві можливості мають місце.

Виберемо підгрупи

$$H = A_3 = \left\{ \varepsilon, \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \pi^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}, \text{ та } K = \langle \tau_{12} \rangle.$$

Оскільки $|H| = 3$, то з теореми Лагранжа (наслідок 12.5) випливає, що $|S_3 : H| = 2$.

13.1. Пропозиція. Нехай G — група, H — її підгрупа. Якщо $|G : H| = 2$, то для кожного $x \notin H$ має місце рівність $xH = Hx = G \setminus H$.

Доведення. Дійсно, як праве так і ліве розбиття на суміжні класи за підгрупою H складається з двох підмножин, одна з яких — сама підгрупа H . Отже другий елемент цього розбиття співпадає з $G \setminus H$.

Таким чином, множина всіх лівих суміжних класів групи S_3 за підгрупою A_3 співпадає з множиною всіх таких правих суміжних

класів. Щодо підгрупи K , то для неї будемо мати три таких правих суміжних класи:

$$K, K \odot \tau_{13} = \{\tau_{13}, \pi^2\}, K \odot \tau_{23} = \{\tau_{23}, \pi\},$$

та три таких лівих суміжних класи:

$$K, \tau_{13} \odot K = \{\tau_{13}, \pi\}, \tau_{23} \odot K = \{\tau_{23}, \pi^2\}.$$

Звідси видно, що множина всіх лівих суміжних класів групи S_3 за підгрупою K не співпадає з множиною всіх правих суміжних класів за підгрупою K .

Нехай G — група, H — така її підгрупа, що множина всіх лівих суміжних класів групи G за підгрупою H співпадає з множиною всіх таких правих суміжних класів. Якщо $x \in G$, то існує такий елемент y , що $xH = Hy$. Оскільки $x \in xH$, то $x \in Hy$, а значить $Hy = Hx$, тобто $xH = Hx$.

Підгрупа H групи G називається *нормальною* (yG), якщо $xH = Hx$ для кожного елемента $x \in G$.

Якщо A, B — дві підмножини групи G , то покладемо

$$AB = \{ab \mid a \in A, b \in B\}.$$

У випадку, коли підмножина A (відповідно B) складається з одного елемента a (відповідно b) замість $\{a\}B$ (відповідно $A\{b\}$) будемо використовувати більш короткий запис aB (відповідно Ab). Аналогічно можна визначити добуток будь-якого скінченного набору підмножин групи. Оскільки множення елементів групи є асоціативним, то і множення підмножин також буде асоціативним.

Дві підгрупи A, B називаються *переставними*, якщо $AB = BA$.

Наступне твердження показує, яку роль має ця властивість.

13.2. Пропозиція. *Нехай G — група, A, B — її підгрупи. Добуток AB тоді і тільки тоді буде підгрупою, коли підгрупи A і B — переставні. У цьому випадку $AB = \langle A \cup B \rangle = \langle A, B \rangle$.*

Д о в е д е н н я . Припустимо, що AB — підгрупа G . Оскільки $A \leq AB$ і $B \leq AB$, то $BA \leq AB$. Нехай x — довільний елемент AB . Оскільки AB — підгрупа, то згідно з теоремою 10.4 разом з елементом x вона містить і елемент x^{-1} . Таким чином, $x^{-1} = uv$, для деяких елементів $u \in A, v \in B$. Маємо тепер

$$x = (x^{-1})^{-1} = (uv)^{-1} = v^{-1}u^{-1}.$$

Знову використовуючи теорему 10.4, отримаємо включення $u^{-1} \in A, v^{-1} \in B$, із яких випливає, що $v^{-1}u^{-1} \in BA$, тобто і $AB \leq BA$, що доводить рівність $AB = BA$.

Навпаки, нехай $AB = BA$. Якщо $x, y \in AB$, то $x = a_1b_1, y = a_2b_2$, для деяких елементів $a_1, a_2 \in A, b_1, b_2 \in B$. Тепер

$$xy^{-1} = (a_1b_1)(a_2b_2)^{-1} = (a_1b_1)(b_2^{-1}a_2^{-1}) = a_1(b_1b_2^{-1})a_2^{-1}.$$

Оскільки B — підгрупа, то за наслідком 10.5 вона містить елемент $b_1 b_2^{-1}$, отже $(b_1 b_2^{-1}) a_2^{-1} \in BA = AB$, а тому $(b_1 b_2^{-1}) a_2^{-1} = a_3 b_3$, де $a_3 \in A$, $b_3 \in B$. Таким чином,

$$xy^{-1} = a_1(a_3 b_3) = (a_1 a_3) b_3 \in AB.$$

Згідно з наслідком 10.5 AB буде підгрупою.

Наступне твердження є дуже корисним.

13.3. Пропозиція. Нехай G — група, A, B, C — такі її підгрупи, що $A \leq C$. Тоді $(AB) \cap C = A(B \cap C)$.

Доведення. Дійсно, $A(B \cap C) \subseteq AB$ та $A(B \cap C) \subseteq AC = C$, отже $A(B \cap C) \subseteq (AB) \cap C$. Навпаки, нехай $x \in (AB) \cap C$, тоді $x = ab$, де $a \in A$, $b \in B$. Маємо $b = a^{-1}x \in AC = C$, зокрема, $b \in B \cap C$ і $x \in A(B \cap C)$, що доводить включення $(AB) \cap C \subseteq A(B \cap C)$, а з ним і потрібну нам рівність $(AB) \cap C = A(B \cap C)$.

Слід відзначити, що з включення $A \leq C$ отримуємо, що $A \cap C = A$, і доведена вище рівність може бути записана у наступному вигляді

$$(AB) \cap C = (A \cap C)(B \cap C).$$

На жаль, у загальному випадку рівність $(AB) \cap C = (A \cap C)(B \cap C)$ виконується далеко не завжди.

Підгрупа групи G , яка переставна з кожною підгрупою G , називається *переставною* або *квазінормальною*. Найбільш важливим прикладом переставних підгруп будуть нормальні підгрупи, до яких ми зараз повернемося. Наведемо основні ознаки нормальних підгруп.

13.4. Пропозиція. Нехай G — група, H — її підгрупа. Наступні твердження рівносильні:

- (1) H — нормальна підгрупа G ;
- (2) $(xH)(yH) = xyH$ для будь-яких елементів $x, y \in G$;
- (3) $x^{-1}Hx \subseteq H$ для кожного елемента $x \in G$;
- (4) $x^{-1}Hx = H$ для кожного елемента $x \in G$.

Доведення. (1) $\Leftrightarrow$ (2) Маємо

$$(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH).$$

Оскільки H — підгрупа, то для довільних елементів $u, v \in H$ маємо, зважаючи на теорему 10.4, $uv \in H$, тобто $HH \subseteq H$. З іншого боку, оскільки $e \in H$, то $H = eH \subseteq HH$, а отже, $HH = H$. Таким чином, якщо підгрупа H нормальна, то $(xH)(yH) = xyH$.

(1) $\Leftrightarrow$ (3) Для кожного $x \in G$ маємо

$$x^{-1}Hx = (x^{-1}Hx)e \subseteq (x^{-1}Hx)H = (x^{-1}H)(xH) = x^{-1}xH = eH = H.$$

(3) $\Leftrightarrow$ (4) Нехай $x \in G$. Тоді $x^{-1}Hx \subseteq H$. Але ж і для елемента x^{-1} подібне включення має місце: $(x^{-1})^{-1}Hx^{-1} = xHx^{-1} \subseteq H$, тому

$$H = (x^{-1}x)H(x^{-1}x) = x^{-1}(xHx^{-1})x \subseteq x^{-1}Hx,$$

і отже, $x^{-1}Hx = H$.

(4) $\Leftrightarrow$ (1) Маємо

$$xH = x(x^{-1}Hx) = (xx^{-1})Hx = eHx = Hx.$$

Наведемо деякі стандартні нормальні підгрупи. Зразу домовимось використовувати для запису того факту, що підгрупа H нормальна в групі G наступне позначення $H \triangleleft G$.

Очевидно, $\langle e \rangle \triangleleft G$ та $G \triangleleft G$. Якщо група G не має інших нормальних підгруп, то G називається *простою групою*. Антипод простої групи — група, всі підгрупи якої нормальні. Такі групи називають за раз *дедекіндовими* на честь Р. Дедекінда, який ще в 1897 р. отримав опис скінченних груп із цією властивістю [4]. Очевидно, кожна абелева група є дедекіндовою. З наслідку 12.11 випливає, що *проста абелева група — це група простого порядку*. Також слід відзначити, що кожна підгрупа центра $\zeta(G)$ групи G буде нормальною.

13.5. Наслідок. Нехай G — група, S — система нормальних підгруп групи G . Перетин $\cap S$ підгруп цієї системи також буде нормальною підгрупою G .

Доведення. Нехай $S' = \cap S$. З наслідку 10.7 випливає, що S' — підгрупа. Нехай $x \in S'$, $g \in G$. Якщо U — довільна підгрупа із системи S , тоді $x \in U$, а оскільки U — нормальна, вона разом з елементом x містить і $g^{-1}xg$. Звідси випливає, що $g^{-1}xg$ належить до перетину всіх підгруп системи S , тобто до S' . Залишилось застосувати пропозицію 13.4.

13.6. Наслідок. Нехай G — група, L — локальна система нормальних підгруп групи G . Тоді об'єднання $\cup L$ підгруп цієї системи також буде нормальною підгрупою G .

Доведення. Нехай $V = \cup L$. З наслідку 10.9 випливає, що V буде підгрупою. Нехай $x \in V$, $g \in G$. Виберемо тепер підгрупу $L \in L$, яка містить у собі елемент x . Оскільки L — нормальна підгрупа, то разом з елементом x вона містить і $g^{-1}xg$. Звідси випливає, що $g^{-1}xg \in V$, і за пропозицією 13.4 підгрупа V також нормальна.

13.7. Наслідок. Нехай G — група, L — лінійно впорядкована система нормальних підгруп групи G . Тоді об'єднання $\cup L$ підгруп цієї системи також буде нормальною підгрупою G .

13.8. Наслідок. Нехай G — група, $H_1 \leq H_2 \leq \dots \leq H_n \leq \dots$ — зростаюча система нормальних підгруп групи G . Тоді об'єднання $\bigcup_{n \in \mathbb{N}} H_n$ підгруп цієї системи також буде нормальною підгрупою G .

Нехай M — підмножина групи G , S — система всіх тих нормальних підгруп, які містять у собі M . Тоді перетин $\langle M \rangle^G = \cap S$ буде за

наслідком 13.5 нормальною підгрупою групи G . Цей перетин називають *нормальною підгрупою, породженою підмножиною M , або нормальним замкненням множини M* . Якщо H — нормальна підгрупа групи G , що містить у собі підмножину M , то H містить у собі і підгрупу $\langle M \rangle^G$, у цьому сенсі $\langle M \rangle^G$ — найменша з нормальних підгруп, які містять у собі підмножину M . Ясно, що якщо M — нормальна підгрупа групи G , то $\langle M \rangle^G = M$. Разом із цим ми маємо наступне корисне твердження.

13.9. Пропозиція. *Нехай G — група, H — її нормальна підгрупа. Якщо $M \subseteq H$, то $\langle M \rangle^G \leq H$.*

Якщо H — підгрупа групи G , то для кожного елемента $x \in G$ підмножина $x^{-1}Hx$ буде підгрупою G . Дійсно, нехай $a, b \in x^{-1}Hx$. Тоді

$$a = x^{-1}ux, b = x^{-1}vx$$

для деяких елементів $u, v \in H$. Маємо тепер

$$ab^{-1} = x^{-1}ux(x^{-1}vx)^{-1} = x^{-1}ux(x^{-1}v^{-1}x) = x^{-1}uv^{-1}x.$$

Оскільки H — підгрупа, $uv^{-1} \in H$. Таким чином, $x^{-1}Hx$ задовольняє умову (SG 3) і за наслідком 10.5 буде підгрупою.

Будемо говорити далі, що підгрупи H і $x^{-1}Hx$ спряжені за допомогою елемента x .

З пропозиції 13.4 випливає, що підгрупа H тоді і тільки тоді нормальна, коли вона співпадає з усякою спряженою до неї підгрупою.

13.10. Пропозиція. *Нехай G — група, H — її підгрупа. Тоді*

$$\bigcap_{x \in G} x^{-1}Hx = \text{Core}_G(H) -$$

нормальна підгрупа групи G . Якщо H містить у собі нормальну підгрупу K , то $K \leq \text{Core}_G(H)$. Інакше кажучи, $\text{Core}_G(H)$ — найбільша нормальна підгрупа, що міститься в підгрупі H .

Доведення. Як ми тільки що довели, $x^{-1}Hx$ — підгрупа G для кожного $x \in G$. З наслідку 10.7 випливає, що $\text{Core}_G(H)$ — підгрупа.

Нехай тепер $u \in \text{Core}_G(H)$, $g \in G$. Маємо

$$u \in (xg^{-1})^{-1}H(xg^{-1}) = gx^{-1}Hxg^{-1},$$

тобто $u = gx^{-1}uxg^{-1}$ для деякого елемента $v \in H$. Звідси отримуємо $g^{-1}ug = x^{-1}vx \in x^{-1}Hx$. Оскільки x — довільний елемент групи G , то $g^{-1}ug \in \text{Core}_G(H)$. З пропозиції 13.4 випливає тепер, що $\text{Core}_G(H)$ — нормальна підгрупа. Далі, оскільки підгрупа K — нормальна, то

$$K = x^{-1}Kx \leq x^{-1}Hx, \text{ тобто } K \leq \bigcap_{x \in G} x^{-1}Hx = \text{Core}_G(H).$$

За аналогією з підгрупами, будемо говорити, що елементи g, u спряжені у групі G , якщо існує такий елемент $x \in G$, що $g = u^{-1}xu$.

Точніше у цьому випадку будемо говорити, що елементи g та y спряжені за допомогою елемента u .

Слід зразу відзначити, що відношення спряженості є відношенням еквівалентності. Дійсно, $g = e^{-1}ue$, так що спряженість є рефлексивною. Якщо $g = u^{-1}yu$, то

$$(u^{-1})^{-1}g u^{-1} = u g u^{-1} = u (u^{-1} y u) u^{-1} = (uu^{-1}) y (uu^{-1}) = y,$$

тобто елемент y спряжений з елементом g за допомогою елемента u^{-1} , отже спряженість є симетричною. Нарешті, нехай $g = u^{-1}yu$ та $y = v^{-1}zv$, тоді маємо

$$g = u^{-1}yu = g = u^{-1}(v^{-1}zv)u = u^{-1}v^{-1}zvu = (vu)^{-1}z(vu),$$

і це показує, що спряженість є транзитивною.

Якщо x — елемент групи G , то клас еквівалентності елемента x за відношенням спряженості називається класом спряженості елемента x і позначається x^G , інакше кажучи, $x^G = \{g^{-1}xg \mid g \in G\}$. Класи спряжених елементів складуть розбиття групи G .

13.11. Пропозиція. Нехай G — група, $x \in G$. Елементи $u^{-1}xu$ та $v^{-1}xv$ співпадають тоді і тільки тоді, коли u і $v^{-1} \in C_G(x)$.

Доведення. Дійсно, якщо $u^{-1}xu = v^{-1}xv$, то отримаємо $uv^{-1}xuv^{-1} = x$, або $(uv^{-1})^{-1}x(uv^{-1}) = x$. А це означає, що $uv^{-1} \in C_G(x)$. Повторюючи все у зворотному порядку, отримаємо достатність.

13.12. Наслідок. Нехай G — група, $x \in G$. Існує бієкція множини x^G на множину $\{g C_G(x) \mid g \in G\}$.

Доведення. Дійсно, розглянемо відображення ϕ , яке визначене за наступним правилом: $\phi: u^{-1}xu \longrightarrow u C_G(x)$, $u \in G$.

Відображення ϕ — ін'єктивне: якщо $u C_G(x) = v C_G(x)$, то $uv^{-1} \in C_G(x)$, і пропозиція 13.11 доводить рівність $u^{-1}xu = v^{-1}xv$. Сюр'єктивність відображення ϕ очевидна.

13.13. Наслідок. Нехай G — група, $x \in G$. Якщо множина x^G скінченна, то скінченною буде й індекс $|G : C_G(x)|$. Більш того, $|x^G| = |G : C_G(x)|$.

Нехай G — група. Покладемо $FC(G) = \{x \in G \mid x^G \text{ — скінченна}\}$.

13.14. Наслідок. Нехай G — група. Підмножина $FC(G)$ є підгрупою.

Доведення. Дійсно, з рівності $(g^{-1}xg)^{-1} = g^{-1}x^{-1}g$ випливає, що $(x^{-1})^G = (x^G)^{-1}$, зокрема, якщо клас x^G є скінченним, то скінченним буде і клас $(x^{-1})^G$.

Далі рівність $g^{-1}(xy)g = g^{-1}xg g^{-1}yg$ доводить включення $(xy)^G \subseteq x^G y^G$, зокрема, якщо класи спряженості x^G та y^G є скінченними, то скінченним буде і $(xy)^G$. Застосування теореми 10.4 доводить тепер, що $FC(G)$ буде підгрупою.

Розглянемо тепер множину $L(G)$ усіх підгруп групи G . Як і для елементів, можна довести, що відношення “підгрупи H і K є спряженими” буде відношенням еквівалентності на множині $L(G)$. Як і для елементів, будемо говорити про класи спряжених підгруп, клас спряженості підгрупи H буде позначатися через $\text{cl}_G(H)$ (тут підкреслюється, що розглядається клас спряженості H у всій групі G , бо можливо розглядати і класи спряженості у підгрупах, які містять у собі H). З пропозиції 13.4 випливає, що підгрупа H тоді і тільки тоді нормальна в G , коли $\text{cl}_G(H) = \{H\}$.

Нехай G — група, H — її підгрупа. Підмножина

$$N_G(H) = \{x \in G \mid x^{-1}Hx = H\}$$

називається нормалізатором підгрупи H у групі G .

13.15. Пропозиція. Нехай G — група, H — її підгрупа. Нормалізатор $N_G(H)$ буде підгрупою групи G .

Доведення. Нехай $x \in N_G(H)$, тоді $x^{-1}Hx = H$. Звідси отримуємо, що і $xHx^{-1} = (x^{-1})^{-1}Hx^{-1} = H$, тобто $x^{-1} \in N_G(H)$. Нехай тепер $x, y \in N_G(H)$, маємо

$$(xy)^{-1}H(xy) = y^{-1}x^{-1}Hxy = y^{-1}(x^{-1}Hx)y = y^{-1}Hy = H,$$

тобто разом з елементами x, y підмножина $N_G(H)$ містить і їх добуток. За теоремою 10.4 $N_G(H)$ буде підгрупою.

Образно кажучи, $N_G(H)$ — це найбільша підгрупа, в якій H нормальна.

13.16. Пропозиція. Нехай G — група, $x \in G$. Елементи $u^{-1}Hu$ та $v^{-1}Hv$ співпадають тоді і тільки тоді, коли $uv^{-1} \in N_G(H)$.

Доведення аналогічне доведенню пропозиції 13.11.

13.17. Наслідок. Нехай G — група, $H \leq G$. Існує бієкція множини $\text{cl}_G(H)$ на множину $\{gN_G(H) \mid g \in G\}$.

Доведення. Дійсно, розглянемо відображення ϕ , яке визначене за наступним правилом:

$$\phi: u^{-1}Hu \longrightarrow uN_G(H), \quad u \in G.$$

Відображення ϕ — ін’єктивне: якщо $uN_G(H) = vN_G(H)$, то $uv^{-1} \in N_G(H)$, і пропозиція 13.16 доводить рівність $u^{-1}Hu = v^{-1}Hv$. Сюр’єктивність відображення ϕ очевидна.

13.18. Наслідок. Нехай G — група, $H \leq G$. Якщо множина $\text{cl}_G(H)$ скінченна, то скінченною буде й індекс $|G : N_G(H)|$. Більш того, $|\text{cl}_G(H)| = |G : N_G(H)|$.

З п.(2) пропозиції 13.4 випливає, що множина всіх суміжних класів групи G за нормальною підгрупою H буде сталою відносно операції множення підмножин. Більш того, відносно зруження цієї

операції ця множина буде групою. Дійсно, асоціативність операції множення підмножин ми вже відзначали вище, зокрема, множення суміжних класів є асоціативним. Одиничним елементом буде сама підгрупа H :

$$(xH)H = xHH = xH, H(xH) = (Hx)H = (xH)H = xH.$$

Нарешті, оберненим елементом до суміжного класу xH буде елемент $x^{-1}H$:

$$(xH)(x^{-1}H) = (xx^{-1})H = eH = (x^{-1}x)H = (x^{-1}H)(xH).$$

Цю групу називають фактор-групою групи G за нормальною підгрупою H і позначають через G/H .

Слід відзначити, що деякі властивості групи унаслідуються усіма її фактор-групами. Наприклад, якщо G — абелева, то і кожна її фактор-група буде абелевою. Дійсно, маємо $xHyH = xyH = yxH = yHxH$ для кожної нормальної підгрупи H і довільних елементів x, y групи G .

А ось інші властивості, наприклад, властивість “бути нескінченною”, не переносяться на всі фактор-групи. В цьому можна упевнитись, розглянувши (адитивну) групу Z цілих чисел та її підгрупу nZ . З теореми 12.10 випливає рівність $|Z/nZ| = n$, яка показує, що нескінченна група Z має скінченні фактор-групи. З іншого боку, очевидно, що будь-яка фактор-група скінченної групи буде скінченною. Таким чином, одне з перших природних питань, яке виникає при розгляді кожного конкретного класу груп X , це питання про те, чи буде X замкненим відносно формування фактор-груп?

З фактор-групами пов'язане також інше питання. Якщо $H = \langle e \rangle$, то для кожного елемента $x \in G$ маємо $xH = x\langle e \rangle = \{x\}$, а також $xHyH = \{x\}\{y\} = \{xy\}$. Це показує, що фактор-група $G/\langle e \rangle$ практично нічим не відрізняється від групи G (використовуючи термінологію наступного параграфа можна сказати, що G та $G/\langle e \rangle$ ізоморфні). Зокрема, вони мають однакові (алгебричні) властивості.

Фактор-група G/H називається власною, якщо H — неединична нормальна підгрупа.

Більше півстоліття тому почалося вивчення впливу множини всіх власних фактор-груп групи на будову всієї групи. Деякий підсумок цих досліджень підведено у книзі Л. А. Курдаченка, Х. Отала та І. Я. Субботіна [5].

Якщо x, y — елементи групи G , то елемент $[x, y] = x^{-1}y^{-1}xy$ будемо називати комутатором елементів x та y . Якщо $xy = yx$, то звідси послідовно отримуємо $y^{-1}xy = x$ та потім $x^{-1}y^{-1}xy = 1$; навпаки, повторюючи теж саме у зворотному порядку, із рівності $[x, y] = 1$ отримаємо $xy = yx$. Таким чином, елементи x та y тоді і тільки тоді переставні, коли $[x, y] = 1$.

Підгрупу групи G , породжену підмножиною $\{[x, y] \mid x, y \in G\}$, називають комутантом або похідною підгрупою групи G та позначають через $[G, G]$.

З очевидної рівності $g^{-1}[x, y]g = [g^{-1}xg, g^{-1}yg]$ випливає, що $D = [G, G]$ — нормальна підгрупа групи G . На роль комутанта вказує наступне твердження.

13.19. Пропозиція. *Нехай G — група.*

(1) *Фактор-група $G/[G, G]$ — абелева.*

(2) *Якщо H — така нормальна підгрупа групи G , що G/H — абелева, то $[G, G] \leq H$.*

Доведення. Дійсно, розглянемо фактор-групу G/D , де $D = [G, G]$. Для кожної пари суміжних класів xD, yD маємо

$$\begin{aligned} [xD, yD] &= (xD)^{-1}(yD)^{-1}(xD)(yD) = (x^{-1}D)(y^{-1}D)(xD)(yD) = \\ &= x^{-1}y^{-1}xyD = [x, y]D = D, \end{aligned}$$

що доводить абелевість G/D . Нехай тепер H — така нормальна підгрупа групи G , що фактор-група G/H — абелева. Аналогічним чином можна довести рівність $H = [x, y]H$, із якої випливає включення $[x, y] \in H$ для кожної пари елементів $x, y \in G$. Звідси випливає включення $[G, G] \leq H$.

14. ГОМОМОРФІЗМИ ГРУП

Розглянемо спочатку факторизацію звичайних відображень. Нехай A — множина, на якій задано відношення еквівалентності Ξ , і введемо нову множину A/Ξ , елементами якої будуть класи еквівалентності за відношенням еквівалентності Ξ . Цю множину будемо називати фактор-множиною множини A за відношенням еквівалентності Ξ . Разом з цим виникає наступне відображення

$$\sigma_{\Xi} : A \longrightarrow A/\Xi,$$

що визначається за наступним правилом:

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

Відображення σ_{Ξ} називається канонічною сюр'єкцією A на фактор-множину A/Ξ .

Нехай A, B — множини, $f: A \longrightarrow B$ — відображення. Пов'яжемо з цим відображенням бінарне відношення $\Delta(f)$, яке визначається за наступним правилом: $(x, y) \in \Delta(f)$ тоді і тільки тоді, коли $f(x) = f(y)$, $x, y \in A$. Відношення $\Delta(f)$, очевидно, рефлексивне: $f(x) = f(x)$; симетричне: рівності $f(x) = f(y)$ та $f(y) = f(x)$ рівносильні; транзитивне: з рівностей $f(x) = f(y)$ та $f(y) = f(z)$ випливає $f(x) = f(z)$, $x, y, z \in A$. Таким чином, $\Delta(f)$ — відношення еквівалентності на множині A .

Розглянемо фактор-множину $A/\Delta(f)$ та пов'яжемо з нею відображення $\psi_f: A/\Delta(f) \rightarrow \text{Im } f$, яке визначається за наступним правилом:

$\psi_f([a]_{\Delta(f)}) = f(a)$ для кожного класу еквівалентності $[a]_{\Delta(f)} \in A/\Delta(f)$.

Перш за все потрібно упевнитись у тому, що ψ_f визначено коректно, тобто не залежить від вибору представника класу еквівалентності. Дійсно, нехай c — елемент множини A , для якого $[c]_{\Delta(f)} = [a]_{\Delta(f)}$. Тоді за самим визначенням відношення $\Delta(f)$ маємо $f(a) = f(c)$, що і доводить коректність.

Відображення ψ_f є бієктивним: для кожного елемента $b \in \text{Im } f$ існує елемент $a \in A$ з властивістю $b = f(a)$, так що маємо $\psi_f([a]_{\Delta(f)}) = f(a) = b$, тобто ψ_f — сюр'єктивне; якщо $\psi_f([a]_{\Delta(f)}) = \psi_f([c]_{\Delta(f)})$, то за визначенням ψ_f маємо $f(a) = f(c)$, а це означає, що $(a, c) \in \Delta(f)$ і отже $[c]_{\Delta(f)} = [a]_{\Delta(f)}$, таким чином ψ_f — ін'єктивне, а отже і бієктивне.

Нарешті, розглянемо такий добуток відображень $j_D \circ \psi_f \circ \sigma_{\Delta(f)}$, де $D = \text{Im } f$, а j_D — канонічна ін'єкція D в B . Для довільного елемента $a \in A$ маємо

$$j_D \circ \psi_f \circ \sigma_{\Delta(f)}(a) = j_D(\psi_f(\sigma_{\Delta(f)}(a))) = j_D(\psi_f([a]_{\Delta(f)})) = j_D(f(a)) = f(a).$$

Оскільки область визначення відображення $j_D \circ \psi_f \circ \sigma_{\Delta(f)}$ збігається з A , а область значень — з B , то отримаємо рівність $f = j_D \circ \psi_f \circ \sigma_{\Delta(f)}$. Підводячи підсумок, сформулюємо все доведене вище у вигляді наступної теореми.

14.1. Теорема. Нехай A, B — множини, $f: A \longrightarrow B$ — відображення.

(1) відношення $\Delta(f)$, визначене за правилом:

$(x, y) \in \Delta(f)$ тоді і тільки тоді, коли $f(x) = f(y)$, $x, y \in A$,
є відношенням еквівалентності на множині A .

(2) відображення $\psi_f: A/\Delta(f) \longrightarrow \text{Im } f$, визначене за правилом:
 $\psi_f([a]_{\Delta(f)}) = f(a)$ для кожного класу еквівалентності
 $[a]_{\Delta(f)} \in A/\Delta(f)$, є бієктивним.

(3) $f = j_D \circ \psi_f \circ \sigma_{\Delta(f)}$.

Зокрема, довільне відображення є добутком сюр'єкції, бієкції та ін'єкції.

Розклад відображення, отриманий у теоремі 14.1, називають канонічним.

Повернемось тепер до груп та їх відображень. Природно ми будемо розглядати не будь-які відображення, а ті, що зберігають операцію, тобто гомоморфізми груп. Почнемо з елементарних властивостей групових гомоморфізмів.

14.2. Пропозиція. Нехай G, U — групи, $f: G \longrightarrow U$ — гомоморфізм.

(1) $f(e) = e_U$ — одиничний елемент групи U .

(2) Якщо $f(x) = u$, то $f(x^{-1}) = u^{-1}$.

(3) Якщо H — підгрупа G , то її образ $f(H)$ буде підгрупою в U .
Зокрема, $f(G) = \text{Im } f$ — підгрупа U .

(4) Якщо V — підгрупа U , то її повний прообраз $f^{-1}(V)$ — підгрупа в G .

(5) Якщо V — нормальна підгрупа U , то її повний прообраз $f^{-1}(V)$ — нормальна підгрупа в G . Зокрема,

$$\text{Ker } f = \{x \in G \mid f(x) = e_U\} = f^{-1}(\langle e_U \rangle) \text{ — нормальна підгрупа } G.$$

Д о в е д е н н я . (1) За визначенням одиничного елемента маємо $ex = x$ для кожного елемента $x \in G$, зокрема, $ee = e$. Звідси отримуємо

$$f(e) = f(ee) = f(e)f(e).$$

Кожний елемент групи U , зокрема, $f(e)$, має обернений; множимо на цей обернений обидві частини останньої рівності і приходимо до рівності

$$e_U = e_U f(e) = f(e).$$

(2) За визначенням елемента, оберненого до x , маємо $xx^{-1} = e = x^{-1}x$. Звідси отримуємо

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e_U = f(e) = f(x^{-1}x) = f(x^{-1})f(x).$$

Ці рівності показують, що $u^{-1} = f(x^{-1})$.

(3) Нехай $u, v \in f(H)$, тоді знайдуться елементи $a, c \in H$, для яких $u = f(a)$, $v = f(c)$. Маємо $uv^{-1} = f(a)f(c^{-1}) = f(ac^{-1}) \in f(H)$, оскільки H — підгрупа G . Згідно з наслідком 10.5 $f(H)$ буде підгрупою U .

(4) Нехай $x, y \in f^{-1}(V)$, тоді $f(x), f(y) \in V$. Знову застосуємо критерій підгрупи: $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} \in V$ і отже $xy^{-1} \in f^{-1}(V)$. За наслідком 10.5 $f^{-1}(V)$ буде підгрупою G .

(5) Нехай g — довільний елемент групи G , $x \in f^{-1}(V)$. Розглянемо елемент $g^{-1}xg$, точніше його образ відносно f :

$$f(g^{-1}xg) = f(g^{-1})f(x)f(g) = (f(g))^{-1}f(x)f(g) \in V,$$

оскільки $V \triangleleft U$. Це означає, що $g^{-1}xg \in f^{-1}(V)$, а отже, $f^{-1}(V)$ — нормальна підгрупа G .

Слід відзначити, що образ нормальної підгрупи не завжди буде нормальною підгрупою; у цьому можна упевнитись, розглянувши канонічну ін'єкцію ненормальної підгрупи в групу.

Нормальну підгрупу $\text{Ker } f$ називають ядром гомоморфізма f .

Розглянемо тепер класичні теореми про гомоморфізми.

14.3. Теорема (теорема про мономорфізми). *Нехай G, U — групи. Гомоморфізм $f: G \longrightarrow U$ тоді і тільки тоді буде мономорфізмом, коли $\text{Ker } f = \langle e \rangle$. Якщо $f: G \longrightarrow U$ — мономорфізм, то $G \cong \text{Im } f$.*

Д о в е д е н н я . Дійсно, якщо f — мономорфізм, то з $x \neq e$ випливає $f(x) \neq f(e) = e_U$. Це означає, що жодний неединичний елемент x не може належати до $\text{Ker } f$, отже $\text{Ker } f = \langle e \rangle$.

Навпаки, нехай $\text{Ker } f = \langle e \rangle$, x, y — такі елементи групи G , що $f(x) = f(y)$. Тоді маємо

$$e_G = f(e) = f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1},$$

і отже $xy^{-1} \in \text{Ker } f$. Це означає, що $xy^{-1} = e$, тобто $x = y$, а значить, f — ін'єктивне відображення.

14.4. Теорема (теорема про епіморфізми). Нехай G, U — групи, $f: G \rightarrow U$ — епіморфізм. Тоді група U ізоморфна до фактор-групи $G/\text{Ker } f$.

Доведення. Покладемо для зручності $H = \text{Ker } f$. Розглянемо відношення еквівалентності $\Delta(f)$. Як і в попередній теоремі можна показати, що рівність $f(x) = f(y)$ рівносильна $f(xy^{-1}) = e$, інакше кажучи, $(x, y) \in \Delta(f)$ рівносильне $xy^{-1} \in H$, тобто $\Delta(f) = \Sigma_H$. З результатів розділу 12 отримуємо $[x]_{\Delta(f)} = xH$ для кожного $x \in G$, а значить $G/\Delta(f) = G/H$.

Розглянемо тепер відображення $\psi_f: G/H \rightarrow U$, яке визначається за правилом $\psi_f(xH) = f(x)$. З теореми 14.1 випливає, що ψ_f — бієкція, так що залишається довести тільки, що ψ_f — гомоморфізм. Маємо

$$\psi_f(xH yH) = \psi_f(xyH) = f(xy) = f(x)f(y) = \psi_f(xH) \psi_f(yH).$$

14.5. Теорема (теорема про гомоморфізми). Нехай G, U — групи, $f: G \rightarrow U$ — гомоморфізм. Тоді $G/\text{Ker } f \cong \text{Im } f \leq U$.

Доведення. Дійсно, звуження f до відображення $G \rightarrow \text{Im } f$ буде епіморфізмом, так що з теореми 14.4 отримуємо ізоморфізм $\text{Im } f \cong G/\text{Ker } f$. Нарешті, з пропозиції 14.2 випливає, що $\text{Im } f$ є підгрупою в U .

Розглянемо тепер деякі застосування отриманих результатів, і як перший крок, отримаємо опис циклічних груп.

14.6. Теорема. Нехай $G = \langle g \rangle$ — циклічна група.

(1) Якщо група G — нескінченна, то вона ізоморфна адитивній групі $\mathbb{Z}$ цілих чисел.

(2) Якщо G — скінченна і $|G| = m$, то $G \cong \mathbb{Z}/m\mathbb{Z}$.

Доведення. Розглянемо відображення $f: \mathbb{Z} \rightarrow G$, що визначається за правилом $f(n) = g^n$, $n \in \mathbb{Z}$. З властивостей цілих степенів отримуємо

$$f(n+k) = g^{n+k} = g^n g^k = f(n) f(k),$$

так що f — гомоморфізм. Оскільки кожний елемент групи G є цілим степенем елемента g , то f буде епіморфізмом.

Нехай група G є нескінченною, тоді з нерівності $n \neq k$ випливає, що $f(n) = g^n \neq g^k = f(k)$, тобто відображення f — ін'єктивне, а отже буде ізоморфізмом.

Нехай тепер G — скінченна група. У цьому випадку маємо

$|g| = m$, зокрема, $g^m = e$, а значить $m \in \text{Ker } f$. З пропозиції 10.2 отримуємо включення $\langle m \rangle = mZ \leq \text{Ker } f$. З теореми 10.14 отримуємо, що $\text{Ker } f = \langle t \rangle = tZ$, а оскільки $m \in tZ$, то $m = ts$. З теореми 14.4 отримуємо ізоморфізм $G \cong G/\text{Ker } f$, зокрема, $|G/\text{Ker } f| = m$.

З іншого боку, теорема 12.10 дає рівності $|Z/mZ| = m$ та $|Z/tZ| = t$, які показують, що $t = m$. Таким чином, $G \cong Z/mZ$.

Розглянемо інші цікаві приклади.

14.7. Приклад. Нехай a — дійсне число, $a > 1$. Визначимо відображення $f: R \rightarrow R^\times$, за наступним правилом: $f(x) = a^x$ для кожного $x \in R$. Маємо тепер $f(x+y) = a^{x+y} = a^x a^y = f(x)f(y)$, так що f — гомоморфізм. Очевидно, що f — ін'єктивне та $\text{Im } f$ складається з усіх додатних дійсних чисел, тобто f — ізоморфізм адитивної групи всіх дійсних чисел на мультиплікативну групу всіх строго додатних дійсних чисел.

14.8. Приклад. Визначимо відображення $f: GL_n(R) \rightarrow R^\times$, за наступним правилом: $f(A) = \det(A)$ для кожної матриці $A \in GL_n(R)$. З теореми 8.1 випливають рівності

$$f(AB) = \det(AB) = \det(A) \det(B) = f(A) f(B),$$

які показують, що f — гомоморфізм. Далі

$$\text{Ker } f = \{A \in GL_n(R) \mid \det(A) = 1\} = SL_n(R).$$

Зокрема, $SL_n(R)$ — нормальна підгрупа в $GL_n(R)$. Очевидно, що відображення f — ін'єктивне, і з теореми 14.4 отримуємо

$$GL_n(R)/SL_n(R) \cong R^\times.$$

Аналогічно

$$GL_n(Q)/SL_n(Q) \cong Q^\times \quad \text{і} \quad GL_n(Z)/SL_n(Z) \cong \{1, -1\}.$$

14.9. Приклад. Визначимо відображення $f: T_n(R) \rightarrow D_n(\quad)$, за наступним правилом:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n-1} & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n-1} & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n-1} & a_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & a_{nn} \end{pmatrix} \xrightarrow{f} \begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 & 0 \\ 0 & a_{22} & 0 & \dots & 0 & 0 \\ 0 & 0 & a_{33} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & a_{nn} \end{pmatrix}.$$

З результатів розділу 11 випливає, що f — гомоморфізм (f називають *стираючим гомоморфізмом*). Очевидно, відображення f — сюр'єктивне і $\text{Ker } f = UT_n(R)$, зокрема $UT_n(R)$ — нормальна підгрупа в $T_n(R)$. З теореми 14.4 отримуємо ізоморфізм $T_n(R)/UT_n(R) \cong D_n(R)$. Доречно також відзначити, що $UT_n(R)$ не буде нормальною підгрупою в усій групі $GL_n(R)$.

14.10. Приклад. Нехай G — група. Гомоморфізм $\phi: G \longrightarrow G$ будемо називати *ендоморфізмом* групи G . Множину всіх ендоморфізмів групи G позначимо через $\text{End}(G)$. Ендоморфізм ϕ групи G , який одночасно є підстановкою G , називається *автоморфізмом* групи G . Множину всіх автоморфізмів групи G позначимо через $\text{Aut}(G)$. Зразу слід сказати, що $\text{Aut}(G)$ — підгрупа групи підстановок $S(G)$. Дійсно, нехай $\phi, \psi \in \text{Aut}(G)$, тоді

$$\begin{aligned}(\phi \circ \psi)(xy) &= \phi(\psi(xy)) = \phi(\psi(x)\psi(y)) = \phi(\psi(x)) \phi(\psi(y)) = \\ &= (\phi \circ \psi)(x) (\phi \circ \psi)(y),\end{aligned}$$

так що $\phi \circ \psi \in \text{Aut}(G)$. У розділі 9 ми вже показували, що відображення, обернене до ізоморфізму, само буде ізоморфізмом, зокрема, відображення, обернене до автоморфізму, буде автоморфізмом. Таким чином, $\text{Aut}(G)$ задовольняє всі умови критерію підгрупи (теорема 10.4), отже $\text{Aut}(G) \leq S(G)$.

У групі G візьмемо довільний елемент g і пов'яжемо з ним відображення $\text{in}_g: G \longrightarrow G$, що визначається за правилом: $\text{in}_g(x) = g^{-1}xg$ для кожного $x \in G$. Маємо

$$\text{in}_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \text{in}_g(x) \text{in}_g(y),$$

так що $\text{in}_g(x)$ — ендоморфізм. Якщо x — довільний елемент групи G , то з рівностей $\text{in}_g(gxg^{-1}) = g^{-1}(gxg^{-1})g = x$ випливає, що $\text{in}_g(x)$ — сюр'єкція; якщо $\text{in}_g(x) = g^{-1}xg = g^{-1}yg = \text{in}_g(y)$, то помноживши справа на g^{-1} , а зліва на g , отримаємо $x = y$, так що $\text{in}_g(x)$ — ін'єкція, тобто $\text{in}_g(x)$ — автоморфізм. Відображення in_g називають *внутрішнім автоморфізмом, індукованим елементом g* .

Тепер розглянемо нове відображення $\Phi: G \longrightarrow \text{Aut}(G)$, визначене за таким правилом: $\Phi(g) = \text{in}_{g^{-1}}$ для кожного елемента $g \in G$. З наступної допоміжної рівності

$$\begin{aligned}\text{in}_{gh}(x) &= (gh)^{-1}x(gh) = h^{-1}g^{-1}xgh = h^{-1}(g^{-1}xg)h = \\ &= \text{in}_h(\text{in}_g(x)) = (\text{in}_h \circ \text{in}_g)(x)\end{aligned}$$

випливає, що $\text{in}_{gh} = \text{in}_h \circ \text{in}_g$. Тепер маємо

$$\Phi(gh) = \text{in}_{(gh)^{-1}} = \text{in}_{g^{-1}h^{-1}} = \text{in}_{g^{-1}} \circ \text{in}_{h^{-1}} = \Phi(g) \circ \Phi(h),$$

і це показує, що Φ — гомоморфізм.

Нехай $u \in \text{Ker } \Phi$, тоді $\Phi(u) = \text{in}_{u^{-1}} = \varepsilon_G$, отже

$$\text{in}_{u^{-1}}(x) = g x g^{-1} = \varepsilon_G(x) = x$$

для кожного $x \in G$. У свою чергу, рівність $gxg^{-1} = x$ еквівалентна $gx = xg$ для кожного $x \in G$, а це показує, що $g \in \zeta(G)$, тобто $\text{Ker } \Phi \leq \zeta(G)$. Протилежне включення очевидне, тому отримуємо рівність $\text{Ker } \Phi = \zeta(G)$. $\text{Im } \Phi$ позначимо через $\text{Inn}(G)$. За пропозицією 14.2 $\text{Inn}(G)$ — підгрупа в $\text{Aut}(G)$, її називають *групою внутрішніх автоморфізмів групи G* . З теореми 14.5 отримуємо ізоморфізм $\text{Inn}(G) \cong G/\zeta(G)$.

14.11. Приклад. Нехай G — група, H — її підгрупа, $R_H = \{xH \mid x \in G\}$ — розбиття G на ліві суміжні класи за підгрупою H . Якщо $g \in G$, то визначимо відображення $\tau_g: R_H \longrightarrow R_H$ за наступним правилом: $\tau_g(xH) = (gx)H$. Очевидно, воно визначено коректно.

Відображення τ_g : — ін'єктивне: $xH = g(g^{-1}xH) = \tau_g(g^{-1}xH)$.

Відображення τ_g : — ін'єктивне: якщо $\tau_g(x) = \tau_g(y)$, то $gxH = gyH$. Звідси $(gx)^{-1}(gy) \in H$, але $(gx)^{-1}(gy) = x^{-1}g^{-1}gy = x^{-1}y$, і це означає, що $xH = yH$. Таким чином, τ_g — підстановка множини R_H . Розглянемо тепер відображення $\Psi: G \longrightarrow S(R_H)$, яке визначається за правилом: $\Psi(g) = \tau_g$ для кожного $g \in G$.

Маємо

$$\tau_{gv}(xH) = (gv)(xH) = g(vxH) = \tau_g(vxH) = \tau_g(\tau_v(xH)) = \tau_g \circ \tau_v(xH),$$

тобто $\tau_{gv} = \tau_g \circ \tau_v$. Тому $\Psi(gv) = \tau_{gv} = \tau_g \circ \tau_v = \Psi(g) \circ \Psi(v)$, так що Ψ — гомоморфізм. Нехай $K = \text{Ker } \Psi$. Якщо $g \in \text{Ker } \Psi$, $\Psi(g) = \tau_g = \epsilon$, де ϵ — тотожна підстановка множини R_H . Інакше кажучи, $\tau_g(xH) = gxH = xH$ для кожного $x \in G$. Зокрема, для $x = e$ отримуємо $gH = H$, тобто $g \in H$. Таким чином, $K \leq H$.

Нехай тепер L — нормальна підгрупа G , яка міститься в підгрупі H . Якщо $g \in L$, то для довільного $x \in G$ маємо $x^{-1}gx = g_1 \in L$. Звідси $gx = xg_1$, а тому $\tau_g(xH) = gxH = xg_1H = xH$, тобто $L \leq K$.

Таким чином, K — найбільша нормальна підгрупа, яку містить у собі H , тобто $K = \text{Core}_G(H)$.

Якщо $H = \langle e \rangle$, то і $K = \langle e \rangle$, і за теоремою 14.3 Ψ — мономорфізм, так що доведена теорема Келі.

14.12. Теорема (теорема Келі). Кожна група G ізоморфна підгрупі групи підстановок деякої множини.

14.13. Наслідок. Якщо група G — скінченна, $|G| = n$, то G ізоморфна підгрупі групи S_n .

14.14. Наслідок. Нехай група G містить у собі підгрупу H скінченного індексу, $|G:H| = n$. Тоді H містить у собі підгрупу K , що нормальна в усій групі G , причому $|G/K| \leq n!$.

15. КІЛЬЦЯ, ПІДКІЛЬЦЯ, ЇХ ЕЛЕМЕНТАРНІ ВЛАСТИВОСТІ. ПРИКЛАДИ КІЛЕЦЬ

Ми вже розглядали множини, на яких задано одну бінарну алгебричну операцію. Проте, в математиці часто доводиться зустрічатися з множинами, на яких задано кілька алгебричних операцій, причому ці операції ще певним чином зв'язані між собою. Як правило зв'язок між операціями забезпечується законом дистрибутивності. Одним з перших прикладів такого роду є множини $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ множина

дійсних функцій, а також множини матриць, $M_n(Z)$, $M_n(Q)$, $M_n(R)$. Історично, витоки теорії кілець та полів з'являються в теорії чисел та в теорії поліномів, основні поняття теорії полів з'являються в теорії Галуа. Сформувавшись, це поняття знайшло численні застосування у різних розділах алгебри й інших математичних дисциплінах.

Множина R , на якій задано дві бінарні алгебричні операції — додавання та множення, називається кільцем, якщо вона задовольняє наступні умови:

(R 1) відносно операції додавання R — абелева група.

Це означає, що операція додавання комутативна, тобто

$$a + b = b + a \quad \text{для будь-яких } a, b \in R;$$

операція додавання асоціативна:

$$a + (b + c) = (a + b) + c \quad \text{для будь-яких } a, b, c \in R;$$

існує нульовий елемент O_R :

$$a + O_R = a \quad \text{для будь-якого } a \in R;$$

для кожного елемента $a \in R$ існує протилежний елемент $-a$:

$$a + (-a) = O_R.$$

(R 2) операції додавання і множення зв'язані законами дистрибутивності:

$$(a + b)c = ac + bc, \quad a(b + c) = ab + ac \quad \text{для довільних } a, b, c \in R.$$

Розглядаючи R тільки з операцією додавання, ми будемо говорити про адитивну групу кільця R .

Наявність протилежного елемента дозволяє ввести в кільці операцію віднімання за правилом $a - b = a + (-b)$.

Відзначимо деякі елементарні наслідки з аксіом кільця.

15.1. Пропозиція. Нехай R — кільце. Мають місце наступні рівності:

$$a \cdot O_R = O_R \cdot a = O_R \quad \text{для всіх } a \in R.$$

$$a(-b) = (-a)b = -ab.$$

$$a(b - c) = ab - ac; \quad (a - b)c = ac - bc \quad \text{для довільних } a, b, c \in R.$$

Д о в е д е н н я . Дійсно, для кожного $b \in R$ маємо $b + O_R = b$. Скориставшись законами дистрибутивності, одержимо

$$ab = a(b + O_R) = ab + a \cdot O_R \quad \text{і} \quad ba = (b + O_R)a = ba + O_R \cdot a.$$

Оскільки для елемента ab кільця R існує протилежний елемент, то, додаючи його до обох частин цих рівностей, одержуємо $a \cdot O_R = O_R \cdot a = O_R$.

З означення протилежного елемента і законів дистрибутивності одержуємо

$$O_R = a \cdot O_R = a(b + (-b)) = ab + a(-b);$$

$$O_R = O_R \cdot b = (a + (-a)) \cdot b = ab + (-a) \cdot b.$$

Ці рівності показують, що кожен з добутків $a(-b)$ і $(-a)b$ — це елемент, протилежний ab .

Доведені щойно рівності показують, що операції віднімання і множення теж зв'язані законами дистрибутивності:

$$a(b - c) = ab - ac, \quad (a - b)c = ac - bc.$$

Кільце R називається асоціативним, якщо множення в R асоціативне:

$$(R\ 3) \quad a(bc) = (ab)c \text{ для всіх } a, b, c \in R.$$

Кільце R називається комутативним, якщо множення в R комутативне:

$$(R\ 4) \quad ab = ba \text{ для будь-яких } a, b \in R.$$

Будемо говорити також, що R — кільце з одиницею, якщо R має одиничний елемент e відносно операції множення:

$$(R\ 5) \quad ae = ea = a \text{ для кожного } a \in R.$$

Надалі будемо розглядати лише асоціативні кільця з одиницею. Треба сказати, проте, що і теорія деяких типів неасоціативних кілець (у певному розумінні близьких до асоціативних) розвинута досить глибоко. Відзначимо найважливіші з цих типів кілець.

Кільце R називається лівим кільцем (або кільцем Li), якщо воно задовольняє такі умови:

$$(LR\ 1) \quad a^2 = O_R \text{ для будь-якого } a \in R;$$

$$(LR\ 2) \quad (ab)c + (bc)a + (ca)b = O_R \text{ для всіх } a, b, c \in R.$$

Умова $(LR\ 2)$ називається тотожністю Якобі.

Кільце R називається йордановим кільцем, якщо воно комутативне і задовольняє таку умову:

$$(JR) \quad ((a \cdot a)b)a = (a \cdot a)(b \cdot a) \text{ для будь-яких елементів } a, b \in R.$$

Кільце R називається альтернативним, якщо воно задовольняє умови

$$(AR\ 1) \quad (aa)b = a(ab);$$

$$(AR\ 2) \quad (ba)a = b(aa)$$

для довільних елементів $a, b \in R$.

Розгляд неасоціативних кілець не є нашою метою; інформацію про такі кільця можна знайти, наприклад, у таких класичних монографіях, як [6, 7, 8, 9, 10].

Починаючи з цього моменту, говорячи "кільце", будемо розуміти під цим асоціативне кільце з одиницею.

Нехай R — кільце, в якому $O_R = e$. Тоді маємо $a = ae = aO_R = O_R$ для кожного $a \in R$. Таким чином, кільце, в якому нульовий і одиничний елементи рівні, складається лише з одного нульового елемента. Такі кільця будемо називати тривіальними. А надалі будемо розглядати тільки кільця, у яких нульовий і одиничний елементи різні.

З визначення кільця R випливає, що відносно операції множення воно буде напівгрупою з одиницею. Тому ми можемо розглянути групу $U(R)$ всіх інвертованих елементів цієї напівгрупи. Далі $U(R)$ будемо називати групою інвертованих елементів кільця R .

Відзначимо зразу ж, що $0_R \notin U(R)$.

Кільце R називається тілом, якщо кожен його ненульовий елемент інвертований, тобто $U(R) = R \setminus \{0_R\}$. Комутативне тіло називається полем.

Ненульовий елемент a кільця R називається лівим (відповідно правим) дільником нуля, якщо в R існує такий ненульовий елемент b , що $ab = 0_R$ (відповідно $ba = 0_R$).

Для комутативного кільця поняття правого і лівого дільника нуля збігаються.

Нехай $ab = 0_R$ і припустимо, що $a \in U(R)$. Тоді

$$0_R = a^{-1} \cdot 0_R = a^{-1}(ab) = (a^{-1}a)b = e \cdot b = b.$$

Звідси випливає, що інвертований елемент не може бути дільником нуля.

15.2. Пропозиція. Нехай R — кільце, $a \in R$. Якщо елемент a не є лівим (відповідно правим) дільником нуля, то з рівності $ax = ay$ (відповідно $xa = ya$) завжди випливає $x = y$.

Насправді, $ax = ay$ приводить до рівності $ax - ay = 0_R$. Використовуючи закони дистрибутивності, одержуємо звідси $a(x - y) = 0_R$. Оскільки a не є лівим дільником нуля, то це означає, що $x - y = 0_R$, тобто $x = y$.

15.3. Наслідок. Нехай R — кільце, що не має дільників нуля, a — його ненульовий елемент. Тоді з рівності $ax = ay$ (відповідно $xa = ya$) завжди випливає $x = y$.

Будемо говорити, що кільце R є областю цілісності, якщо воно комутативне і не має дільників нуля.

Нехай R — кільце, H — його підмножина. Будемо говорити, що H — підкільце R , якщо H є сталою підмножиною R відносно обох операцій і H є кільцем відносно звужень цих операцій.

15.4. Теорема. Непуста підмножина H кільця R тоді і тільки тоді є підкільцем, коли вона задовольняє наступні умови:

(SR 1) якщо $x, y \in H$, то $x - y \in H$;

(SR 2) якщо $x, y \in H$, то $xy \in H$.

Доведення. Нехай H — підкільце в R . Зокрема, H є сталою підмножиною відносно операції додавання і буде групою відносно звуження цієї операції. Інакше кажучи, H — підгрупа адитивної групи кільця R . Наслідок 10.5 показує, що умова (SR 1) буде необхідною. Умова (SR 2) показує, що H — стала підмножина відносно операції множення.

Навпаки, нехай підмножина задовольняє вказані умови. Наслідок 10.5 показує, що відносно операції додавання H буде підгрупою R . Зокрема, H є сталою підмножиною відносно операції додавання і буде групою відносно звуження цієї операції. Умова (SR 2) показує, що звуження операції множення на H буде бінарною операцією на підмножині H . Закони дистрибутивності та асоціативності виконуються для всіх елементів з R , зокрема вони виконуються і для всіх елементів із H . Отже H задовольняє всі умови (R 1) — (R 3), а тому буде підкільцем в R .

Слід відзначити, що, на відміну від підгруп, підкільце не обов'язково містить одиничний елемент усього кільця. Підкільце H кільця R називається унітарним, якщо H містить одиничний елемент кільця R .

Надалі той факт, що H — підкільце у кільці R , буде записуватись так: $H \leq R$.

15.5. Наслідок. Нехай R — кільце, S — система підкілець кільця R . Перетин $\cap S$ підкілець цієї системи також буде підкільцем R .

Доведення. Нехай $S = \cap S$, $x, y \in S$, U — довільне підкільце з системи S , тоді $x - y, xy \in U$, і отже $x - y, xy$ належить перетину всіх таких підгруп, тобто S . Залишилось застосувати теорему 15.4.

Слід відзначити, що об'єднання підкілець не завжди буде підкільцем, оскільки і об'єднання підгруп не завжди буде підгрупою, як ми вже бачили це раніше.

15.6. Наслідок. Нехай R — кільце, L — локальна система підкілець кільця R . Тоді об'єднання $\cup L$ підкілець цієї системи також буде підкільцем R .

Доведення. Нехай $V = \cup L$, $x, y \in V$. Існують такі підкільця H, K з системи L , що $x \in H, y \in K$. Виберемо тепер підкільце $L \in L$, яке містить у собі обидва підкільця H, K . Таким чином, $x, y \in L$. Оскільки L — підкільце, $x - y, xy \in L$ за теоремою 15.4, і отже $x - y, xy \in V$. Залишилось знову застосувати теорему 15.4.

15.7. Наслідок. Нехай R — кільце, L — лінійно впорядкована система підкілець кільця R . Тоді об'єднання $\cup L$ підкілець цієї системи також буде підкільцем R .

15.8. Наслідок. Нехай R — кільце, $H_1 \leq H_2 \leq \dots \leq H_n \leq \dots$ — зростаюча система підкілець кільця R . Тоді об'єднання $\bigcup_{n \in \mathbb{N}} H_n$ також буде підкільцем R .

Нехай M — підмножина кільця R , S — система всіх тих підкілець, які містять у собі M . Тоді перетин $r(M) = \cap S$ буде за

наслідком 15.5 підкільцем кільця R . Цей перетин називають *підкільцем*, *породженням* підмножиною M , а множина M називається *системою породжуючих елементів* для підкільця $r(M)$. Зокрема, якщо $r(M) = R$, то будемо говорити, що M породжує все кільце R . Кільце R називається *скінченною породженням*, якщо воно породжується деякою своєю скінченною підмножиною.

Якщо H — підкільце в R , що містить у собі підмножину M , то H містить у собі і підкільце $r(M)$, у цьому сенсі $r(M)$ — найменше з підкілець, які містять у собі підмножину M . Ясно, що якщо M — підкільце кільця R , то $r(M) = M$. Разом із цим ми маємо наступне корисне твердження.

15.9. Пропозиція. Нехай R — кільце, H — його підкільце. Якщо $M \subseteq H$, то $r(M) \subseteq H$.

Нехай T — тіло, H — його підмножина. Будемо говорити, що H — *підтіло* T , якщо H — унітарне підкільце, яке є тілом відносно операцій додавання і множення, що задані в T .

15.10. Теорема. Нехай T — тіло. Підмножина H тіла T тоді і тільки тоді є підтілом T , коли H задовольняє наступні умови:

(SF 1) якщо $x, y \in H$, то $x - y, xy \in H$;

(SF 2) $e \in H$;

(SF 3) якщо $x \in H, x \neq 0_T$, то $x^{-1} \in H$.

Твердження теореми майже очевидне. Наступні наслідки, аналогічні відповідним твердженням для підкілець, тому їх доведення ми опускаємо.

15.11. Наслідок. Нехай T — тіло. Підмножина H тіла T тоді і тільки тоді буде його підтілом, коли H задовольняє наступні умови:

(SF 4) H містить ненульові елементи;

(SF 5) якщо $x, y \in H$, то $x - y, xy \in H$;

(SF 6) якщо $x, y \in H, y \neq 0_T$, то $xy^{-1} \in H$.

15.12. Наслідок. Нехай T — тіло, S — система підтіл T . Перетин $\cap S$ підтіл, що належать до цієї системи, також буде підтілом T .

Як і для підкілець, об'єднання підтіл не завжди буде підтілом.

15.13. Наслідок. Нехай T — тіло, L — локальна система підтіл T . Тоді об'єднання $\cup L$ підтіл, що належать до цієї системи, також буде підтілом T .

15.14. Наслідок. Нехай T — тіло, L — лінійно впорядкована система підтіл T . Тоді об'єднання $\cup L$ підтіл, що належать до цієї системи, також буде підтілом T .

15.15. Наслідок. Нехай T — тіло, $H_1 \leq H_2 \leq \dots \leq H_n \leq \dots$ — зростаюча система підтіл T . Тоді об'єднання $\bigcup_{n \in \mathbb{N}} H_n$ також буде підтілом T .

Із наслідку 15.12 випливає, що перетин T_0 усіх тіл підтіла T є підтілом, яке вже не містить власних підтіл.

Тіло T називається простим, якщо воно не містить у собі власних (тобто відмінних від T) підтіл.

Нехай T — тіло, H — його підтіло. Якщо H комутативне, то будемо говорити, що H — підполе T .

Як і для груп розглянемо корисну конструкцію декартового (прямого) добутку скінченної множини кілець. Нехай $R_1, \dots, R_n$ — кільця, $D = R_1 \times \dots \times R_n$ — їх декартовий добуток як множин. На множині D визначимо операції додавання та множення за правилами

$$(y_1, \dots, y_n) + (x_1, \dots, x_n) = (y_1 + x_1, \dots, y_n + x_n),$$

де $y_j, x_j \in R_j, 1 \leq j \leq n$,

$$(y_1, \dots, y_n)(x_1, \dots, x_n) = (y_1 x_1, \dots, y_n x_n),$$

де $y_j, x_j \in R_j, 1 \leq j \leq n$.

Оскільки y_j, x_j — елементи одного і того ж кільця R_j , то їх сума та добуток визначені у цьому кільці $R_j, 1 \leq j \leq n$, так що ми отримали дійсно операції на D . Застосовуючи ті ж самі аргументи, що використовувались при розгляді декартових добутків груп, можна довести, що операції додавання та множення асоціативні, додавання комутативне, має нульовий елемент, яким буде набір $(0_1, \dots, 0_n)$, де 0_j — нульовий елемент кільця $R_j, 1 \leq j \leq n$, і також

$$-(y_1, \dots, y_n) = (-y_1, \dots, -y_n).$$

Якщо e_j — одиничний елемент кільця $R_j, 1 \leq j \leq n$, то набір $(e_1, \dots, e_n)$ буде, очевидно, одиничним елементом для D . Нарешті, покажемо, що додавання та множення пов'язані законами дистрибутивності. Дійсно,

$$\begin{aligned} ((y_1, \dots, y_n) + (x_1, \dots, x_n)) (z_1, \dots, z_n) &= \\ &= (y_1 + x_1, \dots, y_n + x_n) (z_1, \dots, z_n) = \\ &= ((y_1 + x_1)z_1, \dots, (y_n + x_n)z_n) = (y_1 z_1 + x_1 z_1, \dots, y_n z_n + x_n z_n) = \\ &= (y_1 z_1, \dots, y_n z_n) + (x_1 z_1, \dots, x_n z_n) = \\ &= (y_1, \dots, y_n)(z_1, \dots, z_n) + (x_1, \dots, x_n)(z_1, \dots, z_n). \end{aligned}$$

Інший закон дистрибутивності доводиться аналогічно. Таким чином, всі аксіоми кільця для D виконані. Тому далі, коли мова зайде про декартовий добуток кілець, ми будемо розуміти під цим тільки що побудоване кільце. Це кільце називається також прямою сумою кілець $R_1, \dots, R_n$ (як і для груп, поняття прямої суми та декартового добутку кілець у загальному випадку відрізняються один

від одного, але для випадку скінченної множини кілець вони співпадають). Якщо всі кільця $R_1, \dots, R_n$ — комутативні, то і їх декартовий добуток буде комутативним кільцем.

Розглянемо тепер будову групи $U(D)$. Нехай $(y_1, \dots, y_n) \in U(D)$. Тоді існує такий набір $(z_1, \dots, z_n)$, що

$$(y_1, \dots, y_n)(z_1, \dots, z_n) = (y_1 z_1, \dots, y_n z_n) = (e_1, \dots, e_n).$$

Інакше кажучи, $y_j z_j = e_j$, тобто $y_j \in U(R_j)$ для кожного j , $1 \leq j \leq n$. Нехай тепер $y_j \in U(R_j)$ для кожного j , $1 \leq j \leq n$. Повторюючи попередні аргументи у зворотному порядку, покажемо, що $(y_1, \dots, y_n) \in U(D)$. Таким чином, ми отримали рівність

$$U(R_1 \times \dots \times R_n) = U(R_1) \times \dots \times U(R_n).$$

Розглянемо тепер деякі важливі приклади кілець і підкілець.

Числові кільця. Множина R усіх дійсних чисел є комутативним кільцем. Його унітарні підкільця — множина Q усіх раціональних чисел і множина Z усіх цілих чисел. Більше того, Q і R є полями. Z дає нам також приклад скінченню породженого кільця, воно породжується числом 1. У розділі 11 ми вже відзначали, що для кожного $n \geq 0$ підмножина $nZ = \{nk \mid k \in Z\}$ буде підгрупою Z , зокрема, вона задовольняє умову (SR 1). Далі, $(nk)(nt) = n(nkt)$, тобто nZ задовольняє умову (SR 2) і отже за теоремою 15.4 nZ буде підкільцем Z . З теореми 10.13 випливає, що довільна підгрупа Z співпадає з однією з підмножин nZ , $n \geq 0$, і інших підгруп Z не має. Це означає, що множина всіх підкілець Z збігається з $\{nZ \mid n \geq 0\}$.

Нехай p — просте число, розглянемо адитивну групу Q_p p -ічних дробів. Маємо $(m/(p^k))(r/(p^s)) = (mr)/(p^{k+s})$, а це показує, що Q_p задовольняє умову (SR 2), отже за теоремою 15.4 Q_p буде підкільцем Q , більш того, унітарним підкільцем. Його називають кільцем p -ічних дробів.

Матричні кільця. Нехай R — цілісності. Через $M_n(R)$ позначимо сукупність всіх квадратних матриць порядку n , коефіцієнти яких належать кільцю R . Якщо $A = \|a_{ij}\|_{1 \leq i, j \leq n}$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$ — дві матриці з множини $M_n(R)$, то їх сумою $A + B$ будемо називати матрицю $\|c_{ij}\|_{1 \leq i, j \leq n}$, коефіцієнти якої визначаються за правилом

$$c_{ij} = a_{ij} + b_{ij} \text{ для кожної пари індексів } i, j, 1 \leq i, j \leq n,$$

а добутком AB цих матриць будемо називати матрицю $\|d_{ij}\|_{1 \leq i, j \leq n}$, коефіцієнти якої визначаються за правилом

$$d_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{1 \leq k \leq n} a_{ik}b_{kj}$$

для кожної пари індексів i, j , $1 \leq i, j \leq n$.

Інакше кажучи, ми зберігаємо ті визначення суми та добутку, які вже були введені для числових матриць. Повторюючи дослівно всі аргументи розділу 5, покажемо, що $M_n(R)$ буде кільцем відносно цих операцій. Слід відзначити, що, як і для числових матриць, це кільце не комутативне.

Як і для числових матриць, ми можемо ввести визначення визначника матриці $A = \|a_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$ за правилом

$$\det(A) = \sum_{\pi \in S_n} \text{sign } \pi a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}.$$

Неважко впевнитися в тому, що всі властивості визначників, доведені у розділах 6, 7, а також теорема 8.1 залишаються справедливими для області цілісності R . Нехай $A \in U(M_n(R))$, $a = \det(A)$. Оскільки

$$e = \det(E) = \det(AA^{-1}) = \det(A) \det(A^{-1}) = a \det(A^{-1}),$$

то $a \in U(R)$. Навпаки, нехай A — така матриця, що $\det(A) \in U(R)$. Розглянемо тепер матрицю $B = \|b_{ij}\|_{1 \leq i, j \leq n} \in M_n(R)$, коефіцієнти якої визначаються за правилом $b_{ij} = A_{ji} / \det(A)$, $1 \leq i, j \leq n$. Неважко пересвідчитися в тому, що $AB = BA = E$, тобто матриця B буде оберненою для матриці A . Таким чином,

$$U(M_n(R)) = \{A \in M_n(R) \mid \det(A) \in U(R)\}.$$

Як і для числових матриць, цю групу називають *загальною лінійною групою степеня n над кільцем R* . Зокрема, якщо R — поле, то $U(M_n(R))$ — це знову множина всіх невідроджених матриць.

Знову позначимо через E_{km} матрицю, у якій на (k, m) -му місці стоїть одиничний елемент, а всі інші місця зайняті нулями $E_{km} = \|u_{ij}^{(k, m)}\|_{1 \leq i, j \leq n}$, яка визначається за наступним правилом. Як і для числових матриць, неважко довести таку рівність:

$$E_{km}E_{rs} = \begin{cases} E_{ks}, & \text{якщо } m = r, \\ O, & \text{якщо } m \neq r, \end{cases}$$

зокрема, $E_{12}E_{23} = E_{13}$, $E_{23}E_{12} = O$.

Звідси випливає, що кільце $M_n(R)$ — некомутативне (якщо $n \geq 2$) і містить дільники нуля.

Позначимо тепер через $T_n^*(R)$ підмножину $M_n(R)$, що складається з усіх трикутних (точніше верхньо-трикутних) матриць. Очевидно, різниця двох трикутних матриць є трикутною матрицею. Як і в розділі 11, можна показати, що добуток двох трикутних матриць є матрицею трикутною. Із теореми 15.4 одержуємо, що $T_n^*(R)$ — підкільце $M_n(R)$.

Трикутну матрицю будемо називати нультрикутною, якщо всі елементи її головної діагоналі нульові.

Множину всіх нультрикутних матриць порядку n з коефіцієнтами з кільця R позначимо через $NT_n(R)$. Можна легко пересвідчитися, що підмножина $NT_n(R)$ задовольняє умови (SR 1) і (SR 2), так що з теореми 15.4 одержуємо, що $NT_n(R)$ — підкільце $M_n(R)$.

Позначимо через $D_n^*(R)$ множину всіх діагональних матриць порядку n , коефіцієнти яких належать до кільця R . Далі покладемо

$$RE = \{\lambda E \mid \lambda \in R\},$$

тобто RE — підмножина всіх скалярних матриць. З теореми 15.4 знову одержуємо, що $D_n^*(R)$ і RE — підкільця $M_n(R)$. Із самого означення випливає, що $T_n^*(R)$, $D_n^*(R)$ і RE — унітарні підкільця $M_n(R)$.

Нарешті, нехай

$$RE_{ii} = \{\lambda E_{ii} \mid \lambda \in R\}.$$

Маємо $\lambda E_{ii} - \mu E_{ii} = (\lambda - \mu)E_{ii}$, $\lambda E_{ii} \mu E_{ii} = \lambda \mu E_{ii}$. Із теореми 15.4 випливає, що RE_{ii} — підкільце $M_n(R)$. Далі, $\lambda E_{ii} eE_{ii} = eE_{ii} \lambda E_{ii} = \lambda E_{ii}$.

Ця рівність показує, що $eE_{ii} = E_{ii}$ — одиничний елемент підкільця RE_{ii} . Таким чином, підкільце RE_{ii} хоча і не є унітарним, але має свій одиничний елемент.

Функціональні кільця. Нехай R — довільне кільце, M — довільна множина. У множині R^M усіх функцій, визначених на M , що набувають значень у кільці R , визначимо суму і добуток за правилом:

$$(f + g)(a) = f(a) + g(a), (fg)(a) = f(a)g(a)$$

для будь-якого елемента $a \in M$.

Множина R^M є абелевою групою відносно операції додавання: якщо $f, g \in R^M$, то

$$(f + g)(a) = f(a) + g(a) = g(a) + f(a) = (g + f)(a)$$

для кожного елемента $a \in M$. Звідси випливає, що $f + g = g + f$.

Аналогічно, для $f, g, h \in R^M$ маємо

$$\begin{aligned} (f + (g + h))(a) &= f(a) + (g + h)(a) = f(a) + (g(a) + h(a)) = \\ &= (f(a) + g(a)) + h(a) = (f + g)(a) + h(a) = ((f + g) + h)(a) \end{aligned}$$

для довільного елемента $a \in M$, так що $f + (g + h) = (f + g) + h$.

Задамо відображення θ правилом $\theta(a) = 0_R$ для кожного $a \in M$. Тоді

$$(f + \theta)(a) = f(a) + \theta(a) = f(a) + 0_R = f(a), \text{ тобто } f + \theta = f,$$

для будь-якого $f \in R^M$.

Це означає, що θ — нульовий елемент R^M . Нарешті, відображення $-f$ визначимо за правилом $(-f)(a) = -f(a)$. Очевидно, $f + (-f) = \theta$. Отже, всі аксіоми абелевої групи виконані.

Нехай $f, g, h \in R^M$, $a \in M$, тоді

$$\begin{aligned} (f(g + h))(a) &= f(a)((g + h)(a)) = f(a)(g(a) + h(a)) = f(a)g(a) + f(a)h(a) = \\ &= (fg)(a) + (fh)(a) = (fg + fh)(a), \end{aligned}$$

тобто $f(g + h) = fg + fh$.

Аналогічно доводиться, що $(f + g)h = fh + gh$.

Множення функцій асоціативне:

$$\begin{aligned} (f(gh))(a) &= f(a)(gh)(a) = f(a)(g(a)h(a)) = (f(a)g(a))h(a) = \\ &= (fg)(a)h(a) = ((fg)h)(a). \end{aligned}$$

Одиничним елементом буде функція I , яка визначається за

правилом $I(a) = e$ для кожного елемента $a \in M$: $(fI)(a) = f(a)I(a) = f(a)e = f(a)$, тобто $fI = f$. І аналогічно $If = f$.

Таким чином, відносно введених вище операцій додавання та множення R^M буде кільцем. Якщо R комутативне, то і кільце R^M комутативне:

$$(fg)(a) = f(a)g(a) = g(a)f(a) = (gf)(a).$$

Розглянемо групу $U(R^M)$. Зрозуміло, що вона складається з усіх таких функцій f , що $f(a) \in U(R)$ для всіх $a \in M$.

Кільце R^M має дільники нуля. Наприклад, нехай L — непуста підмножина M . Задамо функції f, g таким чином:

$$f(a) = \begin{cases} e, & \text{якщо } a \in L, \\ O_R, & \text{якщо } a \notin L, \end{cases} \quad g(a) = \begin{cases} O_R, & \text{якщо } a \in L, \\ e, & \text{якщо } a \notin L. \end{cases}$$

Функції f, g — ненульові, проте $f(a)g(a) = O_R$ для будь-якого $a \in M$.

У аналізі найчастіше зустрічається приклад, коли $M = [a, b]$ — відрізок прямої, або $M = R$, а $R = R$ — поле дійсних чисел. Інакше кажучи, $R^M = R^{[a, b]}$ (відповідно $R^M = R^R$) — кільце всіх функцій, заданих на $[a, b]$ (відповідно на R) із значеннями в полі дійсних чисел. Тут виникає досить багато підкільць: підкільце всіх неперервних функцій, підкільце всіх диференційованих функцій, підкільце всіх двічі диференційованих функцій і т.д.

Кільце ендоморфізмів абелевої групи. Нехай A — абелева група, операція в якій записується адитивно. У розділі 14 ми вже розглядали множину $\text{End}(A)$ всіх ендоморфізмів групи A . Задамо додавання ендоморфізмів таким правилом: якщо $f, g \in \text{End}(A)$, то покладемо

$$(f + g)(a) = f(a) + g(a) \text{ для будь-якого елемента } a \in A.$$

Маємо

$$\begin{aligned} (f + g)(a + b) &= f(a + b) + g(a + b) = f(a) + f(b) + g(a) + g(b) = \\ &= f(a) + g(a) + f(b) + g(b) = (f + g)(a) + (f + g)(b). \end{aligned}$$

Це означає, що $f + g$ — ендоморфізм A . Таким чином, відображення

$$(f, g) \longrightarrow f + g, \quad f, g \in \text{End}(A)$$

є бінарною операцією на множині $\text{End}(A)$.

Множина $\text{End}(A)$ є абелевою групою відносно цієї операції:

$$(f + g)(a) = f(a) + g(a) = g(a) + f(a) = (g + f)(a);$$

$$(f + (g + h))(a) = f(a) + (g + h)(a) = f(a) + (g(a) + h(a));$$

$$((f + g) + h)(a) = (f(a) + g(a)) + h(a) = (f(a) + g(a)) + h(a)$$

для будь-якого елемента $a \in A$; звідси одержуємо, що

$$f + g = g + f, \quad f + (g + h) = (f + g) + h$$

для довільних $f, g, h \in \text{End}(A)$.

Задамо відображення θ правилом $\theta(a) = 0_A$ для кожного $a \in A$. Тоді $(f + \theta)(a) = f(a) + \theta(a)$, тобто $f + \theta = f$ для будь-якого $f \in \text{End}(A)$. Це означає, що θ — нульовий елемент $\text{End}(A)$. Нарешті, покладемо $(-f)(a) = -f(a)$. Очевидно, $f + (-f) = \theta$. Отже, всі аксіоми абелевої групи виконані.

Нехай $f, g \in \text{End}(A)$, $a, b \in A$. Маємо

$$\begin{aligned} (f \odot g)(a + b) &= f(g(a + b)) = f(g(a) + g(b)) = \\ &= f(g(a)) + f(g(b)) = (f \odot g)(a) + (f \odot g)(b). \end{aligned}$$

Ця рівність показує, що $f \odot g$ — ендоморфізм A . Таким чином, відображення

$$(f, g) \longrightarrow f \odot g, \quad f, g \in \text{End}(A),$$

є бінарною операцією на множині $\text{End}(A)$.

Нехай $f, g, h \in \text{End}(A)$, $a \in A$. Тоді

$$\begin{aligned} (f \odot (g + h))(a) &= f(g + h)(a) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) = \\ &= (f \odot g)(a) + (f \odot h)(a) = (f \odot g + f \odot h)(a). \end{aligned}$$

Звідси випливає, що

$$f \odot (g + h) = f \odot g + f \odot h.$$

Аналогічно доводиться другий закон дистрибутивності. Як ми вже знаємо з розділу 3, множення відображень асоціативне, а підстановка ε_A , що задається правилом $\varepsilon_A(a) = a$ для кожного $a \in A$, є одиничним елементом відносно операції множення. Таким чином, $\text{End}(A)$ — кільце. Його називають *кільцем ендоморфізмів абелевої групи A* .

Булеві кільця. Нехай M — довільна множина, $A = B(M)$ — її булеан. Якщо $a, b \in A$, то покладемо

$$a + b = (a \cup b) \setminus (a \cap b), \quad ab = a \cap b.$$

Неважко перевірити, що $B(M)$ — кільце. Більше того, в цьому кільці для кожного елемента a маємо $a^2 = a$, $2a = \emptyset = 0_A$. Кільця з такими властивостями називають *булевими*.

Центр кільця. Якщо R — кільце, то через $\zeta(R)$ позначимо множину всіх елементів R , що переставні з кожним елементом R . Нехай $a, b \in \zeta(R)$, $x \in R$. Маємо

$$(a - b)x = ax - bx = xa - xb = x(a - b),$$

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Ці рівності показують, що $a - b, ab \in \zeta(R)$. З теореми 15.4 випливає, що $\zeta(R)$ — підкільце R . Підкільце $\zeta(R)$ називається *центром кільця R* .

Нехай $Ze = \{ne \mid n \in Z\}$. Знову

$$ne - ke = (n - k)e, (ne)(ke) = (nk)e.$$

З теореми 15.4 знову випливає, що Ze — підкільце R , а оскільки

$$(ne)a = n(ea) = na = a(ne),$$

то $ne \in \zeta(R)$. Таким чином, $Ze \leq \zeta(R)$.

Нільпотентні елементи кільця. Нехай R — кільце. Елемент a називають нільпотентним, якщо $a^n = 0_R$ для деякого $n \in \mathbb{N}$. Якщо R — комутативне кільце, то сукупність його нільпотентних елементів буде підкільцем. Справді, знову застосовуємо теорему 15.4. Нехай $a^n = 0_R$, $b^t = 0_R$ для деяких $n, t \in \mathbb{N}$. Розглянемо $(a - b)^{n+t}$. Цей елемент є лінійною комбінацією елементів $a^k b^m$ з деякими цілими коефіцієнтами, причому $k + m = n + t$. Тому якщо $k \geq n$, то $a^k b^m = 0_R$. Якщо ж $k < n$, то $m > t$ і знову $a^k b^m = 0_R$. Таким чином, $(a - b)^{n+t} = 0_R$. Далі,

$$(ab)^{n+t} = a^{n+t} b^{n+t} (a - b)^{n+t} = 0_R.$$

16. ІДЕАЛИ КІЛЕЦЬ, ФАКТОР-КІЛЬЦЯ

Як ми вже бачили раніше, одним з основних понять теорії груп є поняття нормальної підгрупи. Нормальні підгрупи дозволяють отримувати з даної групи нові — її фактор-групи, а також тісно пов'язані з іншим важливим поняттям — поняттям гомоморфізмів. Аналог нормальних підгруп виникає і в кільцях, цим аналогом є ідеали кілець. Поняття ідеалу виникло з задач, що зовсім не є аналогічними тим, з яких виникло поняття нормальної підгрупи. Це також обумовило і різницю в термінах. Поняття ідеалу зникло при вивченні числових кілець, у яких розклад на прості елементи не є однозначним. Намагання якимось чином повернути однозначність хоча б у більш слабкій формі і привело до виникнення того поняття, яке зараз називається ідеалом. І тільки пізніше почала виявлятися аналогія між поняттями нормальної підгрупи групи та ідеалу кільця.

Підкільце H кільця R називається ідеалом (в R), якщо для кожного елемента $x \in R$ та кожного елемента $h \in H$ добутки xh та hx містяться в H .

Це поняття, як правило, поділяється на два.

Підкільце H кільця R називається лівим (відповідно правим) ідеалом (в R), якщо для кожного елемента $x \in R$ та кожного елемента $h \in H$ добуток xh (відповідно hx) міститься в H .

Враховуючи критерій підкільця (теорема 15.4), отримуємо наступний критерій ідеалу.

16.1. Пропозиція. Непуста підмножина H кільця R тоді і тільки тоді є ідеалом, коли вона задовольняє наступні умови:

- (I 1) якщо $x, y \in H$, то $x - y \in H$;
 (I 2) якщо $x \in R, h \in H$, то добутки xh та hx містяться в H .

Кожна підмножина, що є одночасно правим і лівим ідеалом, буде ідеалом кільця. Тому говорять ще про “двосторонній ідеал” кільця. Якщо ж R — комутативне кільце, то всі ці поняття збігаються. У будь-якому кільці R підмножини $\langle 0_R \rangle$ та R є ідеалами.

Кільце R називається простим, якщо його єдиними ідеалами є лише $\langle 0_R \rangle$ та R .

Наступні наслідки, аналогічні відповідним твердженням для підкілець, тому їх доведення ми опускаємо.

16.2. Наслідок. Нехай R — кільце, S — система ідеалів кільця R . Перетин $\cap S$ ідеалів, що належать до цієї системи також буде ідеалом R .

16.3. Наслідок. Нехай R — кільце, S — локальна система ідеалів кільця R . Тоді об'єднання $\cup S$ ідеалів, що належать до цієї системи, також буде ідеалом R .

16.4. Наслідок. Нехай R — кільце, S — лінійно впорядкована система ідеалів кільця R . Тоді об'єднання $\cup S$ ідеалів, що належать до цієї системи, також буде ідеалом R .

16.5. Наслідок. Нехай R — кільце, $H_1 \leq H_2 \leq \dots \leq H_n \leq \dots$ — зростаюча система ідеалів кільця R . Тоді об'єднання $\bigcup_{n \in \mathbb{N}} H_n$ також буде ідеалом R .

Нехай M — підмножина кільця R , S — система всіх тих ідеалів, які містять у собі M . Тоді перетин $\text{id}(M) = \cap S$ буде за наслідком 16.2 ідеалом кільця R . Цей перетин називають ідеалом, породженим підмножиною M , а множина M називається системою породжуючих елементів для ідеалу $\text{id}(M)$. Якщо $M = \{a\}$, то, скорочуючи, замість $\text{id}(\{a\})$ будемо писати $\text{id}(a)$ і говорити про ідеал, породжений елементом a . Цей ідеал частіше називають головним ідеалом кільця R .

Розглянемо випадок, коли кільце R — комутативне. Якщо $x \in R$, то $ax \in \text{id}(a)$. Покладемо $aR = \{ax \mid x \in R\}$. Наша мета зараз — довести рівність $aR = \text{id}(a)$. Уже доведено включення $aR \leq \text{id}(a)$. З іншого боку, покажемо, що aR — ідеал кільця R , тобто aR задовольняє умови (I 1), (I 2). Дійсно, якщо $u, v \in aR$, то $u = ay, v = az$ для деяких елементів $y, z \in R$. Тепер маємо

$$u - v = ay - az = a(y - z) \in aR,$$

$$gu = ug = (ay)g = a(yg) \in aR$$

для довільного елемента g кільця R . Отже aR — ідеал в R . Оскільки $a = ae$, то $a \in aR$, а тому $\text{id}(a) \leq aR$. Це останнє включення доводить рівність $aR = \text{id}(a)$.

Раніше вже відзначалося, що будь-яке підкільце кільця Z має вигляд nZ , де $n \geq 0$. Таким чином, кожне підкільце Z є ідеалом, причому головним ідеалом.

У розділі 13 ми визначили добуток підгруп у довільній групі. По аналогії можна визначити суму підкілець кільця. Нехай R — кільце, H, K — його підкільця.

Покладемо $H + K = \{x + y \mid x \in H, y \in K\}$. Підмножину $H + K$ будемо називати сумою підкілець H, K .

З самого визначення випливає включення $H, K \subseteq H + K$. Як і в ситуації груп, сума підкілець не завжди буде підкільцем. Але якщо хоча б одне з них, наприклад, H , є ідеалом, то $H + K$ — підкільце. Дійсно, нехай $a, b \in H + K$, тоді $a = x + y$, $b = x_1 + y_1$ для деяких елементів $x, x_1 \in H, y, y_1 \in K$. Маємо

$$a - b = (x + y) - (x_1 + y_1) = (x - x_1) + (y - y_1) \in H + K,$$

$$ab = (x + y)(x_1 + y_1) = xx_1 + xy_1 + yx_1 + yy_1.$$

Оскільки H — ідеал, то $xx_1 + xy_1 + yx_1 \in H$, а тому

$$(xx_1 + xy_1 + yx_1) + yy_1 \in H + K.$$

Отже $H + K$ задовольняє умови (SR 1) та (SR 2), і з теореми 15.4 випливає, що $H + K$ — підкільце R . Більш того, якщо H, K — ідеали R , то і їх сума $H + K$ буде ідеалом: якщо $x \in H, y \in K, z \in R$, то

$$z(x + y) = zx + zy \in H + K,$$

$$(x + y)z = xz + yz \in H + K,$$

так що $H + K$ задовольняє умови (I 1), (I 2) і за пропозицією 16.1 буде ідеалом кільця R . Зауважимо також, що якщо ідеали H, K містяться у більшому ідеалі L , то $H + K \leq L$.

16.6. Пропозиція. *Нехай R — кільце, H — його ідеал. Якщо H містить інвертований елемент кільця R , то $H = R$.*

Дійсно, нехай $x \in H \cap U(R)$. Оскільки H — ідеал, то $e = x^{-1}x \in H$. Якщо тепер a — довільний елемент R , то $a = ae \in H$. Це й означає, що $H = R$.

16.7. Наслідок. *Будь-яке тіло є простим кільцем.*

Однак наступна теорема показує, що обернене твердження не є вірним.

16.8. Теорема. *Кільце матриць $M_n(F)$ над полем F є простим.*

Доведення. Нехай L — ненульовий ідеал кільця $M_n(F)$, $B = \|b_{ij}\|_{1 \leq i, j \leq n}$ — ненульова матриця, що належить до L . Існує така пара індексів k, t , що $b_{kt} \neq 0_F$. Розглянемо послідовно наступні добутки:

$$\begin{aligned} E_{st}B &= E_{st}\left(\sum_{1 \leq i, j \leq n} b_{ij}E_{ij}\right) = \sum_{1 \leq i, j \leq n} b_{ij}E_{st}E_{ij} = \\ &= \sum_{1 \leq i, j \leq n} b_{tj}E_{st}E_{ij} = \sum_{1 \leq i, j \leq n} b_{tj}E_{sj}; \end{aligned}$$

$$E_{st}BE_{qr} = \left(\sum_{1 \leq i, j \leq n} b_{tj}E_{sj}\right)E_{qr} = \sum_{1 \leq i, j \leq n} b_{tj}E_{sj}E_{qr} = b_{tq}E_{sr}.$$

Оскільки L — ідеал $M_n(F)$, то $E_{st}BE_{qr} \in L$ для довільних індексів s, t, q, r . Нехай тепер $A = \|a_{ij}\|_{1 \leq i, j \leq n}$ — довільна матриця. З доведеного вище отримуємо, що

$$a_{ij}E_{ij} = (a_{ij}a_{ik}^{-1}E)(E_{ik}BE_{kj}) \in L$$

для довільної пари індексів i, j , а це показує, що

$$A = \sum_{1 \leq i, j \leq n} a_{ij}E_{ij} \in L,$$

отже $L = M_n(F)$.

Як ми бачили у попередньому розділі, $M_n(F)$ містить дільники нуля, а тому не є полем. Але у випадку комутативних кілець твердження, обернене до наслідку 16.7, є вірним:

16.9. Теорема. *Якщо R — комутативне просте кільце, то R є полем.*

Доведення. Дійсно, нехай a — довільний ненульовий елемент кільця R . Оскільки $a \in aR$, то aR — ненульовий ідеал кільця R , а тому $aR = R$. Зокрема, існує такий елемент x , що $ax = e$. Таким чином, довільний ненульовий елемент a має обернений, і отже кільце R є полем.

Нехай R — кільце, H — його ідеал. Оскільки H — підгрупа адитивної групи кільця R , то множина всіх суміжних класів $\{x + H \mid x \in R\}$ є абелевою групою відносно операції додавання, яка визначається за правилом

$$(x + H) + (y + H) = x + y + H.$$

Визначимо тепер множення суміжних класів за таким правилом

$$(x + H)(y + H) = xy + H.$$

Це означення коректне: насправді, нехай x_1, y_1 — такі елементи кільця R , що $x + H = x_1 + H$, $y + H = y_1 + H$, тоді $x_1 = x + u$, $y_1 = y + v$ для деяких елементів $u, v \in H$ і

$$x_1y_1 = (x + u)(y + v) = xy + uy + xv + uv.$$

Оскільки H — ідеал, то $uy, xv, uv \in H$, тому $xy + H = x_1y_1 + H$. Далі

$$\begin{aligned} (x + H)(y + H + z + H) &= (x + H)(y + z + H) = x(y + z) + H = \\ &= xy + xz + H = xy + H + xz + H = (x + H)(y + H) + (x + H)(z + H), \end{aligned}$$

і аналогічно

$$(x + H + y + H)(z + H) = (x + H)(z + H) + (y + H)(z + H);$$

$$\begin{aligned} (x + H)((y + H)(z + H)) &= (x + H)(yz + H) = x(yz) + H = \\ &= (xy)z + H = (xy + H)(z + H) = ((x + H)(y + H))(z + H); \end{aligned}$$

$$(e + H)(x + H) = ex + H = x + H = xe + H = (x + H)(e + H),$$

так що відносно цих операцій додавання і множення множина суміжних класів є кільцем.

Це кільце називається *фактор-кільцем кільця R за ідеалом H* і позначається символом R/H .

Відзначимо, якщо кільце R — комутативне, то кожне його фактор-кільце також комутативне.

Розглянемо відображення $\sigma_H: R \longrightarrow R/H$, що визначається рівністю $\sigma_H(x) = x + H$, $x \in R$. Тоді

$$\sigma_H(x + y) = x + y + H = x + H + y + H = \sigma_H(x) + \sigma_H(y);$$

$$\sigma_H(xy) = xy + H = (x + H)(y + H) = \sigma_H(x)\sigma_H(y).$$

Таким чином, як і у випадку груп, приходимо до відображень, що зберігають операції.

Нехай R, S — кільця. У відповідності з загальним означенням (розділ 9), відображення $f: R \longrightarrow S$ називається *кільцевим гомоморфізмом*, якщо воно задовольняє такі умови

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$

для довільних елементів $x, y \in R$.

Оскільки у цій частині ми будемо розглядати тільки кільця, то далі замість слів “кільцевий гомоморфізм” будемо писати просто “гомоморфізм”.

Бієктивний гомоморфізм називається ізоморфізмом.

Якщо $f: R \longrightarrow S$ — ізоморфізм, то, як було показано у розділі 9, $f^{-1}: S \longrightarrow R$ також буде ізоморфізмом. Кільця R і S називаються *ізоморфними*, якщо існує ізоморфізм одного з них на другий, цей факт ми будемо позначати так $R \cong S$.

Очевидно, тотожна підстановка $\varepsilon_R: R \longrightarrow R$ є ізоморфізмом.

Якщо $f: R \longrightarrow S$, $g: S \longrightarrow U$ — гомоморфізми, то добуток $g \circ f$ є також гомоморфізмом.

16.10. Пропозиція. Нехай R, S — кільця, $f: R \longrightarrow S$ — гомоморфізм.

$$(1) \quad f(O_R) = O_S.$$

$$(2) \quad f(-x) = -f(x) \text{ для будь-якого } x \in R.$$

$$(3) \quad \text{Якщо } H \text{ — підкільце } R, \text{ то його образ } f(H) \text{ буде підкільцем в } S. \text{ Зокрема, } f(R) = \text{Im } f \text{ — підкільце } S.$$

(4) Якщо V — підкілець S , то його повний прообраз $f^{-1}(V)$ — підкілець в R .

(5) Якщо V — ідеал S , то його повний прообраз $f^{-1}(V)$ — ідеал в R . Зокрема,

$$\text{Ker } f = \{x \in R \mid f(x) = O_S\} = f^{-1}(\langle O_S \rangle) \text{ — ідеал } R.$$

(6) $f(e)$ — одиничний елемент підкілець $\text{Im } f$.

(7) якщо R — комутативне, то $\text{Im } f$ — комутативне.

Доведення. Оскільки f — гомоморфізм адитивних груп R і S , то твердження (1), (2) випливають з пропозиції 14.2. Із цієї ж теореми випливає, що $f(H)$ — підгрупа адитивної групи S , а $f^{-1}(V)$ — підгрупа адитивної групи кільця R . Нехай $x, y \in H$, $a = f(x)$, $b = f(y)$, тоді $ab = f(x)f(y) = f(xy) \in f(H)$. Із теореми 15.4 випливає тепер, що $f(H)$ є підкілцем S .

Нехай $x, y \in f^{-1}(V)$, тоді $f(x), f(y) \in f^{-1}(V)$, і оскільки V — підкілець, то $f(x)f(y) = f(xy) \in V$, тобто $xy \in f^{-1}(V)$. З теореми 15.4 випливає тепер, що $f^{-1}(V)$ є підкілцем R . Таким чином, твердження (3), (4) також доведені.

Нехай тепер V — ідеал S , $x \in f^{-1}(V)$, $y \in R$, тоді $f(xy) = f(x)f(y) \in V$, тобто $xy \in f^{-1}(V)$. Аналогічно доводиться, що $yx \in f^{-1}(V)$, а це означає, що $f^{-1}(V)$ — ідеал кільця R , так що (5) доведено.

Якщо $a \in \text{Im } f$, то $a = f(x)$ для деякого $x \in R$, тому

$$a = f(x) = f(xe) = f(x)f(e) = af(e);$$

$$a = f(x) = f(ex) = f(e)f(x) = f(e)a,$$

тобто $f(e)$ — одиничний елемент $\text{Im } f$.

Нарешті, нехай R — комутативне, $a, b \in \text{Im } f$, $a = f(x)$, $b = f(y)$ для деяких $x, y \in R$. Тепер

$$ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba.$$

Ідеал $\text{Ker } f$ знову назвемо ядром гомоморфізму f .

Ін'єктивний гомоморфізм називається *мономорфізмом*; сюр'єктивний гомоморфізм називається *епіморфізмом*.

Гомоморфізм кільця R у себе називається *ендоморфізмом*. Ізоморфізм кільця R на себе називається *автоморфізмом*.

Як і для груп, доводяться такі твердження.

16.11. Теорема (теорема про мономорфізми). Нехай R, S — кільця. Гомоморфізм $f: R \longrightarrow S$ тоді і тільки тоді буде мономорфізмом, коли $\text{Ker } f = \langle O_R \rangle$. Якщо $f: R \longrightarrow S$ — мономорфізм, то $R \cong \text{Im } f$.

16.12. Теорема (теорема про епіморфізми). Нехай R, S — кільця, $f: R \longrightarrow S$ — епіморфізм. Тоді кілець S ізоморфне до фактор-кілець $R/\text{Ker } f$.

16.13. Теорема (теорема про гомоморфізми). Нехай R, S — кільця, $f: R \longrightarrow S$ — гомоморфізм. Тоді $R/\text{Ker } f \cong \text{Im } f \leq S$.

16.14. Наслідок (теорема про гомоморфізми для тіл). Нехай T, Z — тіла, $f: T \longrightarrow Z$ — ненульовий гомоморфізм (тобто $\text{Ker } f \neq T$). Тоді $f(e)$ — одиничний елемент Z , $\text{Im } f$ — підтіло Z і f — мономорфізм. Зокрема, T ізоморфне деякому підтілу Z .

Доведення. Дійсно, припустимо, що $f(e) = O_Z$. Для кожного елемента $x \in T$ маємо тоді

$$f(x) = f(xe) = f(x)f(e) = f(x)O_Z = O_Z,$$

що суперечить умовам про f . Таким чином, $f(e)$ — ненульовий елемент Z , і отже $f(e)$ має обернений в Z .

З визначення одиничного елемента отримуємо $f(e) = f(ee) = f(e)f(e)$, і помноживши обидві частини цієї рівності на елемент, обернений до $f(e)$, отримуємо, що $f(e) = e_Z$ — одиничний елемент Z . З пропозиції 16.10 випливає, що $\text{Im } f$ — підкільце Z , більш того, тільки що ми довели, що $\text{Im } f$ — унітарне підкільце Z . Нехай u — ненульовий елемент $\text{Im } f$, тоді $u = f(y)$ для деякого елемента y кільця R . Очевидно y — ненульовий елемент R , так що для нього існує обернений елемент y^{-1} . Покажемо, що елемент $v = f(y^{-1})$ буде оберненим до u , з теореми 15.10 буде впливати тоді, що $\text{Im } f$ — підтіло Z . Маємо

$$uv = f(y)f(y^{-1}) = f(yy^{-1}) = f(e) = e_Z,$$

$$vu = f(y^{-1})f(y) = f(y^{-1}y) = f(e) = e_Z.$$

За пропозицією 16.10, $\text{Ker } f$ — ідеал кільця R . Оскільки $\text{Ker } f \neq T$, то з наслідку 13.7 отримуємо рівність $\text{Ker } f = \{O_R\}$. Залишається застосувати теорему 16.11.

Розглянемо тепер деякі застосування отриманих результатів.

Характеристика кільця. Нехай R — кільце, розглянемо відображення $f: Z \longrightarrow R$, що задається правилом $f(n) = ne$, $n \in Z$. Очевидно,

$$f(n+k) = (n+k)e = ne + ke = f(n) + f(k),$$

$$f(nk) = (nk)e = n(ke) = (ne)(ke) = f(n)f(k)$$

для всіх $n, k \in Z$.

З пропозиції 16.10 випливає, що $\text{Im } f = \{ne \mid n \in Z\} = Ze$ — підкільце R . Із теореми 16.13 отримуємо, що $Ze = \text{Im } f \cong Z/\text{Ker } f$. Оскільки $\text{Ker } f$ — ідеал кільця Z за пропозицією 16.10, то з опису ідеалів кільця Z маємо $\text{Ker } f = nZ$, де $n \geq 0$.

Якщо $\text{Ker } f = \langle 0 \rangle$, то $Ze \cong Z$. У цьому випадку будемо говорити, що кільце R має характеристику 0 і писати $\text{char } R = 0$. Це означає також, що одиничний елемент e має в адитивній групі кільця R нескінченний порядок.

Якщо $\text{Ker } f = nZ$, де $n > 0$, то $Ze \cong Z/nZ$. У цьому випадку будемо говорити, що кільце R має характеристику n і писати $\text{char } R = n$.

Це означає, що одиничний елемент e має в адитивній групі кільця R порядок n . Якщо a — довільний елемент R , то $na = (ne)a = O_R a = O_R$, так що порядок кожного елемента (в адитивній групі кільця) є дільником числа n .

Якщо n не є простим числом, то $n = kt$, де $1 < k < n$, $1 < t < n$. Зокрема, $k, t \notin n\mathbb{Z}$, тому $ke \neq O_R$, $te \neq O_R$. Разом із тим

$$(ke)(te) = (kt)e = ne = O_R.$$

Таким чином, якщо $\text{char } R$ не є простим числом, то кільце R містить дільники нуля. Звідси випливає твердження:

16.15. Пропозиція. *Якщо кільце R не має дільників нуля, то або $\text{char } R = 0$, або $\text{char } R = p$, де p — просте число. Зокрема, якщо T — тіло, то або $\text{char } T = 0$, або $\text{char } T = p$, де p — просте число.*

Розглянемо зараз будову простих підтіл.

16.16. Пропозиція. *Якщо T — тіло, тоді його центр $z(T)$ є підполем.*

Доведення. Оскільки $O_T, e \in \zeta(T)$, то $\zeta(T)$ — ненульова підмножина T . Уже відзначалося, що $\zeta(T)$ — підкільце T , зокрема, умови (SF 1) і (SF 2) виконані для $\zeta(T)$. Нехай $O_T \neq x \in \zeta(T)$, y — довільний елемент T . Тоді $yx = xy$. Маємо

$$\begin{aligned} yx^{-1} &= eyx^{-1} = (x^{-1}x)yx^{-1} = x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1} = \\ &= (x^{-1}y)(xx^{-1}) = (x^{-1}y)e = x^{-1}y. \end{aligned}$$

Ця рівність показує, що $x^{-1} \in \zeta(T)$, тобто умова (SF 3) також виконана.

16.17. Наслідок. *Просте підтіло T_0 тіла T є його підполем.*

Наведемо тепер приклади простих полів.

Поле $\mathbb{Q}$ раціональних чисел. Нехай P — деяке підполе $\mathbb{Q}$. З (SF 2) випливає, що $1 \in P$. Оскільки P — підкільце $\mathbb{Q}$, то для будь-якого $r \in \mathbb{Z}$ маємо $r1 = r \in P$. Якщо $0 \neq k \in P$ і $k \in \mathbb{Z}$, то із (SF 3) отримуємо, що $1/k \in P$. Тепер для всіх $r, k \in \mathbb{Z}$, $k \neq 0$, маємо $r/k = r(1/k) \in P$. Це співвідношення доводить рівність $P = \mathbb{Q}$.

Поле $F_p = \mathbb{Z}/p\mathbb{Z}$, де p — просте число. Покажемо спочатку, що фактор-кільце $\mathbb{Z}/p\mathbb{Z}$ є полем. Нехай $p\mathbb{Z} \neq x + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$. Оскільки $x \notin p\mathbb{Z}$, то числа x і p взаємно прості. Тому знайдуться такі цілі числа k, r , що $xk + pr = 1$. Тепер маємо

$$1 + p\mathbb{Z} = xk + pr + p\mathbb{Z} = xk + p\mathbb{Z} = (x + p\mathbb{Z})(k + p\mathbb{Z}).$$

Якщо P — підполе F_p , то P — підкільце F_p , а тому адитивна група P є підгрупою адитивної групи F_p . Із теореми Лагранжа (наслідок 12.5) одержуємо тепер, що $|P|$ ділить $|F_p| = p$. Оскільки p — просте число і $|P| \geq 2$, то це означає, що $|P| = p$. Отже, $P = F_p$.

Наступна теорема свідчить, що інших прикладів простих тіл немає.

16.18. Теорема. Нехай T — тіло, T_0 — його просте підтіло.

(1) Якщо $\text{char } T = p$ — просте число, то $T_0 \cong F_p$.

(2) Якщо $\text{char } T = 0$, $T_0 \cong \mathbb{Q}$.

Д о в е д е н н я . Знову розглянемо відображення $f: Z \rightarrow T$, що задається правилом $f(n) = ne$, $n \in Z$. Як було показано вище, це відображення є гомоморфізмом. Якщо $\text{char } T = p$ — просте число, то $\text{Ker } f = pZ$. Відображення $\psi: Z/pZ \rightarrow T$, що визначається за правилом $\psi(n + pZ) = f(n)$, $n \in Z$, також буде гомоморфізмом, і цей гомоморфізм буде ненульовим, оскільки $\psi(1 + pZ) = f(1) = e \neq O_T$. Очевидно, $\text{Im } \psi = \text{Im } f = Ze$, і залишається застосувати пропозицію 16.14.

Нехай тепер $\text{char } T = 0$. У цьому випадку $\text{Ker } f = \langle 0 \rangle$, тобто f — мономорфізм за теоремою 16.11. Оскільки $e \in T_0$, то Ze — підкільце T_0 . Розширимо наступним чином відображення f до відображення $f_1: \mathbb{Q} \rightarrow T$. Нехай m/n — довільний елемент $\mathbb{Q}$, тоді $n \neq 0$, і отже $f(n) = ne \neq O_T$. Оскільки T — тіло, його ненульовий елемент ne має в T обернений. Тепер покладемо $f_1(m/n) = (me)(ne)^{-1}$. Покажемо, що f_1 визначено коректно, нехай $k/t = m/n$. Маємо тепер наступний ланцюжок рівностей:

$$\begin{aligned} kn = tm &\Rightarrow (ke)(ne) = (te)(me) \Rightarrow (me)(ne)^{-1} = (ke)(te)^{-1} \Rightarrow \\ &\Rightarrow f_1(m/n) = (me)(ne)^{-1} = (ke)(te)^{-1} = f_1(k/t), \end{aligned}$$

так що визначення f_1 є коректним. Відображення f_1 продовжує f : якщо $n \in Z$, то $n = nk/k$ для довільного $0 \neq k \in Z$, отже

$$f_1(n) = f_1(nk/k) = (nke)(ke)^{-1} = (ne)(ke)(ke)^{-1} = ne = f(n).$$

Відображення f_1 є гомоморфізмом:

$$\begin{aligned} f_1((m/n) + (k/t)) &= f_1((mt + kn)/(nt)) = ((mt + kn)e)((nt)e)^{-1} = \\ &= ((mt)e + (kn)e)((ne)(te))^{-1} = ((me)(te) + (ke)(ne))(ne)^{-1}(te)^{-1} = \\ &= (me)(te)(ne)^{-1}(te)^{-1} + (ke)(ne)(ne)^{-1}(te)^{-1} = \\ &= (me)(ne)^{-1} + (ke)(te)^{-1} = f_1(m/n) + f_1(k/t); \\ f_1((m/n) (k/t)) &= f_1((mk)/(nt)) = ((mk)e)((nt)e)^{-1} = \\ &= ((me)(ke)((ne)(te))^{-1} = (me)(ke)(ne)^{-1}(te)^{-1} = \\ &= (me)(ne)^{-1}(ke)(te)^{-1} = f_1(m/n) f_1(k/t). \end{aligned}$$

За наслідком 16.14 $\mathbb{Q} \cong \text{Im } f_1$, а оскільки $\text{Im } f_1$ — підполе T , то $\text{Im } f_1 \geq T_0$. З іншого боку, $ne \in T_0$ для кожного $n \in Z$, і якщо $n \neq 0$, то $(ne)^{-1} \in T_0$, отже $(me)(ne)^{-1} \in T_0$ для кожної пари $m, n \in Z$, $n \neq 0$. Таким чином, навпаки $\text{Im } f_1 \leq T_0$, а тому $\text{Im } f_1 = T_0$.

Наступний результат дає можливість отримувати розширення кілець.

16.19. Теорема. Нехай R, K — кільця, $f: R \longrightarrow K$ — мономорфізм. Тоді існує кільце S , ізоморфне K , яке містить R як підкільце. Якщо e_R, e_K — одиничні елементи кілець R та K відповідно і $f(e_R) = e_K$, то e_R — одиничний елемент S . Наприклад, якщо R та K — тіла, то R — підтіло S .

Доведення. Можна вважати, що $K \cap R = \emptyset$, якщо це не так, то замість K розглянемо його ізоморфний образ, що має пустий перетин з R . Наприклад, покладемо $K_1 = K \times \{1\}$ і визначимо операції за правилом

$$(x, 1) + (y, 1) = (x + y, 1); (x, 1)(y, 1) = (xy, 1).$$

Нехай $U = \text{Im } f$. З теореми 16.11 випливає, що U — підкільце K і U ізоморфне R . Нехай $A = K \setminus U$, $S = R \cup U$. Задамо відображення $g: S \longrightarrow K$ правилом

$$g(x) = \begin{cases} f(x), & \text{якщо } x \in R, \\ x, & \text{якщо } x \in A. \end{cases}$$

Неважко перевірити, що g — бієкція S на K . Визначимо тепер операції $+$ і $\times$ в S за правилом

$$x + y = g^{-1}(g(x) + g(y)), \quad x \times y = g^{-1}(g(x)g(y))$$

для будь-яких $x, y \in S$. З цього означення випливає, що

$$g(x + y) = g(g^{-1}(g(x) + g(y))) = g(x) + g(y),$$

$$g(x \times y) = g(g^{-1}(g(x)g(y))) = g(x)g(y).$$

Тепер будемо мати

$$x + y = g^{-1}(g(x) + g(y)) = g^{-1}(g(y) + g(x)) = y + x;$$

$$\begin{aligned} (x + y) + z &= g^{-1}(g(x + y) + g(z)) = g^{-1}(g(x) + g(y) + g(z)) = \\ &= g^{-1}(g(x) + (g(y) + g(z))) = g^{-1}(g(x) + g(y + z)) = x + (y + z); \end{aligned}$$

$$(x + O_R) = g^{-1}(g(x) + g(O_R)) = g^{-1}(g(x) + O_K) = g^{-1}(g(x)) = x;$$

якщо $x \in R$, то

$$x + (-x) = g^{-1}(g(x) + g(-x)) = g^{-1}(g(x + (-x))) = g^{-1}(g(O_R)) = O_R.$$

Якщо $x \in A$, то $-x \notin U$, бо U — підкільце; тому

$$x + (-x) = g^{-1}(g(x) + g(-x)) = g^{-1}(x + (-x)) = g^{-1}(O_K) = O_R.$$

Таким чином, відносно операції додавання S є абелевою групою.

Далі

$$\begin{aligned}(x + y) \times z &= g^{-1}(g(x + y)) g(z) = g^{-1}(g(x) + g(y)) g(z) = \\&= g^{-1}(g(x) g(z) + g(y) g(z)) = g^{-1}(g(x \times z) + g(y \times z)) = \\&= g^{-1}(g(x \times z) + g(y \times z)) = (x \times z) + (y \times z).\end{aligned}$$

Аналогічно доводиться рівність

$$x \times (y + z) = (x \times y) + (x \times z).$$

Продовжуємо перевірку:

$$\begin{aligned}(x \times y) \times z &= g^{-1}(g(x \times y)) g(z) = g^{-1}(g(x) g(y)) g(z) = \\&= g^{-1}(g(x) (g(y) g(z))) = g^{-1}(g(x) g(y \times z)) = x \times (y \times z);\end{aligned}$$

$$x \times g^{-1}(e_K) = g^{-1}(g(x) g^{-1}(g(e_K))) = g^{-1}(g(x) e_K) = g^{-1}(g(x)) = x;$$

$$g^{-1}(e_K) \times x = g^{-1}(g^{-1}(g(e_K)) g(x)) = g^{-1}(e_K g(x)) = g^{-1}(g(x)) = x,$$

так що $g^{-1}(e_K)$ — одиничний елемент кільця S . Зокрема, якщо $f(e_R) = g(e_R) = e_K$, то e_R — одиничний елемент кільця S . Таким чином, S — кільце.

Уже було показано, що

$$g(x + y) = g(x) + g(y), g(x \times y) = g(x) g(y),$$

і тому g — ізоморфізм.

Якщо $x, y \in R$, то

$$\begin{aligned}x + y &= g^{-1}(g(x) + g(y)) = g^{-1}(f(x) + f(y)) = g^{-1}(f(x + y)) = \\&= g^{-1}(g(x + y)) = x + y;\end{aligned}$$

$$x \times y = g^{-1}(g(x)g(y)) = g^{-1}(f(x)f(y)) = g^{-1}(f(xy)) = g^{-1}(g(xy)) = xy,$$

тобто звуження нових операцій на R збігаються з початковими операціями на R . З теореми 15.4 випливає також, що R — підкільце в S .

Нарешті, нехай R, K — тіла. Теорема 15.10 показує, що залишилось тільки перевірити умову (SF 3). Якщо x — ненульовий елемент R , то він має обернений в R . Оскільки одиничний елемент R є також одиничним елементом S , то цей обернений буде оберненим до x і в тілі S .

Ця теорема показує, що для побудови деякого розширення E кільця R достатньо побудувати мономорфізм кільця R у яке-небудь кільце K , що ізоморфне E . Визначимо деякі застосування здобутих результатів.

У розділі 15 ми домовилися розглядати тільки кільця, в яких є одиничний елемент. Наступна теорема дає обґрунтування для цієї домовленості.

16.20. Теорема. Для кожного кільця R існує кільце K з одиницею, яке містить R як підкільце.

Доведення. Якщо кільце R має одиничний елемент, то все доведено. Тому припустимо, що одиничного елемента R не має. З огляду на теорему 16.19 досить побудувати мономорфізм $f: R \rightarrow K$, де K — кільце з одиницею.

Нехай $K = R \times \mathbb{Z}$, задамо операції у K правилами

$$(x, n) + (y, k) = (x + y, n + k),$$

$$(x, n)(y, k) = (xy + kx + ny, nk)$$

для всіх $x, y \in R, n, k \in \mathbb{Z}$.

Оскільки додавання в K зводиться до додавання в R і $\mathbb{Z}$, то воно успадковує властивості додавання в R і $\mathbb{Z}$. Зокрема, K є абелевою групою. При цьому

$$O_K = (O_R, 0), -(x, n) = (-x, -n).$$

Далі

$$\begin{aligned} ((x, n) + (y, k))(z, m) &= (x + y, n + k)(z, m) = \\ &= ((x + y)z + (n + k)z + m(x + y), (n + k)m) = \\ &= (xz + yz + nz + kz + mx + my, nm + km), \end{aligned}$$

$$\begin{aligned} (x, n)(z, m) + (y, k)(z, m) &= (xz + nz + mx, nm) + (yz + \\ &+ kz + my, km) = (xz + nz + mx + yz + kz + my, nm + km), \end{aligned}$$

тобто

$$((x, n) + (y, k))(z, m) = (x, n)(z, m) + (y, k)(z, m).$$

Аналогічно доводиться рівність

$$(x, n)((y, k) + (z, m)) = (x, n)(y, k) + (x, n)(z, m).$$

Множення в K асоціативне:

$$\begin{aligned} ((x, n)(y, k))(z, m) &= (xy + ny + kx, nk)(z, m) = \\ &= ((xy + ny + kx)z + m(xy + ny + kx) + (nk)z, (nk)m) = \\ &= ((xy)z + n(yz) + k(xz) + m(xy) + (mn)y + (mk)x + (nk)z, (nk)m); \\ (x, n)((y, k)(z, m)) &= (x, n)(yz + kz + my, km) = \\ &= (x(yz + kz + my) + n(yz + kz + my) + (km)x, n(km)) = \\ &= (x(yz) + k(xz) + m(xy) + n(yz) + (nk)z + (nm)y + (km)x, n(km)). \end{aligned}$$

Оскільки множення в R і Z асоціативне, то

$$((x, n)(y, k))(z, m) = (x, n)((y, k)(z, m)).$$

Нарешті,

$$(x, n)(O_R, 1) = (x, n) = (O_R, 1)(x, n),$$

таким чином, $(O_R, 1)$ — одиничний елемент кільця K .

Задамо тепер відображення $f: R \longrightarrow K$ за правилом $f(x) = (x, 0)$, $x \in R$. Очевидно,

$$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y);$$

$$f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)f(y)$$

для будь-яких $x, y \in R$, а також $\text{Ker } f = \langle O_R \rangle$. Таким чином, f — шуканий мономорфізм.

У теоремі 14.12 відзначалось, що будь-яка група вкладається в групу підстановок деякої множини. Наступна теорема показує, що для кілець роль такого «універсального об'єкта» відіграють кільця ендоморфізмів абелевих груп.

16.21. Теорема. Для кожного кільця R існує мономорфізм у кільце ендоморфізмів деякої абелевої групи.

Д о в е д е н н я . На підставі теореми 16.20 можна вважати, що кільце R має одиничний елемент. Нехай $a \in R$, розглянемо відображення $\tau_a: R \longrightarrow R$, що визначається рівністю $\tau_a(x) = ax$, $x \in R$. Маємо

$$\tau_a(x + y) = a(x + y) = ax + ay = \tau_a(x) + \tau_a(y),$$

і це означає, що τ_a — ендоморфізм адитивної групи кільця R .

Розглянемо тепер відображення $f: R \longrightarrow \text{End } R$, яке задається правилом $f(a) = \tau_a$, для кожного $a \in R$. Якщо $x \in R$, то

$$\tau_{a+b}(x) = (a + b)x = ax + bx = \tau_a(x) + \tau_b(x) = (\tau_a + \tau_b)(x);$$

$$\tau_{ab}(x) = (ab)x = a(bx) = \tau_a(bx) = \tau_a(\tau_b(x)) = \tau_a \circ \tau_b(x).$$

Звідси випливають рівності

$$f(a + b) = \tau_{a+b} = \tau_a + \tau_b = f(a) + f(b);$$

$$f(ab) = \tau_{ab} = \tau_a \circ \tau_b = f(a) \circ f(b)$$

для будь-яких $a, b \in R$. Ці рівності показують, що f — гомоморфізм. Нарешті, якщо $a \neq b$, то

$$\tau_a(e) = ae = a \neq b = be = \tau_b(e),$$

так що $f(a) = \tau_a \neq \tau_b = f(b)$. Тому f — шуканий мономорфізм.

17. КІЛЬЦЯ ПОЛІНОМІВ ТА ФОРМАЛЬНИХ СТЕПЕНЕВИХ РЯДІВ

Кільце поліномів є одним із самих старих та добре вивчених кілець. Це одне з самих важливих кілець, його роль у теорії комутативних кілець подібна до ролі груп підстановок для теорії скінченних груп. В термінах поліномів формулюються та вирішуються найрізноманітніші проблеми не тільки в алгебрі, а і в багатьох інших математичних дисциплінах. Розглянемо одну задачу, що приводить до цього кільця. Нехай K — комутативне кільце, R — його унітарне цілісне підкільце, M — підмножина K . Розглянемо сукупність M тих підкілець, які містять у собі як підкільце R , так і підмножину M . Нехай $R[M] = \cap M$. За наслідком 15.5 $R[M]$ — підкільце. З його означення випливає, що $R[M]$ — найменше підкільце, яке містить у собі підкільце R і підмножину M . Будемо говорити, що $R[M]$ — *підкільце, породжене над R підмножиною M* .

Найпростіший випадок, коли M складається з єдиного елемента y . У цьому випадку замість $R[M]$ будемо писати $R[y]$. З'ясуємо, з яких елементів складається $R[y]$. З теореми 15.4 випливає, що $y^n \in R[y]$ для кожного $n \in N$. З цієї ж теореми отримуємо, що $ay^n \in R[y]$ для кожного $a \in R$, і отже, усі можливі суми вигляду

$$a_0 + a_1y + a_2y^2 + \dots + a_ny^n \text{ (поліноми від } y),$$

де $a_0, a_1, a_2, \dots, a_n \in R$, містяться в $R[y]$. Більш того, покажемо, що всі ці суми вичерпують підкільце $R[y]$. Дійсно дві довільні такі суми $(a_0 + a_1y + a_2y^2 + \dots + a_ny^n)$ і $(b_0 + b_1y + b_2y^2 + \dots + b_ky^k)$ та нехай, для визначеності, $n \geq k$. Маємо

$$\begin{aligned} & (a_0 + a_1y + a_2y^2 + \dots + a_ny^n) + (b_0 + b_1y + b_2y^2 + \dots + b_ky^k) = \\ &= (a_0 + b_0) + (a_1 + b_1)y + b_2y^2 + \dots + (a_k + b_k)y^k + a_{k+1}y^{k+1} + \dots + a_ny^n; \\ & (a_0 + a_1y + a_2y^2 + \dots + a_ny^n) (b_0 + b_1y + b_2y^2 + \dots + b_ky^k) = \\ &= (a_0 + b_0) + (a_0b_1 + a_1b_0)y + (a_0b_2 + a_1b_1 + a_2b_0)y^2 + \dots + a_nb_ky^{n+k}. \end{aligned}$$

З теореми 15.4 отримуємо, що всі такі суми утворюють підкільце. Оскільки воно містить у собі як R , так і y , то воно співпадає з $R[y]$. Слід відзначити, що y — деякий елемент кільця K , тому різні за виглядом поліноми від y можуть співпадати. Тому, щоб прийти до звичного поняття поліному, слід звільнитися від усіх подібних співвідношень. На цій дорозі і з'являється поняття “невідомої”. Але, у свою чергу, тут ми мусимо якось її визначити. Тому ми віддамо перевагу іншому підходу, де основний акцент переноситься на операції над поліномами, що виникли вище. Кожен поліном повністю визначається заданням своїх коефіцієнтів. З набору коефіцієнтів та операцій і будемо виходити. Більш того, кільце поліномів ми отримаємо як підкільце у деякому більшому кільці — кільці формальних степеневих рядів.

Нехай R — область цілісності. Розглянемо множину $R[[X]]$ (поки що це просто формальне позначення) усіх послідовностей :

$$(a_n)_{n \in N_0} = (a_0, a_1, \dots, a_n, \dots),$$

що складаються з елементів кільця R .

Дві послідовності $(a_n)_{n \in N_0}$ та $(b_n)_{n \in N_0}$ називаються рівними, якщо $a_n = b_n$ для кожного $n \in N_0$.

Операції додавання й множення послідовностей задаються правилами, що були вже вказані вище, а саме:

$$(a_n)_{n \in N_0} + (b_n)_{n \in N_0} = (c_n)_{n \in N_0},$$

де $c_n = a_n + b_n$ для кожного $n \in N_0$;

$$(a_n)_{n \in N_0} (b_n)_{n \in N_0} = (d_n)_{n \in N_0},$$

де $d_n = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0 = \sum_{0 \leq j \leq n} a_j b_{n-j} = \sum_{j+k=n} a_j b_k$ для кожного $n \in N_0$.

Додавання послідовностей зводиться до додавання відповідних елементів кільця R , через це неважко впевнитися в тому, що воно комутативне і асоціативне. Нульовим елементом, очевидно, буде послідовність

$$0 = (0_R, 0_R, \dots, 0_R, \dots).$$

Для кожної послідовності $(a_n)_{n \in N_0}$ існує протилежний елемент — це послідовність $(-a_n)_{n \in N_0}$. Таким чином, для операції додавання виконані всі аксіоми абелевої групи.

Неважко впевнитися в тому, що множення послідовностей комутативне, тому треба доводити тільки один закон дистрибутивності:

$$((a_n)_{n \in N_0} + (b_n)_{n \in N_0}) (c_n)_{n \in N_0} = (a_n)_{n \in N_0} (b_n)_{n \in N_0} + (a_n)_{n \in N_0} (c_n)_{n \in N_0}.$$

Позначимо

$$(u_n)_{n \in N_0} = ((a_n)_{n \in N_0} + (b_n)_{n \in N_0}) (c_n)_{n \in N_0},$$

$$(v_n)_{n \in N_0} = (a_n)_{n \in N_0} (b_n)_{n \in N_0} + (a_n)_{n \in N_0} (c_n)_{n \in N_0}.$$

Маємо для будь-якого $n \in N_0$

$$u_n = e_{j+k=n} (a_j + b_j) c_k = e_{j+k=n} a_j c_k + e_{j+k=n} b_j c_k;$$

$$v_n = e_{j+k=n} a_j c_k + e_{j+k=n} b_j c_k.$$

Тобто $u_n = v_n$ при кожному $n \in N_0$, таким чином, дистрибутивний закон доведено.

Множення асоціативне:

$$((a_n)_{n \in N_0} (b_n)_{n \in N_0}) (c_n)_{n \in N_0} = (a_n)_{n \in N_0} ((b_n)_{n \in N_0} (c_n)_{n \in N_0}).$$

Дійсно, нехай

$$((a_n)_{n \in N_0} (b_n)_{n \in N_0}) (c_n)_{n \in N_0} = (w_n)_{n \in N_0},$$

$$(a_n)_{n \in N_0} ((b_n)_{n \in N_0} (c_n)_{n \in N_0}) = (z_n)_{n \in N_0}.$$

Маємо тепер при довільному $n \in N_0$

$$w_n = \sum_{m+t=n} \left(\sum_{j+k=m} a_j b_k \right) c_t = \sum_{m+j+k=n} (a_j b_k) c_t;$$

$$z_n = \sum_{j+m=n} a_j \left(\sum_{k+t=m} a_k b_t \right) c_t = \sum_{m+j+k=n} a_j (b_k c_t).$$

Тобто $w_n = z_n$ при кожному $n \in N_0$, таким чином, асоціативність множення доведена.

Відносно операції множення існує одиничний елемент, це, як неважко показати,

$$e = (e, O_R, \dots, O_R, \dots).$$

Таким чином, $R[[X]]$ — комутативне кільце з одиницею. Більш того, $R[[X]]$ — область цілісності. Насправді, нехай $(a_n)_{n \in N_0} \neq O$, $(b_n)_{n \in N_0} \neq O$. Тоді знайдуться такі індекси j, k , що $a_j \neq O_R$, але $a_n = O_R$ при $0 \leq n < j$, $b_k \neq O_R$, але $b_n = O_R$ при $0 \leq n < k$. Якщо $(a_n)_{n \in N_0} (b_n)_{n \in N_0} = (d_n)_{n \in N_0}$, то

$$d_{j+k} = a_0 b_{j+k} + \dots + a_{j-1} b_{k+1} + a_j b_k + a_{j+1} b_{k-1} + \dots + a_{j+k} b_0 = a_j b_k \neq O_R.$$

Послідовність $(a_n)_{n \in N_0}$ назвемо поліномом, якщо знайдеться таке число t , що $a_n = O_R$ при $n \geq t$. Степенем полінома $(a_n)_{n \in N_0}$ називають таке число m , що $a_m \neq O_R$, але $a_n = O_R$ при $n > m$. При цьому a_m називають старшим коефіцієнтом полінома. Якщо $a_n = O_R$ для будь-якого $n \in N_0$, то ніякого степеня полінома не присвоюють, іноді нульовому елементу присвоюють степені $-\infty$.

Підмножину всіх поліномів позначимо через $R[X]$. Нехай $(a_n)_{n \in N_0}, (b_n)_{n \in N_0}$ — два поліноми і m, t — такі числа, що $a_m \neq O_R$, але $a_n = O_R$ при $n > m$, $b_t \neq O_R$, але $b_n = O_R$ при $n > t$.

Тоді $a_n b_n = O_R$ при $n > \max\{m, t\}$; $a_0 b_n + a_1 b_{n-1} + \dots + a_j b_{n-j} + \dots + a_n b_0 = O_R$ при $n > m = t$. З теореми 15.4 випливає, що $R[X]$ — підкільце кільця $R[[X]]$. Очевидно також, що $R[X]$ — унітарне підкільце.

Нехай $X = (O_R, e, O_R, \dots, O_R, \dots)$. З означення множення одержуємо тепер рівність

$$\begin{aligned} X^n &= (O_R, O_R, \dots, O_R, e, O_R, \dots, O_R, \dots). \\ &\quad \downarrow \\ &\quad n \end{aligned}$$

Для довільного елемента $a \in R$ позначимо $\bar{a} = (a, O_R, O_R, \dots, O_R, \dots)$. Тоді

$$\begin{aligned} \bar{a} X^n &= (O_R, O_R, \dots, O_R, a, O_R, \dots, O_R, \dots). \\ &\quad \downarrow \\ &\quad n \end{aligned}$$

Нехай тепер $(a_n)_{n \in N_0}$ — поліном степеня m . Тепер ми маємо змогу можна переписати його в звичайному вигляді:

$$\begin{aligned}(a_n)_{n \in N_0} &= (a_0, O_R, O_R, \dots, O_R, O_R, O_R, \dots) + \\ &+ (O_R, a_1, O_R, \dots, O_R, O_R, O_R, \dots) + \dots + \\ &+ (O_R, O_R, O_R, \dots, O_R, a_m, O_R, \dots) = \bar{a}_0 + \bar{a}_1 X + \dots + \bar{a}_m X^m.\end{aligned}$$

Далі,

$$\bar{a} + \bar{b} = (a + b, O_R, \dots, O_R, \dots) = \overline{a + b};$$

$$\bar{a} \bar{b} = (a b, O_R, \dots, O_R, \dots) = \overline{ab}.$$

Ці рівності показують, що відображення $a \longrightarrow \bar{a}$, $a \in R$, є гомоморфізмом R в $R[[X]]$. Очевидно, цей гомоморфізм є бієктивним, тобто він є мономорфізмом. Зокрема, R і його образ ізоморфні. Оскільки в алгебрі ізоморфні об'єкти ототожнюються, ми можемо ототожнити R з його образом і замість $\bar{a}$ писати a , так що приходимо до звичайного запису полінома $f(X) = a_0 + a_1 X + \dots + a_m X^m$. Надалі степінь полінома $f(X)$ будемо позначати через $\deg f(X)$. З уже відзначеного вище випливають співвідношення

$$\deg(f(X) \pm g(X)) \leq \max\{\deg f(X), \deg g(X)\},$$

$$\deg(f(X) g(X)) = \deg f(X) + \deg g(X).$$

З другої рівності одразу випливає, що $U(R[X]) = U(R)$. Також з цієї рівності випливає, що $R[X]$ не має дільників нуля.

Повернемося тепер до формальних степеневих рядів. Зокрема, отримаємо і для них запис у вигляді нескінченної суми. Для випадку довільного кільця ми не маємо поняття границі послідовності, тому тут буде необхідно зробити деякі домовленості, щоб мати можливість додавати нескінченну множину послідовностей.

Набір $\{A_j \mid j \in N_0\}$ послідовностей $A_j = (a_{jn})_{n \in N_0}$ називається сумовим, якщо для будь-якого $n \in N_0$ множина $\{a_{jn} \mid j \in N_0\}$ містить тільки скінченну підмножину ненульових елементів. У цьому випадку сумою $\sum_{j \in N_0} A_j$ набору послідовностей $\{A_j \mid j \in N_0\}$ називають послідовність $(b_n)_{n \in N_0}$, де b_n — це сума тих елементів множини $\{a_{jn} \mid j \in N_0\}$, які відмінні від нуля.

Прокоментуємо це означення. Щоб з'ясувати, чи буде набір послідовностей $\{a_j \mid j \in N_0\}$ сумовим, треба подумки записати ці послідовності одну під однією і перевірити, чи буде кожен стовпчик цієї нескінченної матриці містити лише скінченну множину ненульових елементів. Підсумовувати таку послідовність треба по стовпчиках, додаючи тільки ненульові елементи кожного стовпчика. Тепер

$$\begin{aligned}(a_n)_{n \in N_0} &= (a_0, O_R, O_R, \dots, O_R, O_R, O_R, \dots) + \\ &+ (O_R, a_1, O_R, \dots, O_R, O_R, O_R, \dots) + \dots + \\ &+ (O_R, O_R, O_R, \dots, O_R, a_m, O_R, \dots) + \dots\end{aligned}$$

Це показує, що набір $\{a_n X^n \mid n \in N_0\}$ є сумовим і його сума дорівнює $(a_n)_{n \in N_0}$. Таким чином, і для формального степеневих ряду $(a_n)_{n \in N_0}$ отримуємо звичний запис у вигляді $\sum_{n \in N_0} a_n X^n$.

Нарешті, з'ясуємо, з яких рядів складається група $U(R[[X]])$. Нехай $f(X) = \sum_{n \in N_0} a_n X^n$, $g(X) = \sum_{n \in N_0} b_n X^n$ і припустимо, що $f(X)g(X) = e$. Звідси одразу ж випливає, що $a_0 b_0 = e$, тобто $a_0 \in U(R)$.

Навпаки, припустимо, що $a_0 \in U(R)$. Якщо з рівності $f(X)g(X) = e$ можна визначити всі коефіцієнти ряду $g(X)$, то це буде означати, що $f(X) \in U(R[[X]])$. Маємо $a_0 b_0 = e$, тобто $b_0 = a_0^{-1}$. Далі, $a_0 b_1 + a_1 b_0 = 0_R$. Звідси $b_1 = -a_1 a_0^{-2}$. Припустимо, що коефіцієнти $b_0, b_1, \dots, b_n$ уже визначені. Тоді коефіцієнт b_{n+1} можна визначити з рівності

$$a_0 b_{n+1} + a_1 b_n + \dots + a_n b_1 + a_{n+1} = 0_R,$$

а саме:

$$b_{n+1} = (-a_1 b_n - \dots - a_n b_1 - a_{n+1}) a_0^{-1}.$$

Таким чином, група $U(R[[X]])$ складається з тих і тільки тих рядів $\sum_{n \in N_0} a_n X^n$, у яких $a_0 \in U(R)$. Зокрема, якщо R — поле, то $U(R[[X]])$ складається з тих і тільки тих рядів $\sum_{n \in N_0} a_n X^n$, у яких $a_0 \neq 0_R$.

Розглянемо зараз питання про ідеали в кільцях поліномів на формальних степеневих рядах. Будову ідеалів у кільці поліномів отримуємо з наступної важливої теореми.

17.1. Теорема. Нехай F — поле, $f(X), g(X) \in F[X]$, причому $g(X) \neq 0_F$.

Тоді знайдуться такі поліноми $q(X), r(X) \in F[X]$, що $f(X) = q(X)g(X) + r(X)$, де або $r(X) = 0_F$ або $\deg r(X) < \deg g(X)$. Таке представлення полінома $f(X)$ є єдиним.

Доведення. Нехай

$$f(X) = a_0 + a_1 X + \dots + a_n X^n,$$

$$g(X) = b_0 + b_1 X + \dots + b_k X^k,$$

де $b_k \neq 0_F$. Застосуємо індукцію за числом n . Якщо $\deg g(X) > \deg f(X)$, то покладемо $r(X) = f(X)$, $q(X) = 0_F$. Тому розглянемо випадок, коли $\deg g(X) \leq \deg f(X)$. Якщо $\deg f(X) = 0$, то $r(X) = 0_F$, $q(X) = a_0 b_0^{-1}$. Нехай тепер $n > 0$ і припустимо, що теорема доведена для поліномів, степінь яких менша ніж n . Поліном $a_n b_k^{-1} X^{n-k} g(X)$ має степінь n і коефіцієнт його при X^n дорівнює a_n . Тому степінь полінома $f(X) - a_n b_k^{-1} X^{n-k} g(X) = f_1(X)$ уже менша від n . З урахуванням індуктивного припущення $f_1(X) = q_1(X)g(X) + r(X)$, де або $r(X) = 0_F$, або $\deg r(X) < \deg g(X)$. Тепер $f(X) = q(X)g(X) + r(X)$, де $q(X) = q_1(X) + a_n b_k^{-1} X^{n-k}$.

Нехай маємо також вираз: $f(X) = q_2(X)g(X) + r_2(X)$, де або $r_2(X) = 0_F$, або $\deg r_2(X) < \deg g(X)$. Тоді

$$q(X)g(X) + r(X) = q_2(X)g(X) + r_2(X).$$

Звідси $g(X)(q(X) - q_2(X)) = r_2(X) - r(X)$. Поліном, розта-

шований у правій частині цієї рівності, або нульовий, або степінь його менша $\deg g(X)$. Якщо $q(X) - q_2(X) \neq 0_F$, то

$$\deg(g(X)(q(X) - q_2(X))) = \deg g(X) + \deg(q(X) - q_2(X)) \geq \deg g(X).$$

Це означає, що $q(X) - q_2(X) = 0_F$. Звідси виходить, що $r_2(X) = r(X)$.

17.2. Наслідок. Нехай F — поле. Тоді кожен ідеал кільця $F[X]$ є головним.

Доведення. Нехай H — ідеал кільця $F[X]$. Якщо $H = \{0_F\}$, то $H = 0_F F[X]$. Припустимо тепер, що H містить ненульові поліноми. Серед них виберемо поліном $g(X)$ найменшого можливого степеня. Нехай $f(X)$ — довільний елемент H . З теореми 17.1 отримуємо розклад $f(X) = q(X)g(X) + r(X)$, де або $r(X) = 0_F$, або $\deg r(X) < \deg g(X)$. Якщо припустити, що $r(X) \neq 0_F$, то $r(X) = f(X) - q(X)g(X) \in H$. Але це суперечить вибору полінома $g(X)$. Одержана суперечність показує, що $r(X) = 0_F$, тобто $f(X) = q(X)g(X)$. Звідси випливає, що $H = g(X) F[X]$.

Ще один приклад комутативного кільця, де кожен ідеал буде головним, отримує з наступної теореми.

17.3. Теорема. Нехай F — поле. Тоді кожен ідеал кільця $F[[X]]$ є головним.

Доведення. Нехай H — ідеал кільця $F[[X]]$. Якщо $H = \{0_F\}$, то $H = 0_F F[[X]]$. Припустимо тепер, що H містить ненульові степеневі ряди. Якщо $\sum_{n \in N_0} a_n X^n \in H$ і $a_0 \neq 0_F$, то як ми бачили вище,

$$\sum_{n \in N_0} a_n X^n \in U(F[[X]])$$

і із пропозиції 16.6 випливає, що $H = F[[X]]$, тобто $H = e F[[X]]$.

Розглянемо тепер випадок, коли коефіцієнти при X^0 кожного ряду з H дорівнюють 0_F . Це означає, що кожен елемент $f(X)$ із H має вигляд $Xg(X)$ для деякого $g(X) \in F[[X]]$. Нехай m — натуральне число, яке має такі властивості: якщо $f(X) \in H$, то $f(X) = X^m g(X)$ для деякого ряду $g(X)$ і існує такий ряд $d(X) = \sum_{n \in N_0} b_n X^n \in H$, що $b_0 = b_1 = \dots = b_{m-1} = 0_F$, але $b_m \neq 0_F$. Звідси отримуємо, що $d(X) = X^m d_1(X)$, причому коефіцієнт при X^0 ряду $d_1(X)$ дорівнює b_1 . Це означає, що $d_1(X) \in U(F[[X]])$.

Нехай $d_2(X)$ — такий ряд, що $d_1(X)d_2(X) = e$. Оскільки H — ідеал кільця $F[[X]]$, то $d(X)d_2(X) = X^m d_1(X)d_2(X) = X^m e = X^m \in H$. Тоді $X^m F[[X]] \leq H$. З іншого боку, кожен ряд $f(X)$ із H має вигляд $f(X) = X^m g(X)$, що доводить рівність $H = X^m F[[X]]$.

Повернемося тепер до розгляду кільця $R[y]$, із якого ми починали цей розділ. Нехай K — комутативне кільце, R — його унітарне

цілісне підкільце, $y \in K$. Якщо $f(X) \in R[X]$, $f(X) = a_0 + a_1X + \dots + a_nX^n$, $a_0, a_1, \dots, a_n \in R$, то позначимо $f(y) = a_0 + a_1y + \dots + a_ny^n$. Очевидно, $f(y) \in R[y]$.

Будемо говорити, що y — корінь полінома $f(X)$, якщо $f(y) = 0_R$.

Корінь може як належати кільцю R , так і знаходитись поза ним. Наприклад, поліном $X^2 - 2$ не має коренів у полі раціональних чисел, його корені належать полю R дійсних чисел; поліном $X^2 + 1$ не має коренів навіть у полі R .

17.4. Пропозиція. *Нехай K — комутативне кільце, R — його унітарне цілісне підкільце, $y \in K$. Відображення $\eta: R[X] \rightarrow K$, що визначається за правилом $\eta(f(X)) = f(y)$, $f(X) \in R[X]$, є гомоморфізмом.*

Це твердження доводиться безпосередньою перевіркою.

Розглянемо тепер $\text{Im } \eta$. З пропозиції 16.10 випливає, що $\text{Im } \eta$ — підкільце K . Якщо $f(X) = a$ — поліном нульового степеня, то $\eta(f(X)) = a$. Звідси випливає включення $R \leq \text{Im } \eta$. З іншого боку,

$$\text{Im } \eta = \{\eta(f(X)) \mid f(X) \in R[X]\} = \{f(y) \mid f(X) \in R[X]\},$$

а вже відзначалося, що $f(y) \in R[y]$ для будь-якого $f(X) \in R[X]$. Це означає, що $\text{Im } \eta = R[y] = \{f(y) \mid f(X) \in R[X]\}$. Розглянемо тепер $\text{Ker } \eta$.

Будемо говорити, що елемент y трансцендентний над кільцем R , якщо y не є коренем жодного ненульового полінома з коефіцієнтами з R .

Іншими словами, якщо елемент y трансцендентний над R , то $\text{Ker } \eta = \{0_R\}$. За теоремою 16.11 η — мономорфізм, тобто $R[X] \cong R[y]$.

Нехай тепер $\text{Ker } \eta \neq \{0_R\}$. З пропозиції 16.10 випливає, що $\text{Ker } \eta$ — ідеал кільця поліномів $R[X]$. $\text{Ker } \eta$ складається з тих і тільки тих поліномів $f(X)$, для яких $f(y) = 0_R$. Інакше кажучи, $\text{Ker } \eta$ складається з усіх поліномів, що мають y своїм коренем.

Будемо говорити, що елемент y алгебричний над R , якщо в кільці поліномів $R[X]$ знайдеться ненульовий поліном, що має y своїм коренем.

Якщо R — поле, то з наслідку 17.2 випливає, що $\text{Ker } \eta = h(X)R[X]$ для деякого полінома $h(X) \in R[X]$. Якщо $r(X)$ — інший поліном з властивістю $\text{Ker } \eta = r(X)R[X]$, то маємо

$$h(X) = r(X)u(X) \quad \text{і} \quad r(X) = h(X)v(X)$$

для деяких $u(X), v(X) \in R[X]$. Звідси одержуємо

$$h(X) = r(X)u(X) = h(X)v(X)u(X),$$

тобто $v(X)u(X) = e$. Оскільки, як ми бачили вище, $U(R[X]) = U(R)$, то це означає, що $v(X) = c \in U(R)$, $u(X) = c^{-1}$. Отже, $r(X) = c h(X)$, де $c \in U(R)$.

Серед усіх поліномів, що породжують ідеал $\text{Ker } \eta$, виберемо той,

старший коефіцієнт якого дорівнює одиничному елементу. Цей поліном позначимо через $m_y(X)$ і будемо називати *мінімальним поліномом для елемента a над полем R* . З теореми 16.13 отримуємо ізоморфізм

$$R[y] = \text{Im } \eta \cong R[X]/\text{Ker } \eta,$$

а якщо ще R — поле, то

$$\text{Ker } \eta = m_y(X)R[X].$$

Нехай F — поле, $y \in F$. З теореми 17.1 одержуємо розклад $f(X) = q(X)(X - y) + r(X)$, де або $r(X) = 0_F$, або $\deg r(X) < \deg (X - y) = 1$. Отже, в будь-якому випадку $r(X) \in F$, тобто $r(X) = b \in F$. З пропозиції 17.4 випливає, що $f(y) = q(y)(y - y) + b = b$. Таким чином, $f(X) = (X - y)q(X) + f(y)$.

Будемо говорити, що поліном $f(X)$ ділиться на поліном $g(X)$, якщо $f(X) = g(X)q(X)$ для деякого полінома $q(X)$.

Таким чином, доведено твердження.

17.5. Пропозиція. Нехай F — поле, $f(X) \in F[X]$. Елемент $y \in F$ у тому і тільки у тому разі є коренем полінома $f(X)$, коли $f(X)$ ділиться на $(X - y)$.

17.6. Наслідок. Нехай F — поле, $f(X) \in F[X]$. Тоді $f(X) = (X - c_1)^{k_1} \dots (X - c_m)^{k_m} q(X)$, де поліном $q(X)$ не має коренів у полі F , $c_j \neq c_t$ при $j \neq t$, $k_1, \dots, k_m \in \mathbb{N}$.

17.7. Наслідок. Нехай F — поле, $f(X) \in F[X]$, $M = \{a \in F \mid a \text{ — корінь } f(X)\}$. Тоді $|M| \leq \deg f(X)$.

Поле F називається алгебрично замкнутим, якщо будь-який поліном $f(X) \in F[X]$ має в полі F хоча б один корінь.

17.8. Наслідок. Поле F у тому і тільки тому разі є алгебрично замкнутим, коли для будь-якого полінома $f(X) \in F[X]$ має місце рівність

$$f(X) = (X - c_1)^{k_1} \dots (X - c_m)^{k_m},$$

де $c_1, \dots, c_m \in F$, $c_j \neq c_t$ при $j \neq t$, $k_1, \dots, k_m \in \mathbb{N}$.

18. ПОЛЕ КОМПЛЕКСНИХ ЧИСЕЛ

Іншим важливим прикладом, що потребує окремого розгляду, є поле комплексних чисел. Комплексні числа виникли в зв'язку із задачами знаходження коренів поліномів з дійсними коефіцієнтами. Прикладом найпростішого полінома, що не має коренів у полі дійсних

чисел, буде $X^2 + 1$. Це приводить до необхідності розглядати вираз $\sqrt{-1}$. Перші спроби введення комплексних чисел були здійснені італійськими математиками. Уже Кардано формально оперував (із усілякими застереженнями) із виразами, що містять квадратні корені з від'ємних величин, а його послідовник Бомбеллі виклав числення з комплексними числами у формі, близької до сучасної. Проте, визнання комплексних чисел відбувалося дуже повільно. Історія математики бачила довгу боротьбу між прихильниками та супротивниками комплексних чисел. Основне питання було пов'язане з пошуками природного пояснення для величини $\sqrt{-1}$. Лише Гаусу вдалася спроба дати переконливе для багатьох обґрунтування. Подальший розвиток математики, а також використання в механіці й фізиці зробили поняття комплексного числа «законним» і звичним.

Нехай P, F — поля. Якщо F — підполе поля P , то будемо говорити, що P — розширення поля F .

Нехай F — підполе поля P , M — деяка підмножина P . Розглянемо сукупність M тих підполів, які містять у собі як підполе F , так і підмножину M . Нехай $F(M) = \cap M$. За наслідком 15.12 $F(M)$ — підполе. З його означення випливає, що $F(M)$ — найменше підполе, яке містить у собі підполе F і підмножину M .

Підполе $F(M)$ називається розширенням поля F , одержаним приєднанням до F підмножини M .

Найпростіший випадок, коли M складається з єдиного елемента y . У цьому випадку замість $F(M)$ будемо писати $F(y)$.

Розширення, одержане приєднанням до F одного елемента y , називається простим розширенням.

Очевидно, $F[M] = F(M)$, зокрема $F[a] = F(a)$.

У термінах розширень можна зараз сформулювати визначення поля комплексних чисел.

Поле комплексних чисел називається розширенням поля дійсних чисел, одержане приєднанням до нього кореня полінома $X^2 + 1$.

Поле комплексних чисел будемо позначати C , а для кореня полінома $X^2 + 1$ будемо використовувати його звичайне позначення i . У таких позначеннях $C = R(i)$. Далі слід звернути увагу на таку обставину. Коли ми давали визначення розширення поля, що отримане приєднанням деякої множини елементів (зокрема, одного елемента), ми вважали, що i поле, яке розширюється, і множина, що приєднується, містяться в одному більш широкому полі. Визначаючи вище поле комплексних чисел, ми не знаємо (поки що), чи існує поле, підполем у якому буде поле дійсних чисел, і яке містить корінь полінома $X^2 + 1$. Тому перше питання, яке тут виникає, це питання про існування поля комплексних чисел. Але спочатку припустимо, що таке поле існує й знайдемо вигляд його елементів. Отже, нехай F — поле, підполем якого буде R , і нехай F містить елемент i — корінь полінома $X^2 + 1$. Якщо K — підполе F , яке містить у собі R та елемент i , то разом з кожним дійсним числом x підполе K містить і елемент xi . Отже, якщо $x, y \in R$, то $x + yi \in K$. Таким чином, підполе

C , яке є перетином всіх підполів K , що містять у собі R та елемент i , містить всі елементи $x + yi$. Нехай $S = \{x + yi \mid x, y \in R\}$, тоді маємо включення $S \subseteq C$. Покажемо, що підмножина S є підполем. Скористаємось для цього критерієм підполя. Нехай $a = x + yi$, $b = u + vi$, тоді маємо

$$\alpha - \beta = (x - u) + (y - v)i \in S,$$

$$\alpha\beta = (x + yi)(u + vi) = (xu - yv) + i(yu + xv) \in S.$$

З означення підполя випливає, що одиничний елемент підполя R , тобто число 1, буде одиничним елементом усього поля F , але ж $1 = 1 + 0i \in S$. Аналогічно $i = 0 + 1i \in S$.

Нарешті, нехай $0 \neq a = x + yi \in S$. Зокрема, хоча б одне з чисел x або y — ненульове, а тому $x^2 + y^2 \neq 0$. Маємо

$$(x + yi)(x - yi) = x^2 + y^2.$$

Це підказує наступну рівність

$$(x + yi)^{-1} = (x/(x^2 + y^2) + (-y)/(x^2 + y^2)i) \in S.$$

Таким чином, всі умови теореми 15.10 виконуються для S , отже S — підполе поля F . За самим визначенням, S містить у собі всі дійсні числа, а також елемент i . Це означає, що S містить у собі $C = R(i)$. З іншого боку, ми довели вже включення $S \subseteq C$, яке доводить рівність $C = \{x + yi \mid x, y \in R\}$.

Припустимо, що $x + yi = u + vi$ для деяких $x, y, u, v \in R$. Тоді $x - u = (v - y)i$. Оскільки $i \notin R$, то ця рівність можлива лише в тому випадку, коли $v - y = 0$, $x - u = 0$, тобто $x = u$, $y = v$.

Таким чином, будь-яке комплексне число можна записати однозначно у вигляді $x + yi$, де x, y — дійсні числа. Доданок x називається його *дійсною частиною*, доданок yi — його *уявною частиною*.

Скористаємось тепер усім цим, щоб довести існування поля комплексних чисел. Почнемо зі звичайної трактовки комплексних чисел як точок звичайної площини. Це так звана геометрична модель поля комплексних чисел.

Отже, комплексною площиною ми будемо називати множину $R \times R$ всіх точок $\alpha = (x, y)$, $x, y \in R$, на якій операції додавання та множення задаються наступними рівностями: якщо $\beta = (u, v)$, то

$$\alpha + \beta = (x + u, y + v), \quad \alpha\beta = (xu - yv, yu + xv).$$

Як ми бачимо, ці формули підказані нам попереднім розглядом. Розглянемо тепер властивості цих операцій.

Додавання комутативне:

$$\alpha + \beta = (x + u, y + v) = (u + x, v + y) = \beta + \alpha.$$

Додавання асоціативне:

нехай $\gamma = (z, w)$, тоді

$$\begin{aligned} (\alpha + \beta) + \gamma &= ((x + u) + z, (y + v) + w) = \\ &= (x + (u + z), y + (v + w)) = \alpha + (\beta + \gamma). \end{aligned}$$

Відносно операції додавання існує нульовий елемент, ним буде пара $(0, 0)$:

$$(x, y) + (0, 0) = (x + 0, y + 0) = (x, y).$$

Для кожної пари (x, y) існує протилежний елемент, ним буде $(-x, -y)$:

$$(x, y) + (-x, -y) = (x + (-x), y + (-y)) = (0, 0).$$

Множення комутативне:

$$\alpha\beta = (xu - yv, yu + xv), \beta\alpha = (ux - vy, uy + vx), \text{ тобто } \alpha\beta = \beta\alpha.$$

Множення асоціативне:

$$\begin{aligned} (\alpha\beta)\gamma &= (xu - yv, yu + xv)(z, w) = \\ &= ((xu - yv)z - (yu + xv)w, (yu + xv)z + (xu - yv)w) = \\ &= (xuz - yvz - yuw - xvw, yuz + xvz + xiw - yvw); \end{aligned}$$

$$\begin{aligned} \alpha(\beta\gamma) &= (x, y)(uz - vw, vz + uw) = \\ &= (x(uz - vw) - y(vz + uw), y(uz - vw) + x(vz + uw)) = \\ &= (xuz - xvw - yvz - yuw, yuz - yvw + xvz + xiw), \end{aligned}$$

отже, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Відносно операції множення існує одиничний елемент, ним буде пара $(1, 0)$:

$$(x, y)(1, 0) = (x \cdot 1 - y \cdot 0, y \cdot 1 + x \cdot 0) = (x, y).$$

Для кожної пари $(x, y) \neq (0, 0)$ існує обернений елемент, ним буде $(x/(x^2 + y^2), -y/(x^2 + y^2))$:

$$\begin{aligned} (x, y)(x/(x^2 + y^2), -y/(x^2 + y^2)) &= \\ &= ((x^2 + y^2)/(x^2 + y^2), (yx - xy)/(x^2 + y^2)) = (1, 0). \end{aligned}$$

Додавання та множення пов'язані законом дистрибутивності:

$$\begin{aligned} (\alpha + \beta)\gamma &= ((x, y) + (u, v))(z, w) = (x + u, y + v)(z, w) = \\ &= ((x + u)z - (y + v)w, (y + v)z + (x + u)w) = \\ &= (xz + uz - yw - vw, yz + vz + xw + uw); \end{aligned}$$

$$\begin{aligned} \alpha\gamma + \beta\gamma &= (x, y)(z, w) + (u, v)(z, w) = \\ &= (xz - yw, yz + xw) + (uz - vw, vz + uw) = \\ &= (xz - yw + uz - vw, yz + xw + vz + uw), \end{aligned}$$

отже, $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$.

Таким чином, відносно введених вище операцій додавання та множення $R \times R$ стає полем.

Підмножина $R \times \{0\} = \{(x, 0) \mid x \in R\}$ є підполем. Дійсно,

$$(x, 0) - (y, 0) = (x - y, 0) \in R \times \{0\};$$

$$(x, 0)(y, 0) = (xy - 0 \cdot 0, 0 \cdot y + x \cdot 0) = (xy, 0) \in R \times \{0\};$$

$$(1, 0) \in R \times \{0\},$$

якщо $(x, 0) \neq (0, 0)$, то $x \neq 0$ і $(x, 0)^{-1} = (x^{-1}, 0) \in R \times \{0\}$.

Розглянемо тепер відображення $f: R \longrightarrow R \times \{0\}$, що визначається за правилом $f(x) = (x, 0)$. Маємо

$$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y);$$

$$f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)f(y).$$

Очевидно також, що f є бієктивним, так що f — ізоморфізм. Інакше кажучи, підполе $R \times \{0\}$ ізоморфно до поля R дійсних чисел. Це дає нам можливість ототожнювати пару $(x, 0)$ із дійсним числом x . Цією можливістю ми зараз і скористаємось.

Маємо очевидну рівність

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1)(y, 0).$$

Також $(0, 1)^2 = (-1, 0)$. Таким чином, якщо покласти $i = (0, 1)$, то $i^2 = (-1, 0)$, так що, ототожнюючи пару $(-1, 0)$ з дійсним числом -1 , отримаємо

$$(x, y) = (x, 0) + (0, 1)(y, 0) = x + yi.$$

Таким чином, наше побудоване поле містить у собі як підполе поле R дійсних чисел (точніше його ізоморфну копію), а також містить корінь полінома $X^2 + 1$. Отже, воно містить у собі підполе $R(i) = \mathbb{C}$. Більш того, з попередніх розглядів видно, що воно само співпадає з $\mathbb{C}$.

Наведемо зараз іншу модель поля комплексних чисел, так звану *матричну модель*. Розглянемо підмножину P кільця $M_2(R)$, яка складається з матриць, що мають такий вигляд

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

Рівності

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} + \begin{pmatrix} u & v \\ -v & u \end{pmatrix} = \begin{pmatrix} x+u & y+v \\ -y-v & x+u \end{pmatrix},$$

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} u & v \\ -v & u \end{pmatrix} = \begin{pmatrix} xu+yv & xv-yu \\ -xv-yu & xu+yv \end{pmatrix}$$

показують, що підмножина P є сталою відносно операцій додавання та множення матриць. Додавання елементів множини P є комутативним та асоціативним, оскільки воно комутативне та асоціативне для всіх елементів матричного кільця $M_2(R)$, нульова матриця належить до P , зокрема, вона буде нульовим елементом для P . Нарешті,

$$-\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} -x & -y \\ y & -x \end{pmatrix},$$

і це показує, що відносно операції додавання P буде абелевою групою. Операції додавання та множення пов'язані законами дистрибутивності, оскільки вони мають місце для всіх матриць з $M_2(R)$, з тієї ж причини множення в P є асоціативним. Далі маємо

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} u & v \\ -v & u \end{pmatrix} = \begin{pmatrix} xu - yv & xv - yu \\ -xv - yu & xu - yv \end{pmatrix},$$

$$\begin{pmatrix} u & v \\ -v & u \end{pmatrix} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} ux - vy & vx + uy \\ -vx - uy & ux - vy \end{pmatrix},$$

а це доводить комутативність множення елементів P .

Нехай тепер

$$Y = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \text{ —}$$

довільний ненульовий елемент P . Тоді хоча б одне з чисел x або y — ненульове. Маємо $\det(Y) = x^2 + y^2 \neq 0$. Інакше кажучи, ненульові елементи з P будуть невиродженими матрицями, і тому кожна з них має обернену. Застосовуючи правило знаходження оберненої матриці, отримаємо

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}^{-1} = \begin{pmatrix} u & v \\ -v & u \end{pmatrix},$$

де $u = x/(x^2 + y^2)$, $v = (-y)/(x^2 + y^2)$. Це показує, що $Y^{-1} \in P$. Таким чином P є полем.

Розглянемо відображення $f: C \rightarrow P$, що визначено за правилом

$$f(x + yi) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

Очевидно воно бієктивне, а також якщо $\alpha = x + yi$, $\beta = u + vi$, то

$$f(\alpha + \beta) = f(x + u) + i(y + v) = \begin{pmatrix} x + u & y + v \\ -y - v & x + u \end{pmatrix},$$

$$f(\alpha) + f(\beta) = f(x + iy) + f(u + iv) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} + \begin{pmatrix} u & v \\ -v & u \end{pmatrix},$$

а отже $f(\alpha + \beta) = f(\alpha) + f(\beta)$.

Далі

$$\begin{aligned} f(\alpha\beta) &= f((xu - yv) + i(yu + xv)) = \begin{pmatrix} xu - yv & xv + yu \\ -xv - yu & xu - yv \end{pmatrix} = \\ &= \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} u & v \\ -v & u \end{pmatrix} = f(x + yi)f(u + vi) = f(\alpha)f(\beta). \end{aligned}$$

Всі ці рівності показують, що відображення f зберігає операції додавання та множення, а значить буде ізоморфізмом. Отже, поле C комплексних чисел ізоморфно до побудованого нами поля P . При цьому $f(R) = RE$ — множина всіх скалярних матриць, яка очевидно буде підполем P ,

$$f(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = I.$$

Отже, ми можемо ототожнити скалярну матрицю $x E$ із дійсним числом x . Також

$$I^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -E,$$

зокрема, поле P містить корінь матричного полінома $EX^2 + E$. Тепер ми знову можемо отримати звичайну форму комплексного числа в його матричній моделі:

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = xE + (yE)I.$$

Абсолютним значенням комплексного числа $x + yi$ називають невід'ємне дійсне число

$$\sqrt{x^2 + y^2} = |x + yi|.$$

18.1. Пропозиція. Відображення $\Delta: x + yi \rightarrow x - yi$ є автоморфізмом поля C . При цьому $\Delta^2 = \varepsilon_C$, $\Delta(a) = a$ для кожного $a \in C$.

Д о в е д е н н я . Справді,

$$\begin{aligned} \Delta(x + yi + u + vi) &= \Delta((x + u) + (y + v)i) = (x + u) - (y + v)i = \\ &= (x - yi) + (u - vi) = \Delta(x + yi) + \Delta(u + vi); \\ \Delta((x + yi)(u + vi)) &= \Delta((xu - yv) + (xv + yu)i) = \\ &= (xu - yv) - (xv + yu)i = (x - yi)(u - vi) = \Delta(x + yi)\Delta(u + vi). \end{aligned}$$

Ін'єктивність і сюр'єктивність відображення Δ очевидні. Нарешті,

$$\Delta^2(x + yi) = \Delta(\Delta(x + yi)) = \Delta(x - yi) = x + yi.$$

Із самого означення Δ випливає, що $\Delta(a) = a$ для будь-якого $a \in R$.

Числа $x + yi$ і $x - yi$ називають *комплексно спряженими*. У подальшому будемо писати

$$\Delta(x + yi) = \overline{x + yi}.$$

Очевидно, $(x + yi)(x - yi) = x^2 + y^2 = |x + yi|^2$.

Нехай $r = |x + yi|$. Запишемо комплексне число $x + yi$ у вигляді

$$x + yi = r((x/r) + (y/r)i).$$

Тоді

$$(x^2/r^2) + (y^2/r^2) = (x^2 + y^2)/(x^2 + y^2) = 1.$$

Тому знайдеться такий кут ϕ , що $\cos \phi = x/r$, $\sin \phi = y/r$. Цей кут ϕ називається *аргументом комплексного числа $x + yi$ та позначається через $\arg(x + yi)$* . Зрозуміло, що кут ϕ визначається з точністю до доданка, кратного 360° . Таким чином, маємо $x + yi = r(\cos \phi + i \sin \phi)$. Ця форма називається *тригонометричною формою запису комплексного числа*.

Тригонометрична форма запису виявляється досить зручною при діях, пов'язаних із множенням. Дійсно, нехай

$$x + yi = r(\cos \phi + i \sin \phi),$$

$$u + vi = q(\cos \psi + i \sin \psi),$$

тоді

$$\begin{aligned} (x + yi)(u + vi) &= r(\cos \phi + i \sin \phi)q(\cos \psi + i \sin \psi) = \\ &= rq((\cos \phi \cos \psi - \sin \phi \sin \psi) + i(\sin \phi \cos \psi + \cos \phi \sin \psi)) = \\ &= rq(\cos(\phi + \psi) + i \sin(\phi + \psi)). \end{aligned}$$

Таким чином, виходять дуже зручні формули

$$|(x + yi)(u + vi)| = |x + yi||u + vi|,$$

$$\arg((x + yi)(u + vi)) = \arg(x + yi) + \arg(u + vi).$$

Очевидно, ці формули можна розповсюдити на будь-яку скінченну кількість множників. Зокрема,

$$(r(\cos \phi + i \sin \phi))^k = r^k (\cos k\phi + i \sin k\phi), \quad k \in N,$$

або в іншому записі

$$|(x + yi)^k| = |x + yi|^k; \quad \arg((x + yi)^k) = k \arg(x + yi).$$

Ці формули називають *формулами Муавра*. Використовуючи їх, одержуємо можливість здійснити обернену операцію — добування кореня.

18.2. Пропозиція. Для будь-якого комплексного числа

$$x + yi = r(\cos \phi + i \sin \phi)$$

існує рівно k різних комплексних чисел

$$u + vi = q(\cos \xi + i \sin \xi)$$

із властивістю $(u + vi)^k = x + yi$ (коренів k -го степеня з числа $x + yi$). Їх дає формула $q = \sqrt[k]{r}$ (тут $\sqrt[k]{r}$ означає арифметичне значення кореня k -го степеня з додатного дійсного числа r), $\xi = (\phi + 2\pi t)/k$, де $0 \leq t < k$.

Доведення. Справді, із формули Муавра отримуємо $q^k = r$, $k\xi = \phi + 2\pi s$, $s \in N$. Звідси $q = \sqrt[k]{r}$, $\xi = (\phi + 2\pi s)/k$. Число s можна подати у вигляді $s = km + t$, де $0 \leq t \leq k - 1$. Тому

$$(\phi + 2\pi s)/k = (\phi + 2\pi(km + t))/k = (\phi + 2\pi t)/k + 2\pi m,$$

$$\cos((\phi + 2\pi s)/k) = \cos((\phi + 2\pi t)/k),$$

$$\sin((\phi + 2\pi s)/k) = \sin((\phi + 2\pi t)/k),$$

де $0 \leq t \leq k - 1$. Якщо $\cos \chi = \cos \psi$ та водночас $\sin \chi = \sin \psi$, то $\chi - \psi = 2\pi j$ для деякого цілого j . Це означає, що всі числа

$$\sqrt[k]{r} (\cos((\phi + 2\pi t)/k) + i \sin((\phi + 2\pi t)/k)),$$

де $0 \leq t \leq k - 1$, будуть різними, тобто дійсно отримуємо рівно k різних коренів k -го степеня з числа $x + yi$.

18.3. Наслідок. Корені k -го степеня з одиниці знаходяться за формулою

$$\varepsilon_k = \cos(2\pi t/k) + i \sin(2\pi t/k), \text{ де } 0 \leq t < k.$$

18.4. Наслідок. Множина C_k усіх коренів k -го степеня є циклічною підгрупою $U(C)$, причому $|C_k| = k$.

Справді, якщо $\alpha^k = \beta^k = 1$, то очевидно $(\alpha\beta^{-1})^k = 1$, і з наслідку 10.5 отримуємо, що C_k є підгрупою $U(C)$. Далі, із формули Муавра випливає рівність $\varepsilon_k = \varepsilon_1^k$, а це означає, що $C_k = \langle \varepsilon_1 \rangle$.

Корінь θ k -го степеня з одиниці називається *примітивним* або *первісним*, якщо він не є коренем з одиниці степеня d для $d < k$.

Інакше кажучи, k є найменшим натуральним числом, для якого $e^k = 1$, тобто порядок елемента e у групі $U(C)$ дорівнює k . Як ми вже бачили у розділі 10, $|\langle e \rangle| = |e|$, а тому $\langle e \rangle = C_k$. Таким чином,

корінь e k -го степеня з одиниці тоді і тільки тоді буде примітивним, коли $\langle e \rangle = C_k$. З теореми 10.13 випливає тепер

18.5. Наслідок. *Корінь e k -го степеня з одиниці тоді і тільки тоді буде примітивним, коли $e = \varepsilon_m$, де $\text{НСД}(m, k) = 1$.*

Використовуючи поле комплексних чисел, побудуємо два важливих алгебричних об'єкта.

Квазіциклічна група (p -група Прюфера).

Нехай p — просте число, позначимо

$$C_{p^\infty} = \{x \in C \mid x^{p^k} = 1 \text{ для деякого } k \in N_0\}.$$

Покажемо, що C_{p^∞} — підгрупа $U(C)$. Нехай $x, y \in C_{p^\infty}$, k, t — такі числа, що $x^{p^k} = 1$, $y^{p^t} = 1$. Покладемо $m = \max\{k, t\}$. Тоді маємо $(x/y)^{p^m} = 1$. З наслідку 10.5 випливає, що C_{p^∞} — підгрупа $U(C)$.

Нехай $x \in C_{p^\infty}$, k — найменше число, для якого $x^{p^k} = 1$. Інакше кажучи, $|x| = p^k$. Але тоді x — примітивний корінь з одиниці ступеня p^k , тобто $C_{p^k} = \langle x \rangle$. Очевидно,

$$C_p \leq C_{p^2} \leq \dots \leq C_{p^k} \dots, \bigcup_{k \in N} C_{p^k} = C_{p^\infty}.$$

Нехай H — підгрупа C_{p^∞} . Можливі дві ситуації:

(1) Порядки елементів підгрупи H обмежені в сукупності.

(2) Порядки елементів H не обмежені.

Розглянемо перший випадок. Тоді знайдеться таке число k , що $y^{p^k} = 1$, для кожного $y \in H$, і H містить такий елемент x , що $|x| = p^k$. Це означає, з одного боку, що $H \leq C_{p^k}$, а з іншого, що $\langle x \rangle = C_{p^k}$. Інакше кажучи, $H = C_{p^k}$.

Розглянемо другий випадок. Тоді для будь-якого числа $k \in N$ знайдеться такий елемент $z \in H$, що $|z| = p^m$, де $m \geq k$. З рівності $|z| = p^m$ випливає, що $\langle z \rangle = C_{p^m}$, а оскільки $m \geq k$, то

$$C_{p^k} \leq C_{p^m} = \langle z \rangle \leq H.$$

Отже, для будь-якого $k \in N$ підгрупа H містить у собі C_{p^k} . Це означає, що $H = C_{p^\infty}$.

Таким чином, будь-яка власна підгрупа C_{p^∞} є скінченною і циклічною.

Тому групу C_{p^∞} називають квазіциклічною. Інша її назва — p -група Прюфера. У 1938 р. О. Ю. Шмідт поставив питання про опис нескінченних груп, усі власні підгрупи яких скінченні [11]. Довго не вдавалося побудувати відмінних від C_{p^∞} груп такого типу й проблема О.Ю. Шмідта трансформувалася в проблему існування відмінних від C_{p^∞} груп, усі власні підгрупи яких циклічні. Порівняно недавно серії таких груп були побудовані О.Ю. Ольшанським [12, § 28].

Тіло кватерніонів. Розглянемо кільце матриць $M_2(C)$, а в ньому підмножину H , що складається з матриць, які мають наступний вигляд

$$\begin{pmatrix} x & y \\ -\Delta(y) & \Delta(x) \end{pmatrix}, \text{ де } x, y \in C.$$

Покажемо, що H — підкільце $M_2(C)$. Дійсно,

$$\begin{pmatrix} x & y \\ -\Delta(y) & \Delta(x) \end{pmatrix} - \begin{pmatrix} u & v \\ -\Delta(v) & \Delta(u) \end{pmatrix} = \begin{pmatrix} x-u & y-v \\ -(\Delta(y)-\Delta(v)) & \Delta(x)-\Delta(u) \end{pmatrix} = \\ = \begin{pmatrix} x-u & y-v \\ -(\Delta(y-v)) & \Delta(x-u) \end{pmatrix} \in H.$$

$$\begin{pmatrix} x & y \\ -\Delta(y) & \Delta(x) \end{pmatrix} \begin{pmatrix} u & v \\ -\Delta(v) & \Delta(u) \end{pmatrix} = \begin{pmatrix} xu - y\Delta(v) & xv + y\Delta(u) \\ -\Delta(y)u - \Delta(x)\Delta(v) & -\Delta(y)v + \Delta(x)\Delta(u) \end{pmatrix} = \\ = \begin{pmatrix} xu - y\Delta(v) & xv + y\Delta(u) \\ -(\Delta(y)\Delta(\Delta(u)) + \Delta(x)\Delta(v)) & -\Delta(y)\Delta(\Delta(v)) + \Delta(x)\Delta(u) \end{pmatrix} = \\ = \begin{pmatrix} xu - y\Delta(v) & xv + y\Delta(u) \\ -(\Delta(y\Delta(u)) + \Delta(xv)) & -(\Delta(y\Delta(v)) + \Delta(xu)) \end{pmatrix} = \\ = \begin{pmatrix} xu - y\Delta(v) & xv + y\Delta(u) \\ -\Delta(y\Delta(u) + xv) & \Delta(xu - y\Delta(v)) \end{pmatrix} \in H.$$

З теореми 15.4 одержуємо, що H — підкільце $M_2(C)$.

Розглянемо тепер довільний ненульовий елемент H :

$$\alpha = \begin{pmatrix} x & y \\ -\Delta(y) & \Delta(x) \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Маємо $\det(\alpha) = x\Delta(x) + y\Delta(y) = |x|^2 + |y|^2 \neq 0$, зокрема, матриця α не вироджена, і отже має обернену. Застосуємо для її знаходження теорему 8.2, і отримаємо

$$\alpha^{-1} = \begin{pmatrix} \Delta(x)/\det(\alpha) & -y/\det(\alpha) \\ \Delta(y)/\det(\alpha) & x/\det(\alpha) \end{pmatrix} \begin{pmatrix} \Delta(x)/\det(\alpha) & -y/\det(\alpha) \\ -\Delta(-y/\det(\alpha)) & \Delta(\Delta(x)/\det(\alpha)) \end{pmatrix} \in H.$$

Отже, H — тіло. Отримаємо зараз звичайну форму запису для елементів H . Нехай $x = a + bi$, $y = c + di$, тоді

$$\begin{pmatrix} x & y \\ -\Delta(y) & \Delta(x) \end{pmatrix} = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = \\ = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} bi & 0 \\ 0 & -bi \end{pmatrix} + \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix} + \begin{pmatrix} 0 & di \\ -di & 0 \end{pmatrix} = \\ = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Нехай

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Шляхом безпосереднього підрахунку для матриць E, I, J, K одержимо таку таблицю множення:

	E	I	J	K
E	E	I	J	K
I	I	$-E$	K	$-J$
J	J	$-K$	$-E$	I
K	K	J	$-I$	$-E$

Зокрема, $IJ = K$, $JI = -K$, тобто множення некомутативне. Отже, H — некомутативне тіло. H називають тілом кватерніонів, а його елементи — кватерніонами, (точніше — дійсними кватерніонами).

19. КІЛЬЦЕ ПОЛІНОМІВ ВІД КІЛЬКОХ НЕВІДОМИХ

У розділі 17 було побудовано кільце поліномів від однієї невідомої над довільним комутативним кільцем R . Зараз ми звичайним чином розширимо цю конструкцію і розглянемо поліноми від кількох невідомих. Як і у розділі 17 будемо вважати, що комутативне кільце R не має дільників нуля. Отже, нехай $K = R[X]$ — кільце поліномів від однієї невідомої, яке було побудовано у розділі 17. У свою чергу тепер можна розглянути кільце поліномів від однієї невідомої (нової невідомої Y) $Q = K[Y]$ над кільцем K . Невідома Y грає по відношенню до K ту ж саму роль, яку грає X по відношенню до R . Елементи з Q записуються у вигляді

$$b_0 + b_1 Y + \dots + b_m Y^m, \quad b_j \in K, \quad 0 \leq j \leq m,$$

причому такий запис є однозначним. У свою чергу, кожний елемент b_j має вигляд $b_j = a_{j0} + a_{j1}X + \dots + a_{jn(j)}X^{n(j)}$. Із самої побудови кільця поліномів випливає, що невідома є переставною з кожним елементом кільця, над яким будуються поліноми. Зокрема, у нашому випадку, невідомі X та Y будуть переставними. Таким чином, остаточно, кожен елемент Q має вигляд

$$\sum_{1 \leq j \leq m} \sum_{1 \leq k \leq n(j)} a_{jk} X^k Y^j, \quad a_{jk} \in R, \quad 1 \leq k \leq n(j), \quad 1 \leq j \leq m.$$

Кільце $Q = R[X, Y]$ називають кільцем поліномів від двох (незалежних) невідомих X та Y над кільцем R .

Повторюючи це потрібне нам число кроків, можна отримати кільце $R[X_1, \dots, X_n]$ поліномів над R від незалежних невідомих $X_1, \dots, X_n$. Елемент $f \in R[X_1, \dots, X_n]$ буде сумою елементів виду $a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$, які називаються мономами, де $a(k_1, \dots, k_n)$ — елемент кільця R . Число k_j називають степенем монома відносно невідомої X_j , а суму $k_1 + \dots + k_n$ — повним степенем цього монома.

Згадуючи правило рівності поліномів від однієї невідомої, отримуємо наступне правило рівності двох поліномів $f, g \in R[X_1, \dots, X_n]$. Поліноми f та g тоді і тільки тоді співпадають, коли для будь-якого монома $a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$ із розкладу полінома f розклад полінома g містить моном $b(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$, і більш того, $a(k_1, \dots, k_n) = b(k_1, \dots, k_n)$; і навпаки.

Степенем полінома $f \in R[X_1, \dots, X_n]$ відносно невідомої X_j називають найбільший зі степенів ненульових мономів, які входять до розкладу f , відносно невідомої X_j . Це число позначається символом $\deg_j f(X_1, \dots, X_n)$, або коротше $\deg_j f$.

Аналогічно, повним степенем полінома $f \in R[X_1, \dots, X_n]$ називають найбільший з повних степенів ненульових мономів, які входять до розкладу f . Це число позначається символом $\deg f(X_1, \dots, X_n)$, або коротше $\deg f$. Як і для поліномів від одного невідомого, нульовому елементу ніякого степеня не присвоюють, або присвоюють степінь $-\infty$.

Про старший коефіцієнт полінома від кількох невідомих говорити нема сенсу, оскільки його розклад може мати не один моном, що має найбільший степінь.

Поліном $f \in R[X_1, \dots, X_n]$ будемо називати однорідним або формою степеня t , якщо кожен його моном має один і той самий повний степінь, що дорівнює t . Форми степеня 1, 2, 3 називаються відповідно лінійними, квадратичними та кубічними.

Об'єднуючи разом всі мономи, що мають один і той самий повний степінь, ми можемо записати поліном $f(X_1, \dots, X_n)$ у вигляді суми форм різних степенів:

$$f(X_1, \dots, X_n) = f_0(X_1, \dots, X_n) + f_1(X_1, \dots, X_n) + \dots + f_k(X_1, \dots, X_n),$$

де $k = \deg f(X_1, \dots, X_n)$. Слід відзначити також, що таке представлення є однозначним.

У розділі 17 було доведено, що кільце поліномів $R[X]$ не має дільників нуля. Застосовуючи просту індукцію, отримуємо, що і кільце поліномів $R[X_1, \dots, X_n]$ від кількох невідомих над областю цілісності R не має дільників нуля. Цей результат можна трохи підсилити.

19.1. Теорема. Нехай R — область цілісності, $f, g \in R[X_1, \dots, X_n]$. Тоді

$$\deg_j(fg) = \deg_j f + \deg_j g \quad \text{для кожного } j, 1 \leq j \leq n;$$

$$\deg(fg) = \deg f + \deg g.$$

Д о в е д е н н я . Перше твердження було доведено у розділі 17. Нехай $f = f_0 + f_1 + \dots + f_k$ — розклад f у суму форм, де $k = \deg f$, $g = g_0 + g_1 + \dots + g_m$, де $m = \deg g$. Маємо

$$fg = f_0g_0 + (f_0g_1 + f_1g_0) + \dots + f_kg_m.$$

Форми f_k, g_m — ненульові, а оскільки, як було помічено трохи вище, кільце $R[X_1, \dots, X_n]$ не має дільників нуля, то поліном f_kg_m — ненульовий. Очевидно, кожен моном із розкладу інших доданків має повний степінь меншу, ніж $k + m$. Звідси і випливає, що

$$\deg(fg) = k + m = \deg f + \deg g.$$

Нехай K — комутативне кільце, R — його унітарне цілісне підкільце, $y_1, \dots, y_n \in K$. Якщо $f \in R[X_1, \dots, X_n]$, $f = \sum a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$, то покладемо $f(y_1, \dots, y_n) = \sum a(k_1, \dots, k_n) y_1^{k_1} \dots y_n^{k_n}$. Елемент $f(y_1, \dots, y_n)$ кільця K називається значенням полінома $f(X_1, \dots, X_n)$ у точці $(y_1, \dots, y_n)$, або значенням при $X_1 = y_1, \dots, X_n = y_n$.

Будемо говорити, що $(y_1, \dots, y_n)$ — корінь полінома $f(X_1, \dots, X_n)$, якщо $f(y_1, \dots, y_n) = 0_R$.

Як і для кільця поліномів від одного невідомого, має місце

19.2. Пропозиція. Нехай K — комутативне кільце, R — його унітарне цілісне підкільце, $y_1, \dots, y_n \in K$. Відображення $\eta[y_1, \dots, y_n]: R[X_1, \dots, X_n] \rightarrow K$, що визначається за правилом $\eta[y_1, \dots, y_n](f) = f(y_1, \dots, y_n)$, $f(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$, є гомоморфізмом.

Це твердження виводиться з пропозиції 17.4 за допомогою простої індукції.

Як і для випадку однієї невідомої, $\text{Im } \eta[y_1, \dots, y_n] = R[y_1, \dots, y_n]$ — підкільце, що породжене над R елементами $y_1, \dots, y_n$.

Елементи $y_1, \dots, y_n \in K$ називаються алгебрично залежними над R , якщо $\text{Ker } \eta[y_1, \dots, y_n] \neq \{0_R\}$, і відповідно, алгебрично незалежними, якщо $\text{Ker } \eta[y_1, \dots, y_n] = \{0_R\}$.

Зокрема, якщо елементи $y_1, \dots, y_n$ алгебрично незалежні над R , то підкільце $R[y_1, \dots, y_n]$ ізоморфне до кільця поліномів $R[X_1, \dots, X_n]$.

Пропозиція 19.2 вказує на універсальність кільця поліномів. Розглянемо тепер стандартну форму запису поліномів від кількох змінних. Це так звана лексикографічна форма запису, якою користуються при розташуванні слів у словниках. Нехай $f \in R[X_1, \dots, X_n]$ і розглянемо два довільні мономи $a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$ і $a(m_1, \dots, m_n) X_1^{m_1} \dots X_n^{m_n}$ із розкладу полінома f .

Будемо говорити, що моном $a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$ є вищим за моном $a(m_1, \dots, m_n) X_1^{m_1} \dots X_n^{m_n}$, якщо існує номер d із властивістю:

$$k_1 = m_1, \dots, k_{d-1} = m_{d-1}, \text{ але } k_d > m_d.$$

Слід відзначити, що якщо один моном є вищим за інший, то його повний степінь не обов'язково є більшим, тобто лексикографічний

порядок не пов'язаний зі степенем полінома. Очевидно, для кожної пари мономів один обов'язково є вищим за інший, а також, що це відношення є транзитивним. Таким чином, усі члени з розкладу полінома f можуть бути розташовані у відповідності до введеного вище порядку. Такий запис полінома f будемо називати лексикографічним. Моном, який є найвищим при цьому лексикографічному порядку, називається вищим членом полінома f .

19.3. Теорема. Нехай R — область цілісності, $f, g \in R[X_1, \dots, X_n]$. Тоді вищий член полінома fg буде добутком вищого члена f та вищого члена g .

Д о в е д е н н я . Нехай $a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n}$ та $b(t_1, \dots, t_n) X_1^{t_1} \dots X_n^{t_n}$ — вищі члени поліномів f та g відповідно. Добуток fg буде сумою усіх можливих добутків мономів із розкладів f та g .

Нехай $a(m_1, \dots, m_n) X_1^{m_1} \dots X_n^{m_n}$ та $b(r_1, \dots, r_n) X_1^{r_1} \dots X_n^{r_n}$ — довільні мономи з розкладу f та g відповідно. Тоді існує такий номер d (відповідно q), що $k_1 = m_1, \dots, k_{d-1} = m_{d-1}$, але $k_d > m_d$ (відповідно $t_1 = r_1, \dots, t_{q-1} = r_{q-1}$, але $t_q > r_q$). Порівняємо тепер добутки

$$\begin{aligned} & (a(k_1, \dots, k_n) X_1^{k_1} \dots X_n^{k_n})(b(t_1, \dots, t_n) X_1^{t_1} \dots X_n^{t_n}) = \\ & = a(k_1, \dots, k_n)b(t_1, \dots, t_n)X_1^{k_1+t_1} \dots X_n^{k_n+t_n} \end{aligned}$$

та

$$\begin{aligned} & (a(m_1, \dots, m_n) X_1^{m_1} \dots X_n^{m_n})(b(r_1, \dots, r_n) X_1^{r_1} \dots X_n^{r_n}) = \\ & = a(m_1, \dots, m_n)b(r_1, \dots, r_n)X_1^{m_1+r_1} \dots X_n^{m_n+r_n}. \end{aligned}$$

З двох натуральних чисел d, q одне не менше іншого. Нехай $d \leq q$, тоді маємо $k_1 + t_1 = m_1 + r_1, \dots, k_{d-1} + t_{d-1} = m_{d-1} + r_{d-1}$, але $k_d + t_d > m_d + r_d$.

Аналогічно розглядається випадок $q \leq d$. Таким чином,

$$a(k_1, \dots, k_n)b(t_1, \dots, t_n)X_1^{k_1+t_1} \dots X_n^{k_n+t_n}$$

є вищим за

$$a(m_1, \dots, m_n)b(r_1, \dots, r_n)X_1^{m_1+r_1} \dots X_n^{m_n+r_n}.$$

Це й означає, що добуток

$$a(k_1, \dots, k_n)b(t_1, \dots, t_n)X_1^{k_1+t_1} \dots X_n^{k_n+t_n}$$

буде вищим членом полінома fg .

20. РОЗШИРЕННЯ АРИФМЕТИКИ НА КОМУТАТИВНІ КІЛЬЦЯ

Почнемо зі звичного поняття подільності і подивимось як воно трансформується у кільцях. Нехай R — комутативне кільце, що не має дільників нуля. Скажемо, що елемент b кільця R ділиться на елемент a або a ділить b , або b є кратним до a , якщо існує такий елемент $c \in R$, що $b = ac$. Це будемо позначати наступним символом $a \mid b$.

Нехай $a \mid b$ та $b \mid a$, тобто $b = ac$ і $a = bd$ для деяких елементів $c, d \in R$. Маємо тоді $a = a(cd)$, отже $cd = e$ і $c, d \in U(R)$. Елементи $a, b \in R$ називаються асоційованими, якщо $b = au$ для деякого елемента $u \in U(R)$.

20.1. Пропозиція. Нехай R — область цілісності. Відношення “бути асоційованими елементами” є відношенням еквівалентності.

Доведення. Дійсно, із рівності $a = ae$ випливає, що це відношення рефлексивне. Далі, якщо $b = au$, де $u \in U(R)$, то $a = bu^{-1}$ і також $u^{-1} \in U(R)$, тобто відношення асоційованості є симетричним. Нарешті, нехай $c = bv$, де $v \in U(R)$, тоді $c = (au)v = a(uv)$ і $uv \in U(R)$, так що воно буде і транзитивним.

Класи еквівалентності відношення “бути асоційованими елементами” називаються класами асоційованості кільця R .

Якщо $u \in U(R)$, то елемент u буде дільником кожного елемента a . Це випливає з рівностей $a = ae = a(u^{-1}u) = (au^{-1})u$. Елементи, асоційовані з a та елементи з групи $U(R)$ називаються не власними дільниками елемента a .

І відповідно, якщо $a = bc$, де $b, c \in U(R)$, то елементи b, c будуть власними дільниками елемента a .

Класи еквівалентності відношення “бути асоційованими елементами” називаються класами асоційованості кільця R .

Відзначимо зараз наступні властивості подільності.

20.2. Пропозиція. Нехай R — область цілісності.

- (1) Якщо елемент a кільця R ділить елемент b , $a \mid b$, у свою чергу, ділить c , то a ділить c .
- (2) Якщо елемент a кільця R ділить елементи b, c , то a ділить $b + c$.
- (3) Якщо елемент a кільця R ділить елемент b , то a ділить bc .
- (4) Якщо елемент a кільця R ділить елементи $b_1, \dots, b_n$ а $c_1, \dots, c_n$ — довільні елементи R , то a ділить $b_1c_1 + \dots + b_nc_n$.

Ці твердження майже очевидні.

Поняття подільності можна перевести на мову ідеалів. Як покаже подальший розгляд, це буде дуже корисним.

20.3. Пропозиція. Нехай R — область цілісності. Елемент a кільця R тоді і тільки тоді ділить елемент b , коли $bR \leq aR$.

Доведення. Якщо $a \mid b$, то $b = ac$ для деякого елемента $c \in R$. Зокрема, $b \in aR$, і оскільки aR — ідеал, то з цього включення випливає включення ідеалів $bR \leq aR$. Навпаки, якщо $bR \leq aR$, то $b \in aR$, тобто $b = ac$ для деякого елемента $c \in R$.

20.4. Наслідок. Нехай R — область цілісності.

- (1) Елементи a, b кільця R тоді і тільки тоді асоційовані, коли $bR = aR$.
- (2) Якщо a — власний дільник елемента b , то $bR \leq aR$ і $bR \neq aR$.

Нехай R — область цілісності, $a, b \in R$. Елемент d кільця R називається найбільшим спільним дільником елементів a, b , якщо d задовольняє наступні умови:

(GCD 1) d ділить a та d ділить b ;

(GCD 2) якщо c — спільний дільник елементів a, b , то c ділить d .

Очевидно, разом з елементом d , кожен елемент, асоційований з d , також задовольняє умови (GCD 1) та (GCD 2). Навпаки, якщо елемент d_1 задовольняє умови (GCD 1) та (GCD 2), то елементи d, d_1 ділять один одного і тому вони асоційовані. Таким чином, всі найбільші спільні дільники елементів a, b (якщо вони існують) складають клас асоційованих елементів. Той факт, що елемент d — один із найбільших спільних дільників елементів a, b , будемо позначати символом $d = \text{GCD}(a, b)$.

Дуальним до поняття найбільшого спільного дільника є поняття найменшого спільного кратного.

Нехай R — область цілісності, $a, b \in R$. Елемент t кільця R називається найменшим спільним кратним елементів a, b , якщо t задовольняє наступні умови:

(LCM 1) a ділить t та b ділить t ;

(LCM 2) якщо c — спільне кратне елементів a, b , то t ділить c .

Очевидно, разом з елементом m , кожен елемент, асоційований з m , також задовольняє умови (LCM 1) та (LCM 2). Навпаки, якщо елемент m_1 задовольняє умови (LCM 1) та (LCM 2), то елементи m, m_1 ділять один одного і тому вони асоційовані. Таким чином, всі найменші спільні кратні елементів a, b (якщо вони існують) складають клас асоційованих елементів. Той факт, що елемент m — один із найменших спільних кратних елементів a, b , будемо позначати символом $m = \text{LCM}(a, b)$.

У довільному комутативному кільці не кожна пара елементів має найбільший спільний дільник та найменше спільне кратне. Зараз розглянемо більш вузький клас кілець, у яких найбільший спільний дільник та найменше спільне кратне існують для кожної пари елементів.

Комутативне кільце R без дільників нуля називається областю головних ідеалів, якщо кожен його ідеал головний.

20.5. Теорема. *Нехай R — область головних ідеалів. Для кожної пари його елементів a, b у кільці R існує їх найбільший спільний дільник та їх найменше спільне кратне. Більш того, співвідношення $d = \text{GCD}(a, b)$ і $dR = aR + bR$ (відповідно $m = \text{LCM}(a, b)$ та $mR = aR \cap bR$) рівносильні.*

Д о в е д е н н я . У розділі 16 ми відзначали, що $aR + bR$ — ідеал кільця R . Оскільки кожен його ідеал головний, існує такий елемент d , що $dR = aR + bR$. Включення $aR \leq dR$ та $bR \leq dR$ разом із пропозицією 20.3 показують, що $d | a$ і $d | b$.

Нехай c — спільний дільник елементів a, b . Застосовуючи знову пропозицію 20.3, отримаємо включення $aR \leq cR$ і $bR \leq cR$, із яких випливає, що $dR = aR + bR \leq cR$, а це, у свою чергу, показує, що c — дільник елемента d . Отже елемент d задовольняє умови (GCD 1), (GCD 2).

Навпаки, якщо d_1 — довільний найбільший спільний дільник елементів a, b , то як уже відзначалось раніше, елементи d, d_1 — асоційовані. Зокрема, вони породжують один і той самий ідеал, тобто $d_1R = dR = aR + bR$.

Оскільки кожен ідеал кільця R — головний, існує такий елемент m , що $mR = aR \cap bR$. Включення $mR \leq aR$ та $mR \leq bR$ разом із пропозицією 20.3 показують, що $a | m$ та $b | m$. Нехай c — спільний дільник елементів a, b . Застосовуючи знову пропозицію 20.3, отримаємо включення $cR \leq aR$ і $cR \leq bR$, із яких випливає, що $cR \leq aR \cap bR = mR$, а це, у свою чергу, показує, що m — дільник елемента c . Отже елемент m задовольняє умови (LCM 1) та (LCM 2). Навпаки, якщо m_1 — довільне найменше спільне кратне елементів a, b , то як вже відзначалося раніше, елементи m, m_1 — асоційовані. Зокрема, вони породжують один і той самий ідеал, тобто $m_1R = mR = aR \cap bR$.

20.6. Наслідок. *Нехай R — область головних ідеалів, a, b — елементи кільця R . Мають місце наступні твердження:*

(1) *Рівність $a = \text{GCD}(a, b)$ має місце тоді і тільки тоді, коли a ділить b .*

- (2) $\text{GCD}(a, O_R) = a$.
- (3) $\text{GCD}(ax, bx) = x \text{GCD}(a, b)$.
- (4) $\text{GCD}(\text{GCD}(a, b), c) = \text{GCD}(a, \text{GCD}(b, c))$.
- (5) Рівність $a = \text{LCM}(a, b)$ має місце тоді і тільки тоді, коли b ділить a .
- (6) $\text{LCM}(a, O_R) = O_R$.
- (7) $\text{LCM}(ax, bx) = x \text{LCM}(a, b)$.
- (8) $\text{LCM}(\text{LCM}(a, b), c) = \text{LCM}(a, \text{LCM}(b, c))$.
- (9) Якщо $d = \text{GCD}(a, b)$, то існують такі елементи $x, y \in R$, що $d = ax + by$.
- (10) Якщо a, b — ненульові елементи кільця R , то елементи $\text{GCD}(a, b)$ та $\text{LCM}(a, b)$ також ненульові.

Д о в е д е н н я . Майже всі ці твердження очевидні. Доведення потребує мабуть, тільки останнє. Нехай $d = \text{GCD}(a, b)$, $m = \text{LCM}(a, b)$. З теореми 20.5 отримуємо рівності $dR = aR + bR$, $mR = aR \cap bR$. Включення $aR \leq dR$ та $bR \leq dR$ гарантують той факт, що ідеал dR — ненульовий, тобто елемент d — ненульовий.

Припустимо, що $m = O_R$. Це означає, що $aR \cap bR = \{O_R\}$. Добуток ab належить як до ідеалу aR , так і до ідеалу bR , тобто належить до їх перетину. Отже $ab = O_R$, що суперечить нашому припущенню про кільце R . Отримане протиріччя показує, що й елемент m мусить бути ненульовим.

Елементи a, b кільця R називаються взаємно простими, якщо одиничний елемент кільця R є одним із їх найбільших спільних дільників.

20.7. Наслідок. *Нехай R — область головних ідеалів. Елементи a, b кільця R тоді і тільки тоді взаємно прості, коли існують такі елементи $x, y \in R$, що $e = ax + by$ (e — одиничний елемент R).*

Д о в е д е н н я . Необхідність випливає з наслідку 20.6. Нехай у кільці R існують такі елементи x, y , що $e = ax + by$. З цієї рівності випливає, що $e \in aR + bR$. З пропозиції 16.6 випливає, що $R = aR + bR$. Оскільки $eR = R$, то з теореми 20.5 отримуємо, що $e = \text{GCD}(a, b)$.

20.8. Наслідок. *Нехай R — область головних ідеалів, a, b — ненульові елементи кільця R , $d = \text{GCD}(a, b)$, $a = da_1$, $b = db_1$. Тоді елементи a_1, b_1 взаємно прості.*

Д о в е д е н н я . З наслідку 20.6 отримуємо існування у кільці R таких елементів x, y , що $d = ax + by$. Тепер маємо $d = ax + by = da_1x + db_1y$. Скорочуючи на d , що можливо, оскільки R не має дільників нуля, а елемент d , згідно з наслідком 20.6 ненульовий, отримаємо рівність $e = a_1x + b_1y$. Наслідок 20.7 доводить взаємну простоту елементів a_1 та b_1 .

Відзначимо наступні важливі властивості взаємно простих елементів.

20.9. Пропозиція. Нехай R — область головних ідеалів.

(1) Якщо елементи a, b — взаємно прості та елементи a, c — також взаємно прості, то a буде взаємно простим із добутком bc .

(2) Якщо елемент a ділить добуток bc і елементи a, b — взаємно прості, то a ділить c .

Доведення. (1) Із наслідку 20.7 отримуємо існування у кільці R таких елементів x_1, x_2, y_1, y_2 , що $e = ax_1 + bx_2$, $e = ay_1 + cy_2$. Тепер маємо

$$e = (ax_1 + bx_2)(ay_1 + cy_2) = a(ax_1y_1 + bx_2y_1 + cx_1y_2) + (bc)(x_2y_2).$$

Знову застосовуючи наслідок 20.7, отримаємо взаємну простоту елементів a та bc .

(2) Із наслідку 20.7 отримуємо існування у кільці R таких елементів x_1, x_2 , що $e = ax_1 + bx_2$. Тепер маємо $c = ce = cax_1 + cbx_2$, і оскільки a ділить bc , то a ділить c .

Наступне твердження показує взаємний зв'язок між найбільшим спільним дільником та найменшим спільним кратним.

20.10. Теорема. Нехай R — область головних ідеалів, a, b — ненульові елементи кільця R .

(1) Якщо t — найменше спільне кратне елементів a, b і $ab = td$, то d — найбільший спільний дільник елементів a, b .

(2) Якщо d — найбільший спільний дільник елементів a, b , $a = da_1$, $b = db_1$, то елемент $t = da_1b_1$ буде найменшим спільним кратним елементів a, b .

Доведення. (1) Оскільки t — спільне кратне елементів a, b , то $t = a_2a$, $t = b_2b$ для деяких елементів a_2, b_2 кільця R . Тепер маємо $ab = td = aa_2d$. Скорочуючи на ненульовий елемент a , отримаємо рівність $b = a_2d$, яка показує, що b ділиться на d . Аналогічно доводиться, що a ділиться на d .

Нехай тепер c — довільний спільний дільник елементів a, b , тобто $a = a_3c$, $b = b_3c$ для деяких елементів a_3, b_3 кільця R . Елемент a_3b_3c ділиться як на a , так і на b . З визначення найменшого спільного кратного отримуємо тепер існування такого елемента z у кільці R , що $a_3b_3c = tz$. Отже $td = ab = a_3b_3cc = tzc$. З наслідку 20.6 випливає, що t — ненульовий елемент, так що скорочуючи на нього, приходимо до рівності $d = zc$. Отже елемент d задовольняє умови (GCD 1), (GCD 2).

(2) Очевидно t ділить кожен з елементів a, b . Нехай c — довільне спільне кратне a, b , тобто $c = aa_4$, $c = bb_4$ для деяких елементів a_4, b_4 кільця R . Далі, $c = aa_4 = da_1a_4$, $c = bb_4 = db_1b_4$, а тому $da_1a_4 = db_1b_4$. З наслідку 20.6 випливає, що d — ненульовий елемент, так що скорочуючи на нього, приходимо до рівності $a_1a_4 = b_1b_4$. Згідно з наслідком 20.8 елементи a_1, b_1 — взаємно прості і тепер із пропозиції 20.9 отримаємо, що a_1 ділить b_4 : $b_4 = a_1x$. Отже $c = db_1b_4 = db_1a_1x = tx$. Таким чином, t задовольняє умови (LCM 1) та (LCM 2).

Ненульовий елемент p області цілісності R називається простим або нерозкладним, якщо $p \notin U(R)$ і p не може бути представлений у вигляді добутку двох власних дільників. Інакше кажучи, ненульовий і не інвертований елемент p тоді і тільки тоді буде простим, коли у всякому його розкладі $p = ab$ хоча б один із множників a або b буде інвертований.

Прості елементи області головних ідеалів тісно пов'язані з максимальними ідеалами. Ідеал M називається максимальним ідеалом кільця R , якщо для кожного ідеалу H , розташованого між M та R (тобто $M \leq H \leq R$) або $M = H$, або $H = R$.

20.11. Лема. Нехай R — кільце. Ідеал M тоді і тільки тоді є максимальним у R , коли R/M — просте кільце. Зокрема, ідеал M комутативного кільця R тоді і тільки тоді буде максимальним, коли R/M — поле.

Доведення. Нехай M — максимальний ідеал кільця R та нехай Q — довільний ідеал фактор — кільця R/M . Позначимо через H повний прообраз Q відносно епіморфізму σ_M . З пропозиції 16.10 випливає, що H — ідеал у кільці R . Оскільки $M = \text{Ker } \sigma_M$, $M \leq H$. Оскільки σ_M — епіморфізм, то з пропозиції 16.10 випливає, що $\sigma_M(H)$ — ідеал фактор-кільця R/M . З того факту, що M — максимальний ідеал R , випливає одна з рівностей $M = H$, або $H = R$. У першому випадку $Q = \sigma_M(M)$ — нульовий ідеал R/M , а у другому випадку $Q = \sigma_M(R) = R/H$. Це й означає, що R/M — просте кільце.

Навпаки, нехай R/M — просте кільце, H — ідеал, розташований між M та R . Знову за пропозицією 16.10 $\sigma_M(H)$ — ідеал фактор-кільця R/M . З того факту, що це фактор-кільце просте, отримаємо, що або $\sigma_M(H)$ — нульовий ідеал R/M , або $\sigma_M(H) = R/H$. У першому випадку $H = \text{Ker } \sigma_M = M$. Розглянемо другий випадок. Нехай $x \in R$. З рівності $\sigma_M(H) = R/H$ випливає існування такого елемента $h \in H$, що $x + M = h + M$. Звідси $x - h = y \in M$, і, використовуючи включення $M \leq H$, будемо мати $x = h + y \in H$. Це і свідчить про те, що $H = R$. Таким чином, M — максимальний ідеал кільця R .

Якщо кільце R — комутативне, то для доведення другого твердження достатньо використати теорему 16.9.

Відзначимо наступні важливі властивості простих елементів.

20.12. Лема. Нехай R — область головних ідеалів.

(1) Якщо p — простий елемент кільця R , то для довільного елемента a кільця R або p ділить a , або елементи a , p — взаємно прості.

(2) Елемент p кільця R тоді і тільки тоді буде простим, коли ідеал pR буде максимальним у кільці R .

Доведення. (1) Нехай $d = \text{GCD}(a, p)$. Оскільки d — дільник елемента p , то або елементи p та d — асоційовані, або $d \in U(R)$. У першому випадку p також буде найбільшим спільним дільником a і p , зокрема, p ділить a . У другому випадку елементи a і p взаємно прості.

(2) Нехай p — простий елемент кільця R , H — ідеал R , розташований між pR та R . Знайдеться такий елемент $y \in R$, що $H = yR$. Включення $pR \leq yR$ разом із пропозицією 20.3 показують, що y — дільник p . З простоти елемента p отримуємо, що або y є асоційованим з p (і в цьому випадку $pR = yR = H$), або $y \in U(R)$ (у цьому випадку $H = yR = R$). Навпаки, нехай pR — максимальний ідеал кільця R . Якщо $p = zw$ для деяких елементів $z, w \in R$, то з пропозиції 20.3 випливає включення $pR \leq zR$. У свою чергу, із цього випливає, що або $pR = zR$, або $zR = R$. У першому випадку елементи p та z — асоційовані, тобто, $w \in U(R)$. У другому випадку $z \in U(R)$. Отже p — простий елемент кільця R .

Тепер уже можливо навести дві важливі теореми про існування розкладів на прості множники та однозначність таких розкладів.

20.13. Теорема. Нехай R — область головних ідеалів, $0_R \neq a \in R$.

(1) Якщо $a \notin U(R)$, то a розкладається у добуток простих елементів кільця R .

(2) Якщо $a \notin U(R)$ і $a = p_1 \dots p_n = q_1 \dots q_m$ — два розклади у добуток простих елементів кільця R , то $n = m$ і елементи другого розкладу можна перенумерувати таким чином, що $q_j = u_j p_j$, для деяких $u_j \in U(R)$, $1 \leq j \leq n$.

Д о в е д е н н я . (1) Припустимо, що перше твердження теореми невірне. Позначимо через D підмножину тих ненульових елементів $R \setminus U(R)$, які не розкладаються у добуток простих елементів. За нашим припущенням $D \neq \emptyset$. Розглянемо зростаючий ланцюжок таких ідеалів

$$d_1 R \leq d_2 R \leq \dots \leq d_n R \leq \dots,$$

що $d_n \in D$ для кожного $n \in \mathbb{N}$. За наслідком 16.5 $H = \bigcup_{n \in \mathbb{N}} d_n R$ буде ідеалом кільця R . Оскільки кожен ідеал R є головним, $H = dR$ для деякого елемента $d \in R$. З визначення H випливає існування такого номера $k \in \mathbb{N}$, що $d \in d_k R$. Звідси випливає включення $dR \leq d_k R$. З іншого боку, $d_k R \leq H = dR$, так що $d_k R = dR$.

Нехай $a = a_1$ — довільний елемент підмножини D . Припустимо спочатку, що для кожного ідеалу bR , який має властивості $aR \leq bR$ і $aR \neq bR$, елемент b не належить до D . Якщо $b \in U(R)$, то $bR = R$. Припустимо тепер, що $b \notin U(R)$. Враховуючи вибір підмножини D , це свідчить про те, що b розкладається у добуток простих елементів. З пропозиції 20.3 випливає, що b — дільник a , тобто $a = bc$ для деякого елемента $c \in R$. Маємо також $aR \leq cR$. Якщо припустити, що $aR = cR$, то елементи a, c — асоційовані: $c = ua$ для деякого $u \in U(R)$. Тоді маємо $a = bc = bua$, звідки $b \in U(R)$, а це суперечить припущенню відносно b . Отримане протиріччя показує, що $aR \neq cR$. Якщо $c \in U(R)$, то $a = bc$ розкладається у добуток простих елементів. Якщо $c \notin U(R)$, то зі співвідношення $c \notin D$ отримуємо, що c розкладається у добуток простих елементів.

Але тоді і $a = bc$ розкладається у такий же добуток. Отримане протиріччя показує, що для кожного елемента $a = a_1$ із підмножини D існує елемент a_2 , що має властивості: $a_2 \in D$, $a_1 R \leq a_2 R$ і $a_1 R \neq a_2 R$. Однак це дає можливість побудувати нескінченний зростаючий ланцюжок таких ідеалів

$$a_1 R \leq a_2 R \leq \dots \leq a_n R \leq \dots,$$

що $a_n \in D$ для кожного $n \in N$. Як ми вже показали вище, це також неможливо. Отримане протиріччя показує, що підмножина D — пуста.

(2) Друге твердження будемо доводити, використовуючи індукцію за числом n . Якщо $n = 1$, то $a = p_1$ — простий елемент. З визначення простого елемента випливає тепер, що один з множників другого розкладу, наприклад q_1 , є асоційованим з p_1 , а добуток усіх інших — елемент із групи $U(R)$.

Нехай тепер $n > 1$, і припустимо, що твердження уже доведено для елементів, що мають розклад у добуток простих елементів у кількості, меншій ніж n . Маємо $p_1 \dots p_n = q_1 \dots q_m$. З леми 2.12 випливає, що або елементи p_1, q_1 — асоційовані, або ці елементи взаємно прості. У другому випадку з пропозиції 20.9 випливає, що p_1 ділить добуток $q_2 \dots q_m$. Знову або елементи p_1, q_2 — асоційовані, або ці елементи взаємно прості і тоді p_1 ділить добуток $q_3 \dots q_m$.

Повторюючи ці аргументи достатню кількість разів, отримаємо нарешті, що знайдеться такий номер k , що елементи p_1, q_k — асоційовані. Змінюючи нумерацію, можемо вважати, що асоційованими будуть елементи p_1, q_1 — асоційовані, тобто $q_1 = u_1 p_1$, де $u_1 \in U(R)$.

Тепер $p_1 \dots p_n = (p_1 u_1) q_2 \dots q_m = p_1 (u_1 q_2) q_3 \dots q_m$. Скорочуючи на p_1 , отримаємо

$$p_2 \dots p_n = r_2 q_3 \dots q_m, \quad r_2 = u_1 q_2.$$

До елемента $p_2 \dots p_n$ уже можемо застосувати індуктивну гіпотезу. Отже $n - 1 = m - 1$, тобто $n = m$, і (можливо після деякого перенумерування) $r_2 = v p_2$, $q_j = u_j p_j$, для деяких $v, u_j \in U(R)$, $3 \leq j \leq n$. Далі з рівностей $r_2 = v p_2$ та $r_2 = u_1 q_2$ будемо мати $q_2 = u_2 p_2$, де $u_2 = u_1^{-1} v \in U(R)$.

Указане представлення можна зробити просто однозначним наступним чином. У кожному класі асоційованості, що складається з простих елементів області головних ідеалів R , виберемо по одному представнику і позначимо через $\sigma(R)$ множину всіх цих представників. Тоді кожен простий елемент R кільця буде асоційованим із деяким елементом множини $\sigma(R)$. З теореми 20.13 випливає тепер, що кожен ненульовий елемент a кільця R може бути представлений у вигляді $a = u p_1 \dots p_n$, $p_1, \dots, p_n \in \sigma(R)$, $u \in U(R)$ (якщо $n = 0$, то $a = u \in U(R)$, тобто такі представлення дійсно охоплюють усі ненульові елементи кільця R). Представлення елемента a у такому вигляді вже буде просто однозначним. Більше того, об'єднавши разом однакові прості множники, отримаємо представлення $a = u p_1^{k_1} \dots p_m^{k_m}$, де

$p_1, \dots, p_m$ — попарно різні елементи множини $\sigma(R)$, $u \in U(R)$. Розглядаючи розклади двох ненульових елементів $a, b \in R$, можна вважати, що в указані розклади входять одні й ті ж самі елементи з множини $\sigma(R)$, якщо домовитись про те, що деякі з чисел $k_1, \dots, k_m$ можуть дорівнювати нулю. Тепер із теореми 20.13 отримуємо

20.14. Наслідок. Нехай R — область головних ідеалів, a, b — ненульові елементи кільця R , $a = up_1^{k_1} \dots p_m^{k_m}$, $b = vp_1^{t_1} \dots p_m^{t_m}$, де $p_1, \dots, p_m$ — попарно різні елементи множини $\sigma(R)$, $u, v \in U(R)$.

(1) Елемент a ділить елемент b тоді і тільки тоді, коли $k_j \leq t_j$, для кожного j , $1 \leq j \leq m$.

(2) $\text{GCD}(a, b) = p_1^{d_1} \dots p_m^{d_m}$, де $d_j = \min\{k_j, t_j\}$ для кожного j , $1 \leq j \leq m$.

(3) $\text{LCM}(a, b) = p_1^{q_1} \dots p_m^{q_m}$, де $q_j = \max\{k_j, t_j\}$ для кожного j , $1 \leq j \leq m$.

Зокрема, елементи a, b будуть взаємно простими, коли прості множники, що входять до розкладу елемента a , не входять до розкладу елемента b . Також треба відзначити той факт, що довівши існування розкладу на прості множники, ми не отримали ніяких результатів, що дали б можливість реально здобути цей розклад. Це питання не просте. Навіть у випадку кільця цілих чисел доводиться задовольнятися різними варіаціями простого перебору простих чисел, які менші даного.

Комутативне кільце R без дільників нуля називається факторіальною областю або областю з однозначним розкладом, якщо вона задовольняє наступні умови:

(1) якщо a — ненульовий елемент R і $a \notin U(R)$, то a розкладається у добуток простих елементів кільця R ;

(2) якщо $a = p_1 \dots p_n = q_1 \dots q_m$ — два розклади у добуток простих елементів кільця R , то $n = m$ і елементи другого розкладу можна перенумерувати таким чином, що $q_j = u_j p_j$, для деяких $u_j \in U(R)$, $1 \leq j \leq n$.

З теореми 20.13 отримуємо, що кожна область головних ідеалів є областю з однозначним розкладом. Якщо R — область з однозначним розкладом, то для кожної пари її елементів (а значить, і для кожного скінченного набору елементів) існує найбільший спільний дільник і найменше спільне кратне. Вони знаходяться так, як це робилось у наслідку 20.14 для областей головних ідеалів. Завершуючи цю тему, покажемо, що не кожна область з однозначним розкладом буде областю головних ідеалів і zarazом розглянемо деякі важливі приклади областей з однозначним розкладом. Спочатку отримаємо деяке узагальнення теореми 17.1.

20.15. Теорема. Нехай R — комутативне кільце без дільників нуля, $f(X), g(X) \in R[X]$, причому $g(X) \neq 0_R$. Нехай

$$k = \max\{\deg f(X) - \deg g(X) + 1, 0\},$$

d — старший коефіцієнт полінома $g(X)$. Тоді знайдуться

такі поліноми $q(X), r(X) \in R[X]$, що $d^h f(X) = q(X)g(X) + r(X)$, де або $r(X) = O_R$ або $\deg r(X) < \deg g(X)$. Таке представлення полінома $f(X)$ є єдиним.

Д о в е д е н н я . Нехай

$$f(X) = a_0 + a_1 X + \dots + a_m X^m,$$

$$g(X) = b_0 + b_1 X + \dots + b_n X^n,$$

де $a_m = c \neq O_R$, $b_n = d \neq O_R$. Застосуємо індукцію за числом n . Якщо $\deg g(X) > \deg f(X)$, то покладемо $r(X) = f(X)$, $q(X) = O_R$. Тому розглянемо випадок, коли $\deg g(X) \leq \deg f(X)$.

Якщо $\deg f(X) = 0$, то $r(X) = O_R$, $q(X) = c$. Нехай тепер $m > 0$ і припустимо, що теорема доведена для поліномів, степінь яких менший ніж m . Поліном $cX^{m-n}g(X)$ має степінь m і коефіцієнт його при X^n дорівнює cd . Тому степінь полінома $df(X) - cX^{m-n}g(X)$ уже менший від m . За індуктивним припущенням існують такі поліноми $q_1(X), r(X)$, коефіцієнти яких належать до кільця R , що

$$d^{(m-1)-n+1}(df(X) - cX^{m-n}g(X)) = q_1(X)g(X) + r(X),$$

де або $r(X) = O_R$, або $\deg r(X) < \deg g(X)$. Тепер

$$d^h f(X) = q(X)g(X) + r(X),$$

де $q(X) = cd^{m-n}X^{m-n} + q_1(X)$.

Той факт, що таке представлення єдине, доводиться так, як це робилось при доведенні теореми 17.1.

Нехай R — область з однозначним розкладом, $f(X) \in R[X]$. Поліном $f(X)$ називається *примітивним*, якщо найбільший спільний дільник всіх його коефіцієнтів дорівнює одиничному елементу.

Кожний поліном $f(X) \in R[X]$ може бути записаний у вигляді $f(X) = cg(X)$, де $c \in R$, $g(X) \in R[X]$ і $g(X)$ — примітивний поліном. Дійсно, у цьому випадку c — найбільший спільний дільник всіх коефіцієнтів полінома $f(X)$. Навпаки, якщо $f(X) = c_1 g_1(X)$, де $g_1(X)$ — примітивний поліном, то очевидно c_1 також буде найбільшим спільним дільником всіх коефіцієнтів полінома $f(X)$. Отже елементи c і c_1 — асоційовані. Елемент c будемо називати *вмістом* полінома $f(X)$ і позначати $c(f(X))$ або, коротше, $c(f)$. Поліном $f(X)$ є примітивним тоді і тільки тоді, коли $c(f) \in U(R)$.

20.16. Пропозиція (лема Гауса). Нехай R — область з однозначним розкладом, $f(X), g(X) \in R[X]$. Якщо поліноми $f(X)$ та $g(X)$ — примітивні, то їх добуток також буде примітивним поліномом. У загальному випадку $c(fg) = c(f)c(g)$.

Д о в е д е н н я . Нехай

$$f(X) = a_0 + a_1 X + \dots + a_m X^m,$$

$$g(X) = b_0 + b_1 X + \dots + b_n X^n,$$

$$f(X)g(X) = c_0 + c_1 X + \dots + c_{m+n} X^{m+n}.$$

Нехай спочатку $f(X)$, $g(X)$ — примітивні поліноми. Припустимо, що їх добуток не буде примітивним поліномом і виберемо простий дільник q елемента $c(fg)$. Тоді q ділить кожний коефіцієнт полінома $f(X)g(X)$, тобто $q|c_j$ для кожного j , $0 \leq j \leq m+n$. Оскільки поліном $f(X)$ — примітивний, існує такий номер k , що q ділить коефіцієнти $a_0, a_1, \dots, a_{k-1}$, але q не ділить a_k . З аналогічної причини, існує такий номер t , що q ділить коефіцієнти $b_0, b_1, \dots, b_{t-1}$, але q не ділить b_t . Маємо

$$c_{k+t} = a_0 b_{k+t} + a_1 b_{k+t-1} + \dots + a_{k-1} b_{t+1} + a_k b_t + \\ + a_{k+1} b_{t-1} + \dots + a_{k+t} b_0.$$

З цієї рівності випливає, що елемент q мусить ділити добуток $a_k b_t$, що неможливо. Отримане протиріччя показує, що $f(X)g(X)$ — примітивний поліном.

Розглянемо загальний випадок. Тепер

$$f(X) = c(f) f_1(X), \quad g(X) = c(g) g_1(X),$$

де $f_1(X)$, $g_1(X)$ — примітивні поліноми. Далі, $f(X)g(X) = c(f)c(g)f_1(X)g_1(X)$. Як було тільки що доведено, добуток $f_1(X)g_1(X)$ є примітивним поліномом, а це означає, що $c(f)c(g)$ буде вмістом полінома $f(X)g(X)$.

20.17. Лема. *Нехай R — область з однозначним розкладом, $f(X), g(X) \in R[X]$. Припустимо, що поліном $g(X)$ — примітивний та ділить добуток $df(X)$ для деякого (ненульового) елемента $d \in R$. Тоді $g(X)$ ділить $f(X)$.*

Доведення. Маємо $df(X) = g(X)h(X)$ для деякого полінома $h(X) \in R[X]$. З пропозиції 20.16 отримаємо рівність $dc(f) = c(g)c(h)$. Оскільки $c(g) \in U(R)$, то $c(h) = duc(f)$, де $u = (c(g))^{-1}$. Далі $h(X) = c(h)h_1(X)$, де $h_1(X)$ — примітивний поліном, і тепер маємо

$$df(X) = g(X)h(X) = g(X)c(h)h_1(X) = g(X)duc(f)h_1(X),$$

і скорочуючи на d , остаточно маємо $f(X) = c(f)ug(X)h_1(X)$.

20.18. Лема. *Нехай R — область з однозначним розкладом, $f(X), g(X), p(X)$ — поліноми над кільцем R . Припустимо, що $p(X)$ — простий елемент кільця $R[X]$. Якщо $p(X)$ ділить добуток $f(X)g(X)$, то або $p(X)$ ділить $f(X)$, або $p(X)$ ділить $g(X)$.*

Доведення. Якщо $\deg p(X) = 0$, то $p(X)$ — елемент кільця R , зокрема, $p(X) = p$ — простий елемент R . У цьому випадку p ділить елемент $c(fg) = c(f)c(g)$, і з простоти p випливає, що він ділить хоча б один з елементів $c(f)$, $c(g)$ (див. лему 20.14, яка залишається вірною і для областей з однозначним розкладом).

Припустимо, що $\deg p(X) > 0$. З визначення простого елемента зокрема, отримаємо, що поліном $p(X)$ є примітивним. Будемо вважати також, що $p(X)$ не ділить $f(X)$. Нехай

$H = p(X)R[X] + f(X)R[X]$. Серед усіх ненульових поліномів ідеалу H виберемо поліном $h(X)$, що має найменший степінь. Позначимо через d старший коефіцієнт полінома $h(X)$. З теореми 20.15 випливає існування таких поліномів $q(X)$, $r(X) \in R[X]$, що

$$d^k f(X) = q(X)h(X) + r(X),$$

де або $r(X) = 0_R$ або $\deg r(X) < \deg h(X)$.

З рівності

$$r(X) = d^k f(X) - q(X)h(X)$$

випливає, що $r(X) \in H$.

З огляду на вибір $r(X)$ залишається тільки випадок $r(X) = 0_R$, тобто $d^k f(X) = q(X)h(X)$. Перепишемо тепер $h(X)$ у вигляді: $h(X) = c(h)h_1(X)$, де $h_1(X)$ — примітивний поліном. З леми 20.17 випливає, що $h_1(X)$ ділить $f(X)$. За допомогою аналогічних аргументів отримаємо також, що $h_1(X)$ ділить $p(X)$: $p(X) = h_1(X)v(X)$ для деякого полінома $v(X) \in R[X]$. Якщо припустити, що $\deg h_1(X) > 0$, то, враховуючи той факт, що $p(X)$ — простий елемент кільця поліномів, приходимо до співвідношення $v(X) \in U(R[X]) = U(R)$. Інакше кажучи, $h_1(X)$ та $p(X)$ — асоційовані. Оскільки $h_1(X)$ ділить $f(X)$, то тоді $p(X)$ мусить ділити $f(X)$, що суперечить нашому припущенню. Отримано протиріччя показує, що $\deg h_1(X) = 0$, тобто $h_1(X) = w \in R$, $w \in H$, $w = q_1(X)p(X) + q_2(X)f(X)$ для деяких поліномів $q_1(X)$, $q_2(X) \in R[X]$. Тепер маємо

$$h_1(X)g(X) = wg(X) = q_1(X)p(X)g(X) + q_2(X)f(X)g(X).$$

Ця рівність показує, що $p(X)$ ділить $wg(X)$. Як було вже помічено, поліном $p(X)$ — примітивний, і тепер лема 20.17 показує, що $p(X)$ ділить $g(X)$.

20.19. Теорема. *Якщо R — область з однозначним розкладом, то і $R[X]$ буде областю з однозначним розкладом.*

Д о в е д е н н я . Спочатку будемо доводити, що кожен елемент $f(X)$ кільця $R[X]$ розкладається на прості множники. Якщо $\deg f(X) = m = 0$, то $f(X)$ — елемент кільця R , і з умов теореми випливає, що він має розклад на прості множники.

Нехай тепер $m > 0$ і припустимо, що теорема доведена для поліномів, степінь яких менший ніж m . Запишемо поліном $f(X)$ у вигляді $f(X) = c(f)f_1(X)$, де $f_1(X)$ — примітивний поліном. Якщо $f_1(X)$ не розкладається у добуток простих елементів, то все доведено. Тому припустимо, що $f_1(X) = g(X)h(X)$, де $\deg g(X) < \deg f_1(X)$ та $\deg h(X) < \deg f_1(X)$ (якщо, наприклад, $\deg g(X) = \deg f_1(X)$, то $\deg h(X) = 0$, а це означає, що $h(X)$ — елемент кільця R , і отримуємо протиріччя з примітивністю полінома $f_1(X)$). Тепер до поліномів $g(X)$ та $h(X)$ можна застосувати індуктивне припущення і отримати, що $f_1(X)$, а тобто і $f(X)$, розкладається на прості множники.

Однозначність доводиться за допомогою леми 20.18 і тих аргументів, які були використані при доведенні теореми 20.13.

20.20. Наслідок. Якщо R — область з однозначним розкладом, то і $R[X_1, \dots, X_n]$ буде областю з однозначним розкладом.

20.21. Наслідок. Якщо F — поле, то $F[X_1, \dots, X_n]$ буде областю з однозначним розкладом.

20.22. Наслідок. $Z[X_1, \dots, X_n]$ буде областю з однозначним розкладом.

Використовуючи щойно отримані результати, досить просто можна показати, що існують області з однозначним розкладом, які не є областями головних ідеалів. Нехай F — поле, тоді за наслідком 20.21 кільце поліномів $F[X, Y]$ від двох невідомих X та Y буде областю з однозначним розкладом. Розглянемо тепер ідеал $H = XF[X, Y] + YF[X, Y]$. Припустимо, що $H = f(X, Y)F[X, Y]$. Маємо зокрема, $X = h(X, Y)f(X, Y)$ і $Y = g(X, Y)f(X, Y)$. З теореми 19.1 випливає, що $\deg h(X, Y) = 0 = \deg g(X, Y)$, тобто $h(X, Y) = u$, $g(X, Y) = v$ — ненульові елементи поля F . Але ж тоді $f(X, Y) = u^{-1}X = v^{-1}Y$, що є абсурдним, оскільки X та Y — незалежні невідомі.

У завершення наведемо також приклад кільця, в якому розклад на прості множники є можливим для кожного елемента, але не завжди однозначним. Розглянемо наступну загальну конструкцію квадратичних полів і кілець. Нехай r — таке ціле число, що $\sqrt{r} \notin \mathbb{Q}$. Покладемо

$$\mathbb{Q}[\sqrt{r}] = \{a + b\sqrt{r} \mid a, b \in \mathbb{Q}\},$$

$$\mathbb{Z}[\sqrt{r}] = \{a + b\sqrt{r} \mid a, b \in \mathbb{Z}\}.$$

Нехай α, β — довільні елементи $\mathbb{Q}[\sqrt{r}]$, $\alpha = a + b\sqrt{r}$, $\beta = a_1 + b_1\sqrt{r}$, тоді

$$\alpha - \beta = (a - a_1) + \sqrt{r}(b - b_1),$$

$$\alpha\beta = (aa_1 + bb_1r) + \sqrt{r}(ab_1 + ba_1).$$

Таким чином, $\alpha - \beta, \alpha\beta \in \mathbb{Q}[\sqrt{r}]$. Якщо ж $\alpha, \beta \in \mathbb{Z}[\sqrt{r}]$, то $\alpha - \beta, \alpha\beta \in \mathbb{Z}[\sqrt{r}]$. З теореми 15.4 отримуємо, що $\mathbb{Q}[\sqrt{r}], \mathbb{Z}[\sqrt{r}]$ — підкільця $\mathbb{C}$. Також $1 \in \mathbb{Z}[\sqrt{r}]$. Нехай $\alpha \neq 0$, тоді очевидно,

$$\alpha^{-1} = (a/(a^2 - rb^2)) + \sqrt{r}(-b/(a^2 - rb^2)) \in \mathbb{Q}[\sqrt{r}].$$

Теорема 15.10 показує, що $\mathbb{Q}[\sqrt{r}]$ — підполе $\mathbb{C}$. Якщо $r > 0$, то $\mathbb{Q}[\sqrt{r}]$ називають дійсним квадратичним полем, якщо ж $r < 0$, то $\mathbb{Q}[\sqrt{r}]$ називають уявним квадратичним полем.

Нормою числа $\alpha = a + b\sqrt{r}$ називається раціональне число $N(\alpha) = a^2 - rb^2$. Якщо $N(\alpha) = 0$, то $a^2/b^2 = r$. Оскільки $\sqrt{r} \notin \mathbb{Q}$, звідси отримуємо, що $a = 0$, а потім і $b = 0$. Таким чином,

$$N(\alpha) = 0 \text{ тоді і тільки тоді, коли } \alpha = 0.$$

Простим підрахунком можна упевнитись у тому, що

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Зокрема,

$$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}),$$

тобто

$$N(\alpha^{-1}) = 1/N(\alpha).$$

Також відзначимо, що для елементів кільця $Z[\sqrt{r}]$ їх норма є цілим числом, більш того, для випадку $r < 0$ маємо $N(\alpha) \geq 0$ для кожного елемента $\alpha \in Z[\sqrt{r}]$.

20.23. Пропозиція. Нехай $r \in Z$ і $r < 0$.

(1) $U(Z[\sqrt{r}]) = \{1, -1\}$, $r \neq 1$; $U(Z(i)) = \{1, -1, i, -i\}$.

(2) Нехай α — ненульовий елемент кільця $Z[\sqrt{r}]$. Якщо $\alpha \notin U(Z[\sqrt{r}])$, то α розкладається у добуток простих елементів.

Доведення. (1) Нехай $d = -r$, тоді $d > 0$. Якщо $\alpha = a + b\sqrt{r} \in U(Z[\sqrt{r}])$, то з рівності $1 = N(\alpha)N(\alpha^{-1})$ і того факту, що $N(\alpha)$ — ціле число, отримуємо, що $N(1) = 1$. Але ж рівність $a^2 + db^2 = 1$ має у множині цілих чисел такі розв'язки:

$a = 0, b = 1$; $a = 0, b = -1$; $a = 1, b = 0$; $a = -1, b = 0$, для випадку, коли $d = 1$;

$a = 1, b = 0$; $a = -1, b = 0$, для випадку, коли $d > 1$.

(2) Для доведення цього твердження використаємо індукцію за числом $N(\alpha)$. Оскільки $\alpha \notin U(Z[\sqrt{r}])$, то $N(\alpha) > 1$.

Рівність $N(\alpha) = 2$ можлива тільки у випадках, коли $d = 1$, тоді

$$\alpha \in \{1 + i, 1 - i, -1 + i, -1 - i\},$$

і коли $d = 2$, тоді $\alpha \in \{i\sqrt{2}, i\sqrt{2}\}$.

Рівність $N(\alpha) = 3$ можлива тільки у випадках, коли $d = 2$, тоді

$$\alpha \in \{1 + i\sqrt{2}, 1 - i\sqrt{2}, -1 + i\sqrt{2}, -1 - i\sqrt{2}\},$$

і коли $d = 3$, тоді $\alpha \in \{i\sqrt{3}, i\sqrt{3}\}$.

Рівність $N(\alpha) = 4$ можлива тільки у випадках, коли $d = 1$, тоді $\alpha \in \{2, -2, 2i, -2i\}$; коли $d = 2$, тоді $\alpha \in \{2, -2\}$; коли $d = 3$, тоді $\alpha \in \{2, -2\}$; коли $d = 4$, тоді $\alpha \in \{2, -2, 2i, -2i\}$; коли $d > 4$, тоді $\alpha \in \{2, -2\}$.

Неважко переконатись у тому, що в усіх цих випадках твердження має місце. Нехай тепер $N(\alpha) > 4$, і припустимо, що для всіх елементів, які мають меншу норму, існування розкладу на прості елементи уже доведено. Якщо α — простий елемент, то все доведено. Тому припустимо, що $\alpha = \beta\gamma$, де β, γ — власні дільники α . Зокрема, $\beta, \gamma \notin U(Z[\sqrt{r}])$, а тому $N(\beta) > 1$, $N(\gamma) > 1$. З рівності $N(\beta\gamma) = N(\beta)N(\gamma)$, отримуємо нерівності $N(\beta) < N(\alpha)$, $N(\gamma) < N(\alpha)$. Але згідно з індуктивною

гіпотезою, тоді елементи β, γ , а з ними й елемент α , розкладаються у добуток простих елементів.

Тепер уже можна вказати конкретне значення числа r , для яких у кільці $Z[\sqrt{r}]$ існують елементи, які мають два різних розклади на прості елементи. Одним із таких значень є $r = -5$. Дійсно, наприклад, маємо

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}).$$

З пропозиції 20.23 випливає, що елементи 3 та $(2 + i\sqrt{5})$, 3 та $(2 - i\sqrt{5})$ не асоційовані. Залишається тільки упевнитись у тому, що елементи 3, $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ будуть простими у кільці $Z[\sqrt{5}]$.

Нехай $\alpha \in \{3, 2 + i\sqrt{5}, 2 - i\sqrt{5}\}$. Маємо $N(\alpha) = 9$, тому з існування розкладу $\alpha = \beta\gamma$, де β, γ — власні дільники α , і рівності $N(\beta\gamma) = N(\beta)N(\gamma)$, отримуємо що $N(\beta) = N(\gamma) = 3$. Але очевидно, що рівняння $x^2 + 5y^2 = 3$ не має розв'язків у кільці цілих чисел. Це і доводить простоту вказаних елементів.

4

21. ЕВКЛІДОВІ КІЛЬЦЯ

У попередньому розділі деякі звичні арифметичні поняття і результати були розширені з кільця цілих чисел на області головних ідеалів. Зокрема, було доведено існування найбільшого спільного дільника і найменшого спільного кратного елементів в таких кільцях, а також існування розкладу на прості елементи. Але, на жаль, існує принципова різниця між існуванням об'єкта та його конкретним знаходженням. Довівши існування, ми не отримали у попередньому розділі жодного алгоритму. В даному розділі буде розглянутий більш вузький, ніж області головних ідеалів, клас кілець, для якого деякі з таких алгоритмів існують.

Комутативне кільце R без дільників нуля називається евклідовим, якщо існує така функція $\delta: R \setminus \{O_R\} \longrightarrow N_0$, що виконуються наступні умови:

(Е 1) $\delta(xy) \geq \delta(x)$ для довільних елементів $x, y \in R \setminus \{O_R\}$;

(Е 2) для кожної пари елементів $x, y \in R$, де $y \neq O_R$ у кільці R існують такі елементи w, z , що $x = wy + z$, де або $z = O_R$ або $\delta(z) < \delta(y)$.

Першим природним прикладом евклідових кілець є кільце Z цілих чисел, де $\delta(x) = |x|$. Теорема про можливість такого ділення у кільці цілих чисел була наведена Евклідом у його знаменитій енциклопедії давньогрецької математики і тому кільця, що мають вказані вище властивості, були названі евклідовими. З теореми 17.1 випливає, що і кільця поліномів від одного невідомого над полем буде евклідовим. Наведемо ще інші приклади евклідових кілець.

21.1. Пропозиція. Кільце $Z[i]$ буде евклідовим, якщо функцію δ визначити за правилом $\delta(\alpha) = N(\alpha)$ для кожного елемента $\alpha \in Z[i]$.

Д о в е д е н н я . Той факт, що $Z[i]$ — підкільце поля комплексних чисел, був доведений у розділі 20 для більш загальної ситуації. Зокрема звідси випливає, що кільце $Z[i]$ не має дільників нуля. Якщо $\alpha = a + bi$, $a, b \in Z$, $N(\alpha) = a^2 + b^2$. У розділі 20 також була доведена рівність $N(\alpha\beta) = N(\alpha)N(\beta)$, з якої випливає аксіома (Е 1).

Нехай тепер $\alpha = a + bi$, $\beta = c + di \neq 0$, де $a, b, c, d \in Z$. Тоді $\alpha/\beta = x + yi$, де вже $a, b \in Q$. Знайдуться такі числа $u, v \in Z$, що $|x - u| = 1/2$ та $|y - v| = 1/2$.

Покладемо тепер $\delta = u + vi$, $\rho = \alpha - \beta\delta$. За самим визначенням $\delta, \rho \in Z[i]$. Маємо або $\rho = 0$, або

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\delta) = N(\beta((\alpha/\beta) - \delta)) = N(\beta)N((\alpha/\beta) - \delta) = \\ &= N(\beta)N((x - u) + (y - v)i) = N(\beta)((x - u)^2 + (y - v)^2) \leq \\ &\leq N(\beta)(1/4 + 1/4) = 1/2 N(\beta) < N(\beta). \end{aligned}$$

Таким чином, і аксіома (Е 2) також має місце.

Кільце $Z[i]$ називається *кільцем цілих гаусових чисел* на честь К.Ф. Гауса, який вперше детально вивчив його арифметичні властивості.

Розглянемо інший приклад. Нехай

$$\omega = (-1 + \sqrt{-3})/2,$$

тоді число ω є коренями полінома $X^2 + X + 1 \in Z[X]$.

З рівності

$$(X - 1)(X^2 + X + 1) = X^3 - 1$$

отримуємо, що ω буде примітивним коренем третього степеня з 1. Зокрема $\omega^2 + \omega + 1 = 0$, так що

$$\omega^2 = -\omega - 1 = (-1 - \sqrt{-3})/2.$$

З результатів розділу 17 отримуємо, що підкільце $Z[\omega]$ складається з усіх чисел, що мають вигляд $x + y\omega$, $x, y \in Z$. Оскільки $Z[\omega]$ — підкільце поля комплексних чисел, то воно не має дільників нуля. Відзначимо також, що $Z[\omega]$ є замкненим відносно комплексного спряження. Дійсно,

$$\Delta(\sqrt{-3}) = \Delta(i\sqrt{3}) = -i\sqrt{3} = -\sqrt{-3},$$

і тому $\Delta(\omega) = \omega^2$. Таким чином, якщо $\alpha = x + y\omega$, то

$$\Delta(\alpha) = x + y\Delta(\omega) = x + y\omega^2 = (x - y) - y\omega \in Z[\omega].$$

21.2. Пропозиція. Кільце $Z[\omega]$ буде евклідовим, якщо функцію δ визначити за правилом $\delta(\alpha) = N(\alpha)$ для кожного елемента

$\alpha \in Z[\varpi]$ (тут $N(\alpha)$ — квадрат абсолютної величини комплексного числа α).

Доведення. З того факту, що $Z[\varpi]$ — підкільце поля комплексних чисел, випливає, що кільце $Z[\varpi]$ не має дільників нуля. Якщо $\alpha = a + b\varpi$, $a, b \in Z$, то простий підрахунок доводить рівність $N(\alpha) = a^2 - ab + b^2$. Вище вже відзначалось, що має місце рівність $N(\alpha\beta) = N(\alpha)N(\beta)$, з якої випливає аксіома (Е 1).

Нехай $\alpha = a + b\varpi$, $\beta = c + d\varpi \neq 0$, де $a, b, c, d \in Z$. Тоді з включень $\beta\Delta(\beta) = N(\beta) \in N$ та $\alpha\Delta(\beta) \in Z[\varpi]$ випливає, що $(\alpha\Delta(\beta))/(\beta\Delta(\beta)) = \alpha/\beta = x + y\varpi$, де вже $a, b \in Q$. Знайдуться такі числа $u, v \in Z$, що $|x - u| \leq 1/2$ та $|y - v| \leq 1/2$. Покладемо тепер $\delta = u + v\varpi$, $\rho = \alpha - \beta\delta$. За самим визначенням $\delta, \rho \in Z[\varpi]$. Маємо або $\rho = 0$, або

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\delta) = N(\beta((\alpha/\beta) - \delta)) = N(\beta)N((\alpha/\beta) - \delta) = \\ &= N(\beta) N((x - u) + (y - v)\varpi) = N(\beta)((x - u)^2 - (x - u)(y - v) + \\ &\quad + (y - v)^2) \leq N(\beta) (1/4 + 1/4 + 1/4) = 3/4 N(\beta) < N(\beta). \end{aligned}$$

Таким чином, і аксіома (Е 2) також має місце.

Кільце $Z[\varpi]$ було вперше розглянуто Г. Ейзенштейном, який відзначив, що багато властивостей кільця $Z[i]$ зберігаються також в кільці $Z[\varpi]$.

У зв'язку з цими двома прикладами природно виникає питання: які з інших кілець $Z[\sqrt{r}]$ будуть евклідовими? Відповідь на це питання була одержана у книзі [13], де показано, що це має місце тоді і тільки тоді, коли r має одне з наступних значень: $-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97$.

Наступна властивість евклідових кілець є однією з основних.

21.3. Теорема. *Кожне евклідове кільце буде областю головних ідеалів.*

Доведення. Нехай R — евклідове кільце, H — його ідеал. Якщо H — нульовий, то він породжується нульовим елементом і, зокрема, буде головним. Тому розглянемо випадок, коли H — ненульовий ідеал. Нехай

$$\Delta(H) = \{\delta(x) \mid 0_R \neq x \in H\}.$$

Оскільки $\Delta(H)$ — підмножина N_0 , то $\Delta(H)$ має найменший елемент m . Нехай y — елемент H , для якого $\delta(y) = m$. Якщо тепер x — довільний елемент ідеалу H , то з аксіоми (Е 2) випливає існування таких елементів w, z , що $x = wy + z$, де або $z = 0_R$, або $\delta(z) < \delta(y)$. Оскільки H — ідеал, то $wy \in H$, отже $z = x - wy \in H$. Якщо припустити, що $z \neq 0_R$, то маємо $\delta(z) < \delta(y)$, а це суперечить вибору елемента y . Отримане протиріччя доводить рівність $z = 0_R$, з якої випливає, що $x = wy$. Інакше кажучи, $H \leq yR$. Оскільки включення $yR \leq H$ також має місце, то $yR = H$.

З теореми 20.13 випливає

21.4. Наслідок. Нехай R — евклідове кільце, $0_R \neq a \in R$.

(1) Якщо $a \notin U(R)$, то a розкладається у добуток простих елементів кільця R .

(2) Якщо $a \notin U(R)$ і $a = p_1 \dots p_n = q_1 \dots q_m$ — два розклади у добуток простих елементів кільця R , то $n = m$ і елементи другого розкладу можна перенумерувати таким чином, що $q_j = u_j p_j$, для деяких $u_j \in U(R)$, $1 \leq j \leq n$.

21.5. Наслідок. Нехай R — евклідове кільце. Для кожної пари його елементів a, b у кільці R існує їх найбільший спільний дільник та їх найменше спільне кратне.

Це твердження випливає з теореми 20.5 та 21.3.

Для областей головних ідеалів було доведено існування найбільшого спільного дільника та найменшого спільного кратного для будь-якої пари елементів. Але не завжди видно як їх реально знаходити. Для евклідових кілець найбільший спільний дільник можна знайти, користуючись наступним алгоритмом, який називають алгоритмом Евкліда. Наведемо зараз цей алгоритм.

Нехай R — евклідове кільце, a, b — довільні елементи кільця R . Якщо $a = 0_R$, то $\text{GCD}(a, b) = b$. Тому будемо вважати, що обидва елемента a, b — ненульові. Ділимо a на b : $a = bq_1 + r_1$, де або $r_1 = 0_R$, або $\delta(r_1) < \delta(b)$. Наступний крок: ділимо b на r_1 : $b = bq_2 + r_2$, де або $r_2 = 0_R$, або $\delta(r_2) < \delta(r_1)$. Якщо $r_2 \neq 0_R$, то ділимо r_1 на r_2 : $r_1 = r_2q_3 + r_3$, де або $r_3 = 0_R$, або $\delta(r_3) < \delta(r_2)$. Якщо $r_3 \neq 0_R$, то продовжимо цей процес далі, і т.д.

У загальному випадку, якщо $r_j \neq 0_R$, то продовжуємо ділити r_{j-1} на r_j . Оскільки на кожному кроці $\delta(r_{j-1}) < \delta(r_j)$, то враховуючи той факт, що значеннями цих функцій будуть натуральні числа, можемо бачити, що цей процес не може бути нескінченним. Це означає, що на деякому етапі відповідна остача r_k мусить бути нульовою. Таким чином, отримуємо наступний ланцюжок рівностей:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\dots\dots\dots \\ r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, \\ r_{k-2} &= r_{k-1}q_k + r_k, \\ r_{k-1} &= r_kq_{k+1}. \end{aligned} \tag{E}$$

Маємо тепер

$$r_{k-2} = r_{k-1}q_k + r_k = r_kq_{k+1}q_k + r_k = r_k(q_{k+1}q_k + e),$$

так що r_k ділить r_{k-2} .

Далі

$$\begin{aligned} r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} = r_k(q_{k+1}q_k + e)q_{k-1} + r_kq_{k+1} = \\ &= r_k(q_{k+1}q_kq_{k-1} + q_{k-1} + q_{k+1}), \end{aligned}$$

так що r_k ділить r_{k-3} . Продовжуючи далі підніматися по ланцюжку рівностей (E), отримаємо в кінці, що r_k ділить a та b , тобто r_k — спільний дільник a і b .

Нехай тепер u — довільний спільний дільник a і b . З рівності $r_1 = a - bq_1$ отримуємо, що u ділить r_1 . Далі з рівності $r_2 = b - r_1q_2$ отримуємо, що u ділить r_2 . Продовжуючи далі спускатися по ланцюжку рівностей (E), отримаємо в кінці, що u ділить r_k . Це і означає, що r_k буде найбільшим спільним дільником елементів a і b . Знайшовши $\text{GCD}(a, b)$ за допомогою теореми 20.10 можемо знайти і $\text{LCM}(a, b)$.

З теореми 20.5 випливає, що для елемента $d = \text{GCD}(a, b)$ у евклідовому кільці R існують такі елементи x, y , що $d = ax + by$. Алгоритм Евкліда також дає можливість знаходити ці елементи x, y . Дійсно, з ланцюжка рівнянь (E) маємо:

$$d = r_k = r_{k-2} - r_{k-1}q_k.$$

У свою чергу $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$, так що

$$\begin{aligned} d &= r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k = r_{k-2} - r_{k-3}q_k + r_{k-2}q_{k-1}q_k = \\ &= r_{k-2}(e + q_{k-1}q_k) - r_{k-3}q_k = r_{k-2}y_1 - r_{k-3}x_1. \end{aligned}$$

Використовуючи далі рівність $r_{k-2} = r_{k-4} - r_{k-3}q_{k-2}$, приходимо до рівності $d = r_{k-3}y_2 - r_{k-4}x_2$. Продовжуючи далі підніматися по ланцюжку рівностей (E), отримаємо зрештою рівність $d = ax + by$.

22. НЕЗВІДНІ ПОЛІНОМИ

У попередньому розділі ми вже відзначали, що за теоремою 17.1 кільце поліномів $F[X]$, де F — поле, є евклідовим. З наслідку 21.5 отримуємо

22.1. Пропозиція. *Нехай F — поле. Для кожної пари поліномів $f(X), g(X) \in F[X]$ існує їх найбільший спільний дільник та їх найменше спільне кратне, що також належать до кільця $F[X]$.*

Визначення простого елемента для кільця поліномів над полем може бути переписано у наступному вигляді:

Нехай R — комутативне кільце без дільників нуля (зокрема, R — поле). Поліном $f(X)$ степеня ≥ 1 з коефіцієнтами із R

називається незвідним або нерозкладним над R , якщо його не можна представити у вигляді $f(X) = u(X)v(X)$, де $u(X), v(X) \in R[X]$ та $0 < \deg u(X) < \deg f(X)$, $0 < \deg v(X) < \deg f(X)$.

З самого означення випливає, що кожен поліном першого степеня є незвідним. Слід звернути увагу також на ту обставину, що говорячи про незвідність або звідність полінома, завжди треба уточнювати, над яким полем він розглядається. Так, наприклад, поліном $X^2 - 2$ є незвідним над полем Q , але над R він вже розкладається у добуток двох лінійних множників; поліном $X^4 + 4$ є звідним над Q : $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$, а обидва множники з його розкладу будуть незвідними не тільки над Q , а і над R . Більш знайомий приклад: поліном $X^2 + 1$ є незвідним над R , але $X^2 + 1 = (X + i)(X - i)$ над полем комплексних чисел.

У розділі 17 була доведена рівність $U(F[X]) = U(F)$. З наслідку 20.21 отримуємо, що кільце поліномів $F[X]$ над полем F є областю з однозначним розкладом. У розділі 20 ми вже відзначали, як зробити розклад однозначним. У випадку кільця поліномів над полем множини $\sigma(F[X])$, як правило, складають незвідні поліноми, старші коефіцієнти яких є одиничними елементами поля F .

Такі поліноми будемо називати *унітарними*.

З теореми 20.13 отримуємо тепер пропозицію:

22.2. Пропозиція. Нехай F — поле, $f(X)$ — поліном степеня ≥ 1 . Тоді $f(X) = a(p_1(X))^{k_1} \dots (p_m(X))^{k_m}$, де a — старший коефіцієнт полінома $f(X)$, $p_1(X), \dots, p_m(X)$ — попарно різні незвідні поліноми, старші коефіцієнти яких дорівнюють одиничному елементу поля F . Таке представлення є єдиним.

Наступна властивість також є важливою.

22.3. Теорема. Нехай F — поле. Множина незвідних поліномів кільця $F[X]$ є нескінченною.

Д о в е д е н н я . Якщо поле F — нескінченне, то теорема тривіальна, оскільки кожен поліном першого степеня є незвідним. Розглянемо тепер випадок, коли поле F є скінченним. Припустимо, що вже знайдені m попарно різних незвідних поліномів $p_1(X), \dots, p_m(X)$. Можна вважати, що всі вони унітарні. Нехай $q(X) = p_1(X), \dots, p_m(X) + e$. За пропозицією 22.2 $q(X)$ має незвідний унітарний дільник $u(X)$. Припустимо, що $u(X)$ співпадає з деяким з уже знайдених поліномів, тобто $u(X) = p_i(X)$. З рівності $e = q(X) - p_1(X), \dots, p_m(X)$ і наслідку 20.7 випливає, що $q(X)$ є взаємно простим з кожним із поліномів $p_1(X), \dots, p_m(X)$. Але тоді й $u(X)$ є взаємно простим з кожним із поліномів $p_1(X), \dots, p_m(X)$. Таким чином, маючи довільну скінченну множину незвідних поліномів, ми завжди можемо знайти незвідний поліном, взаємно простий з кожним з уже вибраних. Це і означає, що множина незвідних поліномів кільця $F[X]$ є нескінченною.

22.4. Наслідок. Нехай F — поле. Степені незвідних поліномів кільця $F[X]$ не обмежені.

Зокрема не є обмеженими степені незвідних поліномів кільця $F[X]$, де F — просте поле ненульової характеристики. Зараз ми побажимо, що та ж сама ситуація має місце і для кільця поліномів над простим полем нульової характеристики, тобто над полем Q раціональних чисел. Отже, розглянемо питання про незвідність поліномів з раціональними коефіцієнтами.

Передусім слід відзначити, що якщо поліном $f(X) \in Q[X]$ має не всі цілі коефіцієнти, то помноживши $f(X)$ на найменше спільне кратне s знаменників усіх коефіцієнтів $f(X)$, отримаємо поліном $sf(X)$, усі коефіцієнти якого будуть уже цілими числами. Очевидно, що поліноми $f(X)$ та $sf(X)$ мають однакові корені. Також якщо один з них є незвідний над Q , то таким буде і інший. З іншого боку, якщо $f(X)$ — поліном з цілими коефіцієнтами, незвідний над кільцем цілих чисел, то чи буде він незвідним і над полем раціональних чисел.

22.5. Теорема. *Поліном $f(X) \in Z[X]$ є незвідним над кільцем цілих чисел тоді і тільки тоді, коли він є незвідним над полем раціональних чисел.*

Д о в е д е н н я . Очевидно, якщо $f(X)$ є незвідним над Q , то він буде незвідним і над Z . Навпаки, нехай $f(X)$ є незвідним над Z , і припустимо, що він є звідним над Q : $f(X) = f_1(X)f_2(X)$, де $f_1(X), f_2(X) \in Q[X]$ та $0 < \deg f_1(X) < \deg f(X), 0 < \deg f_2(X) < \deg f(X)$. Помножуючи обидві частини на найменше спільне кратне знаменників усіх коефіцієнтів $f_1(X)$ та $f_2(X)$, будемо мати $af(X) = f_3(X)f_4(X)$, де $f_3(X), f_4(X) \in Z[X]$ та $\deg f_1(X) = \deg f_3(X), \deg f_2(X) = \deg f_4(X)$. У свою чергу, звідси отримуємо рівність $af(X) = bf_5(X)f_6(X)$, де $f_5(X), f_6(X) \in Z[X], \deg f_5(X) = \deg f_3(X), \deg f_6(X) = \deg f_4(X)$ та $f_5(X), f_6(X)$ — примітивні поліноми.

З леми 20.17 отримуємо тепер, що $f_5(X)$ ділить $f(X)$. Водночас, $\deg f_1(X) = \deg f_5(X)$, так що $0 < \deg f_5(X) < \deg f(X)$. Отримане протиріччя показує, що $f(X)$ є незвідним над Q .

Таким чином, ми отримали право у питаннях відносно звідності поліномів над полем раціональних чисел обмежитись розглядом розкладів поліномів з цілими коефіцієнтами на множники, коефіцієнти яких також будуть цілими числами.

Питання про те, чи буде даний поліном $f(X) \in Z[X]$ незвідним над Q , є досить непростим. Існує метод Кронекера, який дає можливість сказати, чи буде $f(X)$ незвідним над Q . Але цей метод є дуже громіздким, і застосовувати практично його можливо дуже рідко. Однак існує багато результатів, що дають достатні умови незвідності над Q . Одним з найбільш відомих таких результатів є наступний критерій Ейзенштейна.

22.6. Теорема. *Нехай $f(X) = a_0 + a_1X + \dots + a_nX^n \in Z[X]$ і припустимо, що існує таке просте число p , яке задовольняє наступні умови:*

- (i) старший коефіцієнт a_n не ділиться на p ;
- (ii) усі інші коефіцієнти полінома $f(X)$ діляться на p ;
- (iii) a_0 не ділиться на p^2 ;

Тоді поліном $f(X)$ є незвідним над полем раціональних чисел.

Доведення. Припустимо протилежне, нехай $f(X)$ є звідним над Q . За теоремою 22.5 він буде звідним і над Z : $f(X) = f_1(X)f_2(X)$, де $f_1(X), f_2(X) \in Z[X]$ та $0 < \deg f_1(X) < \deg f(X)$, $0 < \deg f_2(X) < \deg f(X)$. Нехай

$$\begin{aligned}f_1(X) &= b_0 + b_1X + \dots + b_kX^k, \\f_2(X) &= c_0 + c_1X + \dots + c_tX^t.\end{aligned}$$

Маємо $a_0 = b_0c_0$. З умов (ii), (iii) випливає, що або b_0 ділиться на просте число p , а c_0 не ділиться на p , або навпаки, b_0 не ділиться на p , а c_0 ділиться на p .

Розглянемо перший випадок. За правилом множення поліномів $a_1 = b_0c_1 + b_1c_0$. Звідси $b_1c_0 = a_1 - b_0c_1$. Оскільки обидва числа a_1 та b_0 діляться на p , то b_1c_0 ділиться на p . З пропозиції 20.9 випливає, що b_1 ділиться на p . Аналогічно, з рівності $a_2 = b_0c_2 + b_1c_1 + b_2c_0$ отримуємо $b_2c_0 = a_2 - b_0c_2 - b_1c_1$, а з останньої рівності випливає, що b_2 ділиться на p .

За допомогою аналогічних міркувань і того факту, що $k < n$, отримаємо, що b_k ділиться на p . У свою чергу, з рівності $a_n = b_nc_t$ випливає, що a_n ділиться на p , що суперечить умовам. Аналогічно, припустивши, що b_0 не ділиться на p , а c_0 ділиться на p , ми також отримаємо протиріччя.

22.7. Наслідок. *Степені незвідних поліномів кільця $Q[X]$ не обмежені.*

На відміну від поля Q , поле C комплексних чисел є алгебрично замкненим за класичною теоремою К. Гауса (цей результат донедавна називався основною теоремою алгебри), тобто кожен незвідний поліном над C має степінь 1. Також треба сказати, що кожен незвідний поліном над полем R дійсних чисел має степінь 1 або 2.

22.8. Наслідок. *Поліном $f_p(X) = 1 + X + \dots + X^{p-1} \in Z[X]$, де p — просте число, є незвідним над полем раціональних чисел.*

Доведення. Коренями цього полінома будуть корені степеня p з одиниці, окрім самої одиниці. Усі вони разом з одиницею ділять коло одиничного радіуса на p рівних частин. Тому поліном $f_p(X)$ називають *поліномом ділення кола*.

Розглянемо поліном $g(X) = f_p(X + 1)$. Якщо припустити, що $f_p(X) = g_1(X)g_2(X)$, де $g_1(X), g_2(X) \in Z[X]$ та $0 < \deg g_1(X) < \deg f_p(X)$, $0 < \deg g_2(X) < \deg f_p(X)$, то

$$g(X) = f_p(X + 1) = g_1(X + 1)g_2(X + 1) = g_3(X)g_4(X),$$

де $g_3(X), g_4(X) \in Z[X]$ та $0 < \deg g_3(X) < \deg g(X)$, $0 < \deg g_4(X) < \deg g(X)$.

Таким чином, питання про незвідність $f_p(X)$ рівносильне питанню про незвідність полінома $g(X)$. Маємо далі

$$\begin{aligned}g(X) &= f_p(X + 1) = ((X + 1)^p - 1)/(X + 1 - 1) = \\&= X^{p-1} + C_1^p X^{p-2} + \dots + C_{p-2}^p X + C_{p-1}^p,\end{aligned}$$

де $C_k^p = (p!)/((k!)(p-k)!)$ — біноміальні коефіцієнти.

З рівності $(p!) = (k!)(p-k)!C_k^p$ та того факту, що p ділить $(p!)$, але p не ділить $(k!)(p-k)!$ (оскільки останнє число є добутком чисел менших p , а тому взаємно простих з p), отримуємо, що C_k^p ділиться на p . Останній коефіцієнт $C_{p-1}^p = p$, так що $g(X)$ задовольняє всі умови теореми 22.6. Застосування цієї теореми доводить незвідність $g(X)$.

За пропозицією 22.2 кожен поліном розкладається у добуток степенів незвідних поліномів. Як вже відзначалось трохи вище, не існує задовільних критеріїв незвідності поліномів з раціональними коефіцієнтами. Тому питання про те, як реально отримати розклад полінома у добуток степенів незвідних поліномів, є дуже не простим. Зараз наведемо результат, який дає можливість знижувати степінь, виділяючи кратні незвідні множники. Він базується на понятті похідної поліному.

Нехай R — комутативне кільце, $f(X) = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Похідною полінома $f(X)$ будемо називати поліном

$$f'(X) = a_1 + 2a_2X + \dots + na_nX^{n-1}.$$

22.9. Лема. Нехай R — комутативне кільце. Для довільних поліномів $f(X), g(X) \in R[X]$ мають місце рівності

$$(f(X) + g(X))' = f'(X) + g'(X),$$

$$(f(X)g(X))' = f'(X)g(X) + f(X)g'(X).$$

Д о в е д е н н я . Нехай

$$f(X) = a_0 + a_1X + \dots + a_nX^n,$$

$$g(X) = b_0 + b_1X + \dots + b_kX^k.$$

Під час доведення першої рівності можна вважати, що $n = k$ (цього завжди можна досягти, додаючи відповідні члени з нульовими коефіцієнтами). Маємо

$$\begin{aligned} (f(X) + g(X))' &= (a_0 + b_0 + (a_1 + b_1)X + \dots + (a_n + b_n)X^n)' = \\ &= (a_1 + b_1) + 2(a_2 + b_2)X + \dots + n(a_n + b_n)X^{n-1} = \\ &= a_1 + 2a_2X + \dots + na_nX^{n-1} + b_1 + 2b_2X + \dots + nb_nX^{n-1} = f'(X) + g'(X). \end{aligned}$$

При доведенні другої рівності уже не обов'язково вважати числа k і n рівними. Для доведення цієї рівності застосуємо індукцію за степенем полінома $g(X)$, тобто за числом k . Якщо $g(X) = 0_R$, то рівність є тривіальною. Нехай $k = 0$, тоді

$$f(X)g(X) = b_0a_0 + b_0a_1X + \dots + b_0a_nX^n;$$

$$\begin{aligned} (f(X)g(X))' &= b_0a_1 + 2b_0a_2X + \dots + nb_0a_nX^{n-1} = \\ &= f'(X)b_0 = f'(X)g(X) + f(X)g'(X). \end{aligned}$$

Нехай тепер $k > 0$ і припустимо, що лема є вірною для

поліномів, степенів яких є меншою за k . Нехай $h(X) = b_0 + b_1X + \dots + b_{k-1}X^{k-1}$, тоді $g(X) = h(X) + b_kX^k$, і отже

$$f(X)g(X) = f(X)(h(X) + b_kX^k) = f(X)h(X) + f(X)b_kX^k.$$

Звідси і доведеної вище першої рівності отримуємо

$$\begin{aligned}(f(X)g(X))' &= (f(X)h(X) + f(X)b_kX^k)' = \\ &= (f(X)h(X))' + (f(X)b_kX^k)'. \end{aligned}$$

За індуктивним припущенням $(f(X)h(X))' = f'(X)h(X) + f(X)h'(X)$. Далі маємо

$$f(X)b_kX^k = b_ka_0X^k + b_ka_1X^{k+1} + \dots + b_ka_nX^{k+n};$$

$$(f(X)b_kX^k)' = (b_ka_0X^k)' + (b_ka_1X^{k+1})' + \dots + (b_ka_nX^{k+n})'.$$

Розглядаємо тепер похідну довільного члена останньої суми:

$$\begin{aligned}(b_ka_jX^{k+j})' &= (k+j)b_ka_jX^{k+j-1} = kb_ka_jX^{k+j-1} + j b_ka_jX^{k+j-1} = \\ &= (kb_kX^{k-1})a_jX^j + b_kX^k(ja_jX^{j-1}). \end{aligned}$$

Отже,

$$\begin{aligned}(f(X)b_kX^k)' &= (kb_kX^{k-1})a_0 + b_kX^k O_R + (kb_kX^{k-1})a_1X + b_kX^ka_1 + \\ &+ \dots + (kb_kX^{k-1})a_nX^n + b_kX^k(na_nX^{n-1}) = (a_1 + 2a_2X + \dots + \\ &+ na_nX^{n-1})b_kX^k + (a_0 + a_1X + \dots + a_nX^n)(kb_kX^{k-1}) = \\ &= f'(X)b_kX^k + (f(X)(b_kX^k))'. \end{aligned}$$

Нарешті,

$$\begin{aligned}(f(X)g(X))' &= (f(X)h(X))' + (f(X)b_kX^k)' = \\ &= f'(X)h(X) + f(X)h'(X) + f'(X)b_kX^k + (f(X)(b_kX^k))' = \\ &= f'(X)(h(X) + b_kX^k) + f(X)(h'(X) + (b_kX^k)') = \\ &= f'(X)(h(X) + b_kX^k) + f(X)(h(X) + b_kX^k)' = \\ &= f'(X)g(X) + f(X)g'(X). \end{aligned}$$

22.10. Наслідок. Нехай R — комутативне кільце. Для довільних поліномів $f_1(X), \dots, f_n(X) \in R[X]$ мають місце рівності

$$(f_1(X) \dots f_n(X))' = \sum_{1 \leq j \leq n} f_1(X) \dots f_{j-1}(X) f_j'(X) f_{j+1}(X) \dots f_n(X).$$

Зокрема, $(f(X)^n)' = n(f(X)^{n-1})f'(X)$.

Нехай R — комутативне кільце без дільників нуля, $f(X) \in R[X]$. Будемо говорити, що незвідний поліном $p(X)$ входить до розкладу $f(X)$ з кратністю m , якщо $f(X)$ ділиться на $(p(X))^m$, але $f(X)$ не ділиться на $(p(X))^{m+1}$. Якщо $p(X) = (X - a)$ входить до розкладу

$f(X)$ з кратністю $t > 1$, то будемо говорити, що корінь a є кратним коренем полінома $f(X)$ та має кратність t .

22.11. Пропозиція. Нехай F — поле характеристики 0, $f(X) \in F[X]$. Якщо незвідний поліном $p(X)$ входить до розкладу $f(X)$ з кратністю t , то $p(X)$ входить до розкладу $f'(X)$ з кратністю $t - 1$.

Доведення. Маємо $f(X) = (p(X))^m u(X)$, де $u(X)$ вже не ділиться на $p(X)$. З леми 20.12 випливає, що $u(X)$ та $p(X)$ будуть взаємно простими. За наслідком 22.9

$$f'(X) = (p(X))^{m-1}(mp'(X)u(X) + p(X)u'(X)).$$

Якщо припустити, що поліном $(mp'(X)u(X) + p(X)u'(X))$ ділиться на $p(X)$, то $p(X)$ мусить ділити $mp'(X)u(X)$. Оскільки $\text{char } F = 0$, то $\deg p'(X) = \deg p(X) - 1$, зокрема $p'(X)$ — ненульовий поліном. З рівності $\deg p'(X) = \deg p(X) - 1$ також випливає, що $p'(X)$ не ділиться на $p(X)$, і тоді за лемою 20.12 поліноми $p'(X)$ та $p(X)$ будуть взаємно простими. Але тоді за пропозицією 20.10 $p(X)$ є взаємно простим з $mp'(X)u(X)$. Отримуємо протиріччя, показує, що $p(X)$ входить до розкладу $f'(X)$ з кратністю $t - 1$.

На застосуванні цієї пропозиції заснований наступний метод. Нехай F — поле нульової характеристики, $f(X) \in F[X]$. За пропозицією 22.2

$$f(X) = a(p_1(X))^{k_1} \dots (p_m(X))^{k_m},$$

де a — старший коефіцієнт полінома $f(X)$, $p_1(X), \dots, p_m(X)$ — попарно різні незвідні поліноми, старші коефіцієнти яких дорівнюють одиничному елементу. З пропозицій 22.11, 20.14 отримуємо, що

$$g(X) = \text{GCD}(f(X), f'(X)) = p_1(X)^{k_1-1} \dots (p_m(X))^{k_m-1}.$$

З результатів попереднього розділу ми знаємо, як знайти поліном $g(X)$. Далі $f(X) = g(X)w(X)$, де очевидно $w(X) = ap_1(X) \dots p_m(X)$. Таким чином, ділячи поліном $f(X)$ на $g(X)$, ми отримаємо поліном $w(X)$, розклад якого має всі ті незвідні множники, що їх має і поліном $f(X)$, але вже з кратністю 1. При цьому степінь може значно знизитися. Залишилось тільки знайти розклад $w(X)$.

Слід сказати, що для полів простої характеристики доведена вище пропозиція не має місце. Наприклад, нехай поле F має просту характеристику $p > 0$, а $f(X) = X^p$. Тоді $f'(X) = pX^{p-1} = (pe)X^{p-1} = 0_F$. Інакше кажучи, поліном степеня > 1 може мати нульову похідну. Але у загальному випадку все ж таки має місце

22.12. Теорема. Нехай F — поле, $f(X) \in F[X]$. Елемент $c \in F$ тоді і тільки тоді буде кратним коренем полінома $f(X)$, коли $f(c) = 0_F$ та $f'(c) = 0_F$.

Доведення. Нехай b — довільний елемент поля F . З теореми 17.1 випливає, що $f(X) = (X - b)^2 q(X) + r(X)$, де або $r(X) = 0_F$ або $\deg r(X) < 2$. Зокрема поліном $r(X)$ можна записати

у вигляді $r(X) = d(X - b) + w$ для деяких елементів $d, w \in F$.
Отже,

$$f(X) = (X - b)^2 q(X) + d(X - b) + w.$$

Застосовуючи лему 22.9 та наслідок 22.10, отримаємо

$$f'(X) = (X - b)(2q(X) + (X - b)q'(X)) + d,$$

звідки $w = f(b)$ та $d = f'(b)$.

Отже, остаточно

$$f(X) = (X - b)^2 q(X) + f'(b)(X - b) + f(b);$$

$$f'(X) = (X - b)(2q(X) + (X - b)q'(X)) + f'(b).$$

Якщо c — кратний корінь полінома $f(X)$, то $f(X)$ ділиться на $(X - c)^2$. А це означає, що $f'(c) = f(c) = O_F$. Навпаки, якщо $f'(c) = f(c) = O_F$, то доведені вище рівності показують, що $f(X)$ ділиться на $(X - c)^2$.

Закінчуючи цей розділ, повернемося знову до поліномів з раціональними коефіцієнтами і з'ясуємо питання про знаходження їх раціональних коренів. Вище вже відзначалось, що помноживши поліном $f(X) \in Q[X]$ на найменше спільне кратне s знаменників усіх його коефіцієнтів, отримаємо поліном $sf(X)$, усі коефіцієнти якого будуть уже цілими числами. Очевидно, що поліноми $f(X)$ та $sf(X)$ мають однакові корені. Тому зразу це питання зводиться до питання знаходження раціональних коренів полінома з цілими коефіцієнтами.

Нехай $f(X) = a_0 + a_1X + \dots + a_nX^n \in Z[X]$, c — цілий корінь полінома $f(X)$. З огляду на пропозицію 17.5 маємо

$$f(X) = (X - c)q(X),$$

де $q(X) = (b_0 + b_1X + \dots + b_{n-1}X^{n-1})$.

Звідси

$$a_n = b_{n-1}, a_{n-1} = b_{n-2} - cb_{n-1}, \dots, a_1 = b_0 - cb_1, a_0 = (-c)b_0 = (-b_0).$$

З цих рівностей ми можемо побачити, що всі коефіцієнти $b_0, b_1, \dots, b_{n-1}$ будуть цілими числами, зокрема, c буде цілим дільником числа a_0 . Таким чином, якщо поліном $f(X)$ має цілі корені, то для їх знаходження необхідно знайти всі дільники числа a_0 (як додатні, так і від'ємні) і перевірити, які з них будуть коренями. Інших цілих коренів поліном $f(X)$ не має. Ця процедура може бути досить довгою, оскільки таких дільників може бути дуже багато. Наступні нотатки можуть дещо скоротити цей процес.

Числа 1 та -1 є дільниками числа a_0 , тому ми мусимо завжди знаходити $f(1)$ та $f(-1)$. Маємо $f(1) = (1 - c)q(1)$, $f(-1) = (-1 - c)q(-1)$. Оскільки всі коефіцієнти $q(X)$ є цілими числами, то числа $q(1)$ та $q(-1)$ також будуть цілими. Таким чином, досить перевіряти не всі дільники числа a_0 , а тільки такі дільники d , для яких $f(1)/(1 - d)$ та $f(-1)/(1 + d)$ є цілими числами.

Наступний етап описує теорема:

22.13. Теорема. Нехай $f(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n \in \mathbb{Z}[X]$. Якщо c — раціональний корінь полінома $f(X)$, то c — ціле число.

Д о в е д е н н я . Припустимо протилежне, нехай c не є цілим числом, тобто $c = m/k$ і можна вважати, що числа m, k — взаємно прості. Маємо тепер

$$0 = a_0 + a_1(m/k) + \dots + a_{n-1}(m/k)^{n-1} + (m/k)^n,$$

звідси

$$(m^n)/k = -a_0k^{n-1} - a_1mk^{n-2} - \dots - a_{n-1}m^{n-1} + (m/k)^n.$$

Оскільки m, k — взаємно прості, то і m^n та k будуть взаємно простими. Але це означає, що у лівій частині останньої рівності стоїть раціональне число, яке не є цілим, в той час, як у правій частині стоїть ціле число. Отримане протиріччя і доводить теорему.

Нехай тепер $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$. Розглянемо поліном $g(X) = a_n^{-1}f(X)$, тобто

$$g(X) = a_n^{-1}a_0 + a_n^{-1}a_1X + \dots + a_n^{-1}X^n.$$

Нехай $Y = a_nX$, тоді

$$g(Y) = a_n^{-1}a_0 + a_n^{-2}a_1Y + \dots + a_{n-1}Y^{n-1} + Y^n.$$

За теоремою 22.13 раціональні корені полінома $g(Y)$ можуть бути тільки цілими числами. Як знайти всі цілі корені полінома $g(Y)$ ми вже бачили раніше. Нарешті, якщо c — цілий корінь полінома $g(Y)$, то c/a_n — корінь полінома $f(X)$.

23. АРИФМЕТИЧНІ ФУНКЦІЇ

У цьому розділі ми розглянемо ряд важливих теоретико-числових функцій. *Теоретико-числовою або арифметичною функцією ми будемо називати кожну функцію $f: \mathbb{N} \rightarrow \mathbb{C}$.*

Наведемо деякі важливі приклади арифметичних функцій.

Через ν позначимо функцію, що ставить у відповідність натуральному числу n кількість його додатних дільників, а через σ позначимо функцію, що ставить у відповідність натуральному числу n суму його додатних дільників. Наступна пропозиція дає формули для цих двох функцій.

23.1. Пропозиція. Нехай n — натуральне число, $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ — його розклад на прості множники, де $p_i \neq p_j$, якщо $i \neq j$. Тоді $v(n) = (k_1 + 1) \dots (k_t + 1)$,
 $\sigma(n) = ((p_1^{k_1+1} - 1)/(p_1 - 1)) \dots ((p_t^{k_t+1} - 1)/(p_t - 1))$.

Доведення. Нехай m — дільник числа n , тоді $m = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$, де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$. Слід відзначити, що розклад як числа n , так і його дільника m є однозначним. Звідси випливає, що відображення, що ставить у відповідність дільнику m числа n набір чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$, буде бієктивним. Таким чином, кількість дільників числа n дорівнює кількості наборів чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$.

Підраховуємо кількість таких наборів, використовуючи індукцію за числом t . Якщо $t = 1$, то очевидно, $v(n) = (k_1 + 1)$. Нехай тепер $t > 1$ і нехай вже доведено, що кількість наборів чисел $(s_1, \dots, s_{t-1})$ довжини $t - 1$, де $0 \leq s_j \leq k_j$, $1 \leq j \leq t - 1$, дорівнює числу $(k_1 + 1) \dots (k_{t-1} + 1)$. Це означає, що кількість наборів чисел $(s_1, \dots, s_t)$ довжини t , що мають на останньому місці фіксоване число s_t , де $0 \leq s_j \leq k_j$, $1 \leq j \leq t - 1$, дорівнює $(k_1 + 1) \dots (k_{t-1} + 1)$. Оскільки $0 \leq s_t \leq k_t$, тобто для числа s_t маємо $(k_t + 1)$ можливих варіантів, то загальна кількість наборів чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$, дорівнює $(k_1 + 1) \dots (k_{t-1} + 1)(k_t + 1)$. Отже, $v(n) = (k_1 + 1) \dots (k_t + 1)$.

Для знаходження формули для функції $\sigma(n)$ також застосуємо індукцію за числом t . Якщо $t = 1$, тобто $n = p_1^{k_1}$, то очевидно,

$$\sigma(n) = 1 + p_1 + p_1^2 + \dots + p_1^{k_1} = (p_1^{k_1+1} - 1)/(p_1 - 1).$$

Нехай $t > 1$, $r = p_1^{k_1} p_2^{k_2} \dots p_{t-1}^{k_{t-1}}$ і нехай вже доведено, що

$$\sigma(r) = ((p_1^{k_1+1} - 1)/(p_1 - 1)) \dots ((p_{t-1}^{k_{t-1}+1} - 1)/(p_{t-1} - 1)).$$

Позначимо через S множину всіх наборів чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$, через M множину всіх наборів чисел $(s_1, \dots, s_{t-1})$ довжини $t - 1$, де $0 \leq s_j \leq k_j$, $1 \leq j \leq t - 1$. Тоді маємо

$$\begin{aligned} \sigma(n) &= \sum_{(s_1, \dots, s_t) \in S} p_1^{s_1} p_2^{s_2} \dots p_{t-1}^{s_{t-1}} p_t^{s_t} = \\ &= \sum_{(s_1, \dots, s_{t-1}) \in M} p_1^{s_1} p_2^{s_2} \dots p_{t-1}^{s_{t-1}} + \sum_{(s_1, \dots, s_{t-1}) \in M} p_1^{s_1} p_2^{s_2} \dots p_{t-1}^{s_{t-1}} p_t + \\ &+ \sum_{(s_1, \dots, s_{t-1}) \in M} p_1^{s_1} p_2^{s_2} \dots p_{t-1}^{s_{t-1}} p_t^2 + \dots + \sum_{(s_1, \dots, s_{t-1}) \in M} p_1^{s_1} p_2^{s_2} \dots p_{t-1}^{s_{t-1}} p_t^{k_t} = \\ &= \left(\sum_{(s_1, \dots, s_{t-1}) \in M} p_1^{s_1} p_2^{s_2} \dots p_{t-1}^{s_{t-1}} \right) (1 + p_t + p_t^2 + \dots + p_t^{k_t}) = \\ &= ((p_1^{k_1+1} - 1)/(p_1 - 1)) \dots ((p_{t-1}^{k_{t-1}+1} - 1)/(p_{t-1} - 1)) ((p_t^{k_t+1} - 1)/(p_t - 1)). \end{aligned}$$

З функцією $\sigma(n)$ пов'язана цікава проблема теорії чисел. *Натуральне число n називається досконалим, якщо $\sigma(n) = 2n$.* Наприклад, досконалими будуть числа 6 та 28. З пропозиції 23.1 випливає, що якщо $2^{k+1} - 1$ — просте число, то $n = 2^k(2^{k+1} - 1)$ — досконале число. Ейлер довів, що будь-яке парне досконале число має такий вигляд. Таким чином, проблема знаходження парних досконалих чисел зводиться до знаходження простих чисел, що мають вигляд $2^{k+1} - 1$. Такі прості числа називають простими числами Мерсенна. З досконалими числами також пов'язані дві важливі проблеми: чи є множина досконалих чисел нескінченною та чи існують непарні досконалі числа?

На множині арифметичних функцій розглянемо специфічну операцію — добуток Діріхле.

Добутком Діріхле двох арифметичних функцій f та g називається функція $f \boxtimes g$, яка визначається за правилом

$$(f \boxtimes g)(n) = \sum_{kt=n} f(k)g(t).$$

23.2. Пропозиція. (1) Множення Діріхле арифметичних функцій комутативне.

(2) Множення Діріхле арифметичних функцій асоціативне.

(3) Множення Діріхле арифметичних функцій має одиничний елемент, яким буде функція $\mathbb{E}$, що визначається за правилом $\mathbb{E}(1)=1$ та $\mathbb{E}(n) = 0$ для $n > 1$.

Доведення. Перше твердження є очевидним, оскільки множення комплексних чисел є комутативним. Щоб довести (2), розглянемо добутки $(f \boxtimes g) \boxtimes h$ та $f \boxtimes (g \boxtimes h)$. Маємо

$$\begin{aligned} ((f \boxtimes g) \boxtimes h)(n) &= \sum_{kt=n} (f \boxtimes g)(k)h(t) = \\ &= \sum_{kt=n} \left(\sum_{uv=k} f(u)g(v) \right) h(t) = \sum_{(uv)t=n} (f(u)g(v))h(t); \\ (f \boxtimes (g \boxtimes h))(n) &= \sum_{um=n} f(u)(g \boxtimes h)(m) = \sum_{um=n} f(u) \left(\sum_{vt=m} g(v)h(t) \right) = \\ &= \sum_{(uv)t=n} (f(u)g(v))h(t). \end{aligned}$$

Оскільки множення комплексних чисел є асоціативним, то

$$((f \boxtimes g) \boxtimes h)(n) = (f \boxtimes (g \boxtimes h))(n)$$

для кожного $n \in \mathbb{N}$, а це означає, що $(f \boxtimes g) \boxtimes h = (f \boxtimes (g \boxtimes h))$. Нарешті,

$$(f \boxtimes \mathbb{E})(n) = \sum_{kt=n} f(k)\mathbb{E}(t) = f(n)\mathbb{E}(1) = f(n)$$

для кожного $n \in \mathbb{N}$, і отже $f \boxtimes \mathbb{E} = f$.

Розглянемо тепер іншу важливу арифметичну функцію S , яка визначається за правилом $S(n) = 1$ для кожного $n \in N$. Маємо тоді

$$(f \boxtimes S)(n) = \sum_{kt=n} f(k) S(t) = \sum_{k|n} f(k)$$

для кожного $n \in N$ (сума береться за усіма дільниками k числа n).

Функція $f \boxtimes S$ називається суматорною функцією для функції f .

На черзі наступна важлива арифметична функція — функція Мебіуса μ , яка визначається так: $\mu(1) = 1$, і якщо $n > 1$ та $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ — його розклад на прості множники, де $p_i \neq p_j$ при $i \neq j$, то $\mu(n) = 0$ у випадку, коли $k_j \geq 2$ хоча б для одного j , і нарешті, $\mu(n) = (-1)^t$, якщо $n = p_1 p_2 \dots p_t$.

23.3. Пропозиція. $\mu \boxtimes S = \mathbb{E}$.

Д о в е д е н н я . Маємо $\mu \boxtimes S(1) = \mu(1) = 1$. Розглянемо тепер основний випадок, коли $n > 1$ та нехай $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ — його розклад на прості множники, де $p_i \neq p_j$ при $i \neq j$. Нехай μ — дільник числа n , тоді $\mu = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$, де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$. Якщо $s_j \geq 2$ хоча б для одного j , то $\mu(m) = 0$.

Позначимо через S множину всіх наборів чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$. Тоді

$$\mu(m) = \sum_{(s_1, \dots, s_t) \in S} \mu(p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}).$$

Нехай $\text{Supp}(s_1, \dots, s_t) = \{j \mid 1 \leq j \leq t, s_j = 1\}$. Маємо

$$\mu(p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}) = \begin{cases} 1, & \text{якщо } |\text{Supp}(s_1, \dots, s_t)| - \text{парне,} \\ -1, & \text{якщо } |\text{Supp}(s_1, \dots, s_t)| - \text{непарне.} \end{cases}$$

Пока $\left\{ \begin{matrix} s_2 \dots p_{t-1}^{s_{t-1}} p_t^{s_t} \end{matrix} \right\}$ ість наборів чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq 1$, у яких $|\text{Supp}(s_1, \dots, s_t)|$ — парне, дорівнює кількості таких наборів, у яких $|\text{Supp}(s_1, \dots, s_t)|$ — непарне. Звідси і буде випливати, що $\mu(n) = 0$.

Щоб довести останнє твердження, застосуємо індукцію за числом t . Нехай спочатку $t = 2$. У цьому випадку парними будуть $|\text{Supp}(0, 0)|$, $|\text{Supp}(1, 1)|$, а непарними — $|\text{Supp}(0, 1)|$ та $|\text{Supp}(1, 0)|$. Таким чином, для $t = 2$ твердження має місце.

Нехай тепер $t > 2$ і припустимо, що твердження має місце для наборів, що мають довжину $t - 1$. Нехай U (відповідно V) — множина наборів чисел $(s_1, \dots, s_t)$ довжини t , де $0 \leq s_j \leq 1$, у яких $s_t = 0$ (відповідно $s_t = 1$). Тоді $|U| = |V|$ дорівнює кількості наборів чисел $(s_1, \dots, s_{t-1})$ довжини $t - 1$, де $0 \leq s_j \leq 1$, $1 \leq j \leq t - 1$. Отже, кількість наборів чисел $(s_1, \dots, s_t)$ з підмножини U , у яких $|\text{Supp}(s_1, \dots, s_t)|$ — парне, дорівнює кількості наборів чисел $(s_1, \dots, s_{t-1})$ довжини $t - 1$, де $0 \leq s_j \leq 1$, у яких $|\text{Supp}(s_1, \dots, s_{t-1})|$ — парне, і відповідно, кількість наборів чисел $(s_1, \dots, s_t)$ з підмножини U , у яких $|\text{Supp}(s_1, \dots, s_t)|$ — непарне, дорівнює кількості наборів чисел $(s_1, \dots, s_{t-1})$ дов-

жини $t - 1$, де $0 \leq s_j \leq 1$, у яких $|\text{Supp}(s_1, \dots, s_{t-1})|$ — непарне.

Аналогічно, кількість наборів чисел $(s_1, \dots, s_t)$ з підмножини V , у яких $|\text{Supp}(s_1, \dots, s_t)|$ — парне, дорівнює кількості наборів чисел $(s_1, \dots, s_{t-1})$ довжини $t - 1$, де $0 \leq s_j \leq 1$, у яких $|\text{Supp}(s_1, \dots, s_{t-1})|$ — непарне, і відповідно, кількість наборів чисел $(s_1, \dots, s_t)$ з підмножини V , у яких $|\text{Supp}(s_1, \dots, s_t)|$ — непарне, дорівнює кількості наборів чисел $(s_1, \dots, s_{t-1})$ довжини $t - 1$, де $0 \leq s_j \leq 1$, у яких $|\text{Supp}(s_1, \dots, s_{t-1})|$ — парне. Застосувавши індуктивне припущення, отримуємо, що кількість наборів чисел $(s_1, \dots, s_t)$ з підмножини U (відповідно V), у яких $|\text{Supp}(s_1, \dots, s_t)|$ — парне, дорівнює кількості наборів чисел $(s_1, \dots, s_t)$, у яких $|\text{Supp}(s_1, \dots, s_t)|$ — непарне. Це і доводить наше твердження.

23.4. Теорема (теорема обернення Мебіуса). Нехай f — арифметична функція, F — суматорна функція для функції f . Тоді

$$f(n) = \sum_{k|n} \mu(k) F(n/k)$$

для кожного $n \in \mathbb{N}$.

Доведення. Маємо $F = f \boxtimes S$, і отже, використовуючи пропозицію 23.2, отримуємо

$$F \boxtimes \mu = (f \boxtimes S) \boxtimes \mu = f \boxtimes (S \boxtimes \mu) = f \boxtimes (\mu \boxtimes S) = f \boxtimes \mathbb{E} = f.$$

Наступною важливою арифметичною функцією, яку ми будемо далі розглядати, є функція Ейлера φ , що визначається так: $\varphi(1) = 1$, і якщо $n > 1$, то $\varphi(n)$ дорівнює кількості натуральних чисел k , що мають властивості $1 < k < n$ та $\text{GCD}(k, n) = 1$.

Наступна теорема дає інші визначення функції Ейлера.

23.5. Теорема. (1) Нехай G — скінченна циклічна група порядку n , тоді $\varphi(n)$ дорівнює кількості породжуючих елементів групи G .

(2) Співвідношення $k + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$ має місце тоді і тільки тоді, коли $\text{GCD}(k, n) = 1$. Зокрема, $\varphi(n) = |U(\mathbb{Z}/n\mathbb{Z})|$.

Доведення. (1) Маємо $G = \langle g \rangle$ для деякого елемента $g \in G$. За теоремою 10.13 елемент $y = g^k \in G$ тоді і тільки тоді буде породжуючим для G , коли $\text{GCD}(k, n) = 1$. З результатів розділу 10 також випливає, що $\langle g \rangle = \{g^0, g^1, g^2, \dots, g^{n-1}\}$, тобто число k може бути вибрано так, що $1 \leq k < n$. Це і означає, що $\varphi(n)$ дорівнює кількості породжуючих елементів групи G .

(2) Нехай $k + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$. Тоді існує такий суміжний клас $s + n\mathbb{Z}$, що $(ks + n\mathbb{Z}) = (k + n\mathbb{Z})(s + n\mathbb{Z}) = 1 + n\mathbb{Z}$. Інакше кажучи, $ks + nr = 1$ для деякого $r \in \mathbb{Z}$. З наслідку 20.7 випливає, що $\text{GCD}(k, n) = 1$. Навпаки, якщо $\text{GCD}(k, n) = 1$, то повторюючи попередні аргументи у зворотному порядку, отримуємо, що $k + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$. Звідси і випливає рівність $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$.

23.6. Наслідок (теорема Ейлера). Нехай n — натуральне число, k — ціле число, взаємно просте з n . Тоді $k^{\varphi(n)} \equiv 1 \pmod{n}$.

Доведення. Оскільки $\text{GCD}(k, n) = 1$, то з доведення попередньої теореми випливає, що $k + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$. З наслідку 12.6 та теореми 23.5 випливає рівність $(k + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$. Залишилося відзначити, що $(k + n\mathbb{Z})^{\varphi(n)} = k^{\varphi(n)} + n\mathbb{Z}$.

23.7. Наслідок (мала теорема Ферма). Нехай p — просте число, k — ціле число, що не ділиться на p . Тоді $k^{p-1} \equiv 1 \pmod{p}$.

Доведення. Дійсно, оскільки p — просте число, то $\varphi(p) = p - 1$, і залишається використати попередній наслідок.

Малу теорему Ферма можна переписати також в такій формі:

Нехай p — просте число, k — ціле число, що не ділиться на p . Тоді $k^p \equiv k \pmod{p}$.

Розглянемо суматорну функцію для функції Ейлера. Нехай G — група, розглянемо на ній бінарне відношення $\circ$, яке вводиться за наступним правилом: $x \circ y$ тоді і тільки тоді, коли $|x| = |y|$, $x, y \in G$. Незавжди упевнитись в тому, що $\circ$ є відношенням еквівалентності. Для довільного натурального числа n через G_n позначимо клас еквівалентності за цим відношенням, що складається з усіх елементів групи, які мають порядок n . Позначимо також через G_∞ сукупність тих елементів групи G , що мають нескінченний порядок. За теоремою 12.1 система підмножин $\{G_n \mid n \in \mathbb{N} \cup \{\infty\}\}$ задає розбиття групи G .

Слід відзначити, що не для кожного натурального n підмножина G_n є не пустою. Зокрема, якщо G — скінченна група, то $G_\infty = \emptyset$. Вільше того, якщо y — довільний елемент групи G , то за наслідком 12.6 $|y|$ є дільником $|G|$.

Таким чином, система підмножин $\{G_k \mid k \mid n\}$ задає розбиття групи G . Звідси випливає рівність $G = \bigcup_{k \mid n} G_k$. Також слід відзначити, що далеко не для кожного дільника k числа n підмножина G_k є не пустою.

23.8. Теорема. $\sum_{k \mid n} \varphi(k) = n$.

Доведення. Нехай $G = \langle g \rangle$ — циклічна група порядку n . Вище ми відзначали, що $G = \bigcup_{k \mid n} G_k$. З іншого боку, нехай k — довільний дільник числа n , $d = n/k$ та $x = g^d$. Маємо $x^k = (g^d)^k = g^{dk} = g^n = e$. Якщо припустити, що $x^t = e$ для деякого натурального числа $t < k$, то $e = x^t = (g^d)^t = g^{dt} = e$ і оскільки $dt < n$, то отримуємо протиріччя з тим фактом, що $|g| = |G| = n$. Отже $|x| = k$. Все це доводить, що для будь-якого дільника k числа n підмножина G_k є не пустою.

Нехай тепер z — елемент групи G , що має порядок k . Маємо $z = g^m$ для деякого натурального числа m , і тоді $e = z^k = (g^m)^k = g^{mk}$. Звідси випливає, що $n = dk \mid mk$, а отже d ділить m , тобто $m = ds$ для деякого натурального s . Таким чином,

$$z = g^m = g^{ds} = (g^d)^s = x^s,$$

що доводить включення $z \in \langle x \rangle$.

Далі $|\langle z \rangle| = |z| = |x| = k$, так що $\langle z \rangle = \langle x \rangle$. Інакше кажучи, довільний елемент групи G , що має порядок k є породжуючим елементом для підгрупи $\langle x \rangle$. За теоремою 23.5 кількість таких елементів дорівнює $\varphi(k)$. Таким чином, для кожного дільника k числа n має місце $|G_k| = \varphi(k)$. Отже,

$$n = |G| = \sum_{k|n} |G_k| = \sum_{k|n} \varphi(k).$$

23.9. Наслідок. Нехай G — скінченна група порядку n . Якщо для кожного дільника k числа n кількість тих елементів x , що задовольняють умову $x^k = e$ не перевищує k , то G — циклічна група.

Доведення. Ми вже говорили, що система підмножин $\{G_k \mid k \mid n\}$ задає розбиття групи G . Звідси випливають рівності $G = \bigcup_{k|n} G_k$ та $|G| = \sum_{k|n} |G_k|$. Припустимо, що для деякого дільника k числа n підмножина G_k є не пустою. Нехай $y \in G_k$. З наслідку 12.6 випливає, що для кожного елемента $z \in \langle y \rangle$ $|z|$ ділить число k , тобто $z^k = e$. Рівність $|y| = |\langle y \rangle| = k$ разом з умовами цього наслідку показує, що всі елементи групи G , що мають порядок k , містяться у підгрупі $\langle y \rangle$. Більш того, кожен з цих елементів буде породжуючим для підгрупи $\langle y \rangle$.

Знову застосувавши теорему 23.5, отримаємо, що кількість таких елементів дорівнює $\varphi(k)$. Таким чином, якщо для деякого дільника k числа n підмножина G_k є не пустою, то $|G_k| = \varphi(k)$. Зіставляючи дві рівності

$$n = |G| = \sum_{k|n} |G_k| \quad \text{та} \quad n = \sum_{k|n} \varphi(k)$$

отримаємо, що для кожного дільника k числа n підмножина G_k є не пустою. Зокрема $G_n \neq \emptyset$. Нехай $g \in G_n$. Рівність $n = |\langle g \rangle| = |\langle g \rangle|$ тягне за собою рівність $\langle g \rangle = G$.

23.10. Наслідок. Нехай F — поле, G — скінченна підгрупа $U(F)$. Тоді G — циклічна група.

Доведення. Нехай $|G| = n$ та k — дільник числа n . Якщо елемент у групи G задовольняє умову $y^k = e$, то він є коренем поліному $X^k - e \in F[X]$. З наслідку 17.7 випливає, що кількість таких елементів не перевищує k . З наслідку 23.9 випливає тепер, що G — циклічна група.

23.11. Наслідок. Нехай F — скінченне поле. Тоді $U(F)$ — циклічна група.

23.12. Наслідок. Нехай p — просте число. Тоді $U(\mathbb{Z}/p\mathbb{Z})$ — циклічна група.

Дійсно, у розділі 16 було доведено, що $\mathbb{Z}/p\mathbb{Z}$ — поле.

Знайшовши суматорну функцію для функції Ейлера, тепер можна отримати формулу для знаходження значень функції Ейлера. Застосувавши тепер теореми 23.4 та 23.8, будемо мати

$$\varphi(n) = \sum_{k|n} \mu(k)(n/k) = n \sum_{k|n} \mu(k)/k$$

для кожного $n \in N$. Нехай $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ — його розклад на прості множники, де $p_i \neq p_j$ при $i \neq j$. Якщо m — дільник числа n , то $m = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$, де $0 \leq s_j \leq k_j$, $1 \leq j \leq t$. Якщо $s_j \geq 2$ хоча б для одного j , то $\mu(m) = 0$. Отже,

$$\begin{aligned} \sum_{k|n} \mu(k)/k &= 1 - \sum_{1 \leq j \leq t} 1/p_j + \sum_{1 \leq j < m \leq t} (1/p_j p_m) - \dots + (-1)^t (1/p_1 p_2 \dots p_t) = \\ &= (1 - (1/p_1)) (1 - (1/p_2)) \dots (1 - (1/p_t)). \end{aligned}$$

Тому

$$\begin{aligned} \varphi(n) &= n(1 - (1/p_1)) (1 - (1/p_2)) \dots (1 - (1/p_t)) = \\ &= p_1^{k_1-1}(p_1 - 1) p_2^{k_2-1}(p_2 - 1) \dots p_t^{k_t-1}(p_t - 1). \end{aligned}$$

Зокрема, якщо p — просте число, $k \in N$, то $\varphi(p^k) = p^{k-1}(p - 1) = p^k - p^{k-1}$.

Окрім того, з отриманої формули можна побачити, що якщо натуральні числа n та k взаємно прості, то $\varphi(nk) = \varphi(n)\varphi(k)$.

Арифметична функція f називається мультиплікативною, якщо вона задовольняє дві наступні умови:

$f(n) \neq 0$ хоча б для одного натурального n ;

якщо натуральні числа n та k взаємно прості, то $f(nk) = f(n)f(k)$.

Наступна теорема дає важливу властивість мультиплікативних функцій.

23.13. Теорема. *Якщо арифметична функція f є мультиплікативною, то мультиплікативною буде її суматорна функція.*

Д о в е д е н н я . Нехай f — мультиплікативна функція, k, t — взаємно прості числа, d — довільний дільник числа kt . Тоді, очевидно, $d = uv$, де $u|k$, $v|t$. Нехай $F = f \boxtimes S$ — суматорна функція для f . Маємо тоді

$$F(kt) = \sum_{u|k, v|t} f(uv) = \sum_{u|k, v|t} f(u)f(v) = \sum_{u|k} f(u) \sum_{v|t} f(v) = F(k)F(t).$$

На закінчення цього розділу скажемо декілька слів про деякі застосування отриманих тут результатів. Не так давно таке застосування у криптографії знайшлося для функції Ейлера. У 1977 р. троє американських математиків — Р. Рейвст, А. Шамір та Л. Адлеман — запропонували нову і досить ефективну криптографічну систему з відкритим ключем. Цей спосіб шифрування був названий на честь його винахідників RSA-шифром.

В класичних криптографічних системах спосіб шифрування тримається у таємниці. А в системах з відкритим ключем тримати в таємниці спосіб шифрування немає потреби. Суть RSA-шифру полягає у наступному. Вибираються два випадкові досить великі прості числа p, q , обчислюється $n = pq$ та $\varphi(n) = (p - 1)(q - 1)$. Далі вибирається

випадкове число $k < \varphi(n)$, яке є взаємно простим з $\varphi(n)$. Як ми бачили в доведенні теореми 23.5 $k + \varphi(n)Z \in U(Z/\varphi(n)Z)$. Інакше кажучи, існує таке натуральне число t , що $kt \equiv 1 \pmod{\varphi(n)}$.

Слід зауважити, що число t можна знайти за допомогою алгоритму Евкліда, який був описаний у розділі 21. Числа n і k визначають спосіб шифрування. Вони не засекречуються і утворюють так званий відкритий ключ. Проте прості множники p, q та число t тримаються в таємниці. Повідомлення, яке потрібно зашифрувати, спочатку записується у цифровій формі за допомогою звичайних цифр 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Після цього повідомлення розбивається на блоки $M_1, \dots, M_s$, що мають довжину w . Число m вибирається так, щоб $10^w < n$. Для надійності числа p, q вибираються приблизно до ста цифр кожне.

Кожен блок M_j можна розглядати як представник суміжного класу $M_j + nZ$. Шифрування блоку M_j полягає в заміні його на такий блок $E(M_j)$, що $E(M_j) \equiv M_j^k \pmod{n}$. Оскільки число n досить велике, реально це можна зробити тільки застосовуючи комп'ютер.

Процедура дешифрування полягає у наступному. З вибору числа t випливає рівність $kt \equiv 1 + r\varphi(n)$. На цьому етапі треба застосувати теорему Ейлера (наслідок 23.6). Але з його умов ми бачимо, що воно є можливим тільки у випадку, коли числа M_j та n є взаємно простими. Покажемо зараз, що це застосування є законним у будь-якому випадку. Нехай m — довільне натуральне число. Якщо m є взаємно простим з n , то за наслідком 23.6 будемо мати $m^{\varphi(n)} \equiv 1 \pmod{n}$ та

$$m^{kt} = m^{1+r\varphi(n)} = m(m^{\varphi(n)})^r \equiv m \pmod{n}.$$

Припустимо тепер, що числа m і $n = pq$ не є взаємно простими. Тоді або m ділиться на p і не ділиться на q , або, навпаки, m ділиться на q і не ділиться на p . Розглянемо перший випадок, другий розглядається аналогічно. Маємо

$$m = pu \quad \text{та} \quad m^{kt} - m = (pu)^{kt} - pu.$$

З іншого боку,

$$m^{kt} = m^{1+r\varphi(n)} = m^{1+r(p-1)(q-1)} = m(m^{(q-1)})^{r(p-1)}.$$

Оскільки числа m і q взаємно прості, наслідок 23.7 приводить до конгруенції $(m^{(q-1)})^{r(p-1)} \equiv 1 \pmod{q}$, а тому

$$m^{kt} \equiv m(m^{(q-1)})^{r(p-1)} \pmod{q} \equiv m(1^{(q-1)})^{r(p-1)} \pmod{q} \equiv m \pmod{q}.$$

Таким чином, $m^{kt} - m$ ділиться на q . Як ми бачили вище, $m^{kt} - m$ ділиться також на p , а тому $m^{kt} - m$ ділиться на $pq = n$. Отже, у кожному випадку $m^{kt} \equiv m \pmod{n}$. Повертаючись до блоку M_j , будемо мати

$$E(M_j)^t = (M_j^k)^t = M_j^{kt} = M_j^{1+r\varphi(n)} = M_j(M_j^{\varphi(n)})^r.$$

Отже, отримаємо конгруенцію $E(M_j)^t \equiv M_j \pmod{n}$. Залишається згадати, що число M_j задовольняє умову $1 \leq M_j < n$, а тому його знаходження з конгруенції $E(M_j)^t \equiv M_j \pmod{n}$ є однозначним.

Проблема надійності RSA-шифру зводиться до питання: чи можна дешифрувати блок $E(M_p)$? Для цього потрібно розв'язати конгруенцію $x^k \equiv E(M_p) \pmod{n}$, не знаючи числа t ? Далі ми будемо розглядати конгруенції $x^k \equiv a \pmod{n}$. І тут можна сказати, що зараз не існує загальних методів для розв'язування таких конгруенцій, за виключенням простого перебору. Але з вибору w випливає, що перебір потребує розгляду 100^{100} можливих варіантів, а це поки що не дуже реально.

Таким чином, для зламування RSA-шифру потрібно розв'язати задачу: як знайти число t за відомими числами n , k . Якщо знати розклад $n = pq$, то число t знайти неважко. Виявляється, що і навпаки, знаючи числа n , k , t , можна знайти розклад $n = pq$. Отже, знаходження числа t вимагає стільки ж зусиль, скільки їх потрібно для знаходження розкладу $n = pq$. Знаходження такого розкладу у випадку, коли кожен з множників має до 100 цифр, є зараз нереальним.

24. КОНГРУЕНЦІЇ

У цьому розділі ми розглянемо питання розв'язування конгруенцій. Це частковий випадок задачі про знаходження коренів поліномів над комутативними кільцями. У розділі 17 були введені поліноми над комутативним кільцем R . Там ми обмежились випадком, коли R — область цілісності. Але така побудова є можливою і для будь-якого комутативного кільця R . Просто для цієї загальної ситуації будуть загублені деякі отримані в розділі 17 властивості кілець поліномів. Одним з перших природних випадків є випадок, коли $R = \mathbb{Z}/n\mathbb{Z}$. Для довільного цілого числа k позначимо через $k^\wedge$ суміжний клас $k + n\mathbb{Z}$. Нехай

$$f(X) = a_0^\wedge + a_1^\wedge X + \dots + a_n^\wedge X^n \in (\mathbb{Z}/n\mathbb{Z})[X],$$

тоді рівняння

$$a_0^\wedge + a_1^\wedge X + \dots + a_n^\wedge X^n = 0^\wedge$$

приводить до конгруенції

$$a_0 + a_1 X + \dots + a_n X^n \equiv 0 \pmod{n}.$$

Ціле число t називається розв'язком даної конгруенції, якщо

$$a_0 + a_1 t + \dots + a_n t^n \equiv 0 \pmod{n}.$$

Але оскільки ми розглядаємо питання про знаходження коренів поліномів над кільцем $(\mathbb{Z}/n\mathbb{Z})[X]$, то до цього означення додамо наступне уточнення.

Розв'язки t і s конгруенції $a_0 + a_1 X + \dots + a_n X^n \equiv 0 \pmod{n}$ називаються еквівалентними, якщо $t + n\mathbb{Z} = s + n\mathbb{Z}$ або $t \equiv s \pmod{n}$.

Таким чином, щоб знайти повний набір розв'язків рівняння $a_0\hat{+} + a_1\hat{X} + \dots + a_n\hat{X}^n = 0\hat{}$, потрібно знайти повний набір представників розв'язків указанного рівняння, тобто потрібно знайти повний набір нееквівалентних розв'язків конгруенції

$$a_0 + a_1t + \dots + a_nt^n \equiv 0 \pmod{n}.$$

Природним першим етапом є розгляд випадку, коли поліном $f(X)$ має степінь 1. Отже, маємо рівняння $c\hat{+} + a\hat{x} = 0\hat{+}$ або $a\hat{x} = b\hat{+}$, де $b\hat{+} = -c\hat{+}$. У свою чергу, таке рівняння приводить нас до конгруенції $ax \equiv b \pmod{n}$.

24.1. Теорема. Нехай n — натуральне число. Конгруенція $ax \equiv b \pmod{n}$ має розв'язки тоді і тільки тоді, коли $d = \text{GCD}(a, n)$ є дільником числа b . Якщо c — один з розв'язків конгруенції $ax \equiv b \pmod{n}$, то $\{c, c + m, \dots, c + (d - 1)m\}$ є повним набором нееквівалентних розв'язків указаної конгруенції, де $m = n/d$.

Доведення. Нехай u — деякий розв'язок конгруенції $ax \equiv b \pmod{n}$, тобто $(a + nZ)(u + nZ) = au + nZ = b + nZ$. Маємо $b = a + nz$ для деякого $z \in Z$. Оскільки d ділить праву частину цієї рівності, d мусить ділити число b .

Навпаки, нехай b ділиться на d , $b = b_1d$. З наслідку 20.6 випливає існування таких цілих чисел v, w , що $av + nw = d$. Помножуючи обидві частини цієї рівності на b_1 , будемо мати $avb_1 + nwb_1 = db_1$ або $a(vb_1) + nwb_1 = b$. Остання рівність показує, що число $u = vb_1$ і дає нам розв'язок конгруенції $ax \equiv b \pmod{n}$.

Слід зазначити, що ми не тільки довели достатність умови $d|b$, а показали, як знаходити розв'язок конгруенції $ax \equiv b \pmod{n}$, оскільки числа v, w ми можемо знайти, застосовуючи алгоритм Евкліда (див. розділ 21).

Нарешті, нехай c, y — два розв'язки конгруенції $ax \equiv b \pmod{n}$. Маємо

$$ac + nZ = b + nZ = ay + nZ,$$

звідки $ac - ay + nZ = nZ$, тобто $ac - ay$ ділиться на n . Нехай $a = a_1d$, тоді $md|(da_1c - da_1y)$, отже, $m|a_1(c - y)$. За наслідком 20.8 числа a_1 та m взаємно прості, тому пропозиція 20.9 показує, що $m|(c - y)$. Отже, $y = c + mk$ для деякого $k \in Z$.

Навпаки, неважко впевнитись у тому, що число y , що має вигляд $y = c + mk$, буде розв'язком конгруенції $ax \equiv b \pmod{n}$. Також очевидно, що розв'язки $c, c + m, \dots, c + (d - 1)m$, не є еквівалентними.

Знову розглянемо довільний розв'язок $y = c + mk$ конгруенції $ax \equiv b \pmod{n}$ і поділимо k на d : $k = ds + r$, $0 \leq r < d$. Тепер

$$y = c + mk = c + m(ds + r) = c + mr + mds = c + mr + ns,$$

так що розв'язок y є еквівалентним до розв'язку $c + mr$. Це й доводить той факт, що система чисел $\{c, c + m, \dots, c + (d - 1)m\}$

є повним набором нееквівалентних розв'язків конгруенції $ax \equiv b \pmod{n}$.

24.2. Наслідок. Нехай n — натуральне число. Конгруенція $ax \equiv b \pmod{n}$ завжди має розв'язки, коли числа a, n є взаємно простими. У цьому випадку всі розв'язки цієї конгруенції є еквівалентними, тобто з точністю до еквівалентності існує тільки один розв'язок цієї конгруенції.

24.3. Наслідок. Нехай p — просте число, a — натуральне число, що не ділиться на p . Тоді конгруенція $ax \equiv b \pmod{p}$ завжди має розв'язки і всі ці розв'язки є еквівалентними, тобто з точністю до еквівалентності існує тільки один розв'язок цієї конгруенції.

Якщо число n має вигляд $n = n_1 \dots n_t$, де $\text{GCD}(n_j, n_k) = 1$ при $j \neq k$, то досить часто конгруенції за модулем n можна звести до системи конгруенцій за модулем чисел $n_1, \dots, n_t$. І тут стає важливою наступна класична китайська теорема про лишки.

24.4. Лема. Нехай n — натуральне число, $b_1, \dots, b_t$ — цілі числа. Якщо $\text{GCD}(b_j, n) = 1, 1 \leq j \leq t$, то і $\text{GCD}(b_1 \dots b_t, n) = 1$.

Доведення. Дійсно з теореми 23.5 випливає, що $b_j + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$ для кожного $j, 1 \leq j \leq t$. З наслідку 9.6 випливає, що $U(\mathbb{Z}/n\mathbb{Z})$ — стала підмножина $\mathbb{Z}/n\mathbb{Z}$, а тому

$$(b_1 + n\mathbb{Z}) \dots (b_t + n\mathbb{Z}) = b_1 \dots b_t + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z}).$$

Застосовуючи знову теорему 23.5, отримаємо, що $\text{GCD}(b_1 \dots b_t, n) = 1$.

24.5. Теорема. Нехай натуральне число n має вигляд $n = n_1 \dots n_t$, де $\text{GCD}(n_j, n_k) = 1$ при $j \neq k$. Якщо $b_1, \dots, b_t$ — довільні цілі числа, то система конгруенцій $x \equiv b_1 \pmod{n_1}, \dots, x \equiv b_t \pmod{n_t}$ має розв'язки. Більш того, якщо c, d — два розв'язки цієї системи конгруенцій, то $c \equiv d \pmod{n}$.

Доведення. Нехай $m_j = n/n_j, 1 \leq j \leq t$. З леми 23.4 випливає, що $\text{GCD}(n_j, m_j) = 1$ для кожного $j, 1 \leq j \leq t$. З наслідку 20.7 випливає існування таких цілих чисел $r_j, s_j, r_j n_j + s_j m_j = 1, 1 \leq j \leq t$. Нехай $e_j = s_j m_j$, тоді $e_j + n_j \mathbb{Z} = 1 + n_j \mathbb{Z}$ та $e_j \in n_k \mathbb{Z}$, якщо $j \neq k$. Покладемо

$$c = b_1 e_1 + \dots + b_t e_t$$

і будемо мати

$$\begin{aligned} c + n_j \mathbb{Z} &= b_j e_j + \sum_{k \neq j} b_k e_k + n_j \mathbb{Z} = (b_j e_j + n_j \mathbb{Z}) + \left(\sum_{k \neq j} b_k e_k + n_j \mathbb{Z} \right) = \\ &= (b_j + n_j \mathbb{Z})(e_j + n_j \mathbb{Z}) + \sum_{k \neq j} (b_k + n_j \mathbb{Z})(e_k + n_j \mathbb{Z}) = \\ &= (b_j + n_j \mathbb{Z})(1 + n_j \mathbb{Z}) = (b_j + n_j \mathbb{Z}). \end{aligned}$$

Інакше кажучи, $c \equiv b_j \pmod{n_j}$, $1 \leq j \leq t$.

Якщо d — інший розв'язок цієї системи конгруенцій, то

$$c + n_j Z = b_j + n_j Z = d + n_j Z$$

або $c - d \in n_j Z$ чи $n_j \mid (c - d)$ для кожного j , $1 \leq j \leq t$. Застосовуючи тепер звичайно, індукцію до пропозиції 20.9, отримаємо, що $n = n_1 \dots n_t$ ділить $(c - d)$.

24.6. Наслідок. Нехай натуральне число n має вигляд $n = n_1 \dots n_t$, де $\text{GCD}(n_j, n_k) = 1$ при $j \neq k$. Тоді

$$Z/nZ \cong Z/n_1Z \times \dots \times Z/n_tZ$$

та

$$U(Z/nZ) \cong U(Z/n_1Z) \times \dots \times U(Z/n_tZ).$$

Д о в е д е н н я . Розглянемо відображення

$$f: Z \longrightarrow Z/n_1Z \times \dots \times Z/n_tZ = R,$$

що визначається за правилом $f(k) = (k + n_1Z, \dots, k + n_tZ)$ для кожного $k \in Z$. Відображення f є гомоморфізмом. Дійсно

$$\begin{aligned} f(k + s) &= (k + s + n_1Z, \dots, k + s + n_tZ) = \\ &= (k + n_1Z + s + n_1Z, \dots, k + n_tZ + s + n_tZ) = \\ &= (k + n_1Z, \dots, k + n_tZ) + (s + n_1Z, \dots, s + n_tZ) = f(k) + f(s); \end{aligned}$$

$$\begin{aligned} f(ks) &= (ks + n_1Z, \dots, ks + n_tZ) = \\ &= ((k + n_1Z)(s + n_1Z), \dots, (k + n_tZ)(s + n_tZ)) = \\ &= (k + n_1Z, \dots, k + n_tZ)(s + n_1Z, \dots, s + n_tZ) = f(k)f(s). \end{aligned}$$

Нехай тепер $(k_1 + n_1Z, \dots, k_t + n_tZ)$ — довільний елемент кільця R . За теоремою 24.5 існує таке число $k \in Z$, що $k + n_jZ = k_j + n_jZ$ для кожного j , $1 \leq j \leq t$. Інакше кажучи,

$$(k_1 + n_1Z, \dots, k_t + n_tZ) = (k + n_1Z, \dots, k + n_tZ) = f(k).$$

Таким чином, f — епіморфізм. За теоремою 16.12 $R \cong Z/\text{Ker } f$. Залишилось з'ясувати, яким буде $\text{Ker } f$. Нехай $k \in \text{Ker } f$, тоді

$$f(k) = (k + n_1Z, \dots, k + n_tZ) = (n_1Z, \dots, n_tZ),$$

так що $k \in n_jZ$ для кожного j , $1 \leq j \leq t$. Отже $n_j \mid k$ для кожного j , $1 \leq j \leq t$. Застосовуючи тепер звичайно, індукцію до пропозиції 20.9, отримаємо, що також $n = n_1 \dots n_t$ ділить k , тобто $k \in nZ$.

Навпаки, якщо $k \in nZ$, то повторюючи попередні аргументи в зворотному порядку, отримаємо включення $k \in \text{Ker } f$. Таким чином, $\text{Ker } f = nZ$ і $Z/nZ \cong R = Z/n_1Z \times \dots \times Z/n_tZ$.

Зважаючи на отриманий у розділі 15 опис групи інвертованих елементів декартового добутку кілець, будемо мати

$$U(Z/nZ) \cong U(Z/n_1Z) \times \dots \times U(Z/n_iZ).$$

24.7. Наслідок. Нехай n — натуральне число, $n = p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}$ — його розклад на прості множники, де $p_i \neq p_j$ при $i \neq j$. Тоді

$$Z/nZ \cong Z/p_1^{k_1}Z \times \dots \times Z/p_i^{k_i}Z$$

та

$$U(Z/nZ) \cong U(Z/p_1^{k_1}Z) \times \dots \times U(Z/p_i^{k_i}Z).$$

Наслідок 24.7 зводить опис Z/nZ та $U(Z/nZ)$ до випадку, коли $n = p^k$ — степінь простого числа p . Як ми побачимо вище, цей випадок розщеплюється ще на два: p — непарне і $p = 2$.

Нехай n — натуральне число, скажемо, що це число має примітивний або первісний корінь, якщо група $U(Z/nZ)$ є циклічною. При цьому число k називається примітивним коренем за модулем n , якщо $\langle k + nZ \rangle = U(Z/nZ)$.

З теореми 23.5 випливає, зокрема, що $\text{GCD}(k, n) = 1$. Більш того, враховуючи той факт, що $|k + nZ| = |\langle k + nZ \rangle|$ з теореми 23.5 отримуємо, що $|k + nZ| = \varphi(n)$.

Нехай k — ціле число, n — натуральне число, для якого $\text{GCD}(k, n) = 1$. Порядком числа k за модулем n будемо називати порядок $k + nZ$ як елемента групи $U(Z/nZ)$.

24.8. Пропозиція. Нехай n — натуральне число. Ціле число k тоді і тільки тоді буде примітивним коренем за модулем n , коли порядок числа k за модулем n дорівнює $\varphi(n)$.

Доведення. Якщо k — примітивний корінь за модулем n , то як ми бачили трохи раніше, $|k + nZ| = \varphi(n)$. Навпаки, нехай порядок числа k за модулем n дорівнює $\varphi(n)$. Тоді також $\varphi(n) = |k + nZ| = |\langle k + nZ \rangle|$. Теорема 23.5 показує, що $\varphi(n) = |U(Z/nZ)|$, так що

$$|\langle k + nZ \rangle| = |U(Z/nZ)|$$

і, отже

$$\langle k + nZ \rangle = U(Z/nZ),$$

зокрема, група $U(Z/nZ)$ є циклічною.

Зразу слід зазначити, що не кожне натуральне число має примітивний корінь. Наприклад,

$$U(Z/8Z) = \{ 1 + 8Z, 3 + 8Z, 5 + 8Z, 7 + 8Z \} \text{ і}$$

$$(3 + 8Z)^2 = 9 + 8Z = 1 + 8Z,$$

$$(5 + 8Z)^2 = 25 + 8Z = 1 + 8Z,$$

$$(7 + 8Z)^2 = 49 + 8Z = 1 + 8Z.$$

В той же час $\phi(8) = |U(Z/8Z)| = 8 - 4 = 4$. Отже, група $U(Z/8Z)$ не є циклічною, так що число 8 не має примітивних коренів.

Але у випадку $p \neq 2$ ситуація є іншою. Розглянемо її детальніше.

24.9. Лема. Нехай t — натуральне число, a, b — цілі числа, p — просте число. Якщо $a \equiv b \pmod{p^t}$, то $a^p \equiv b^p \pmod{p^{t+1}}$.

Доведення. Маємо $a = b + cp^t$ для деякого цілого числа c . Звідси отримуємо рівність

$$a^p = b^p + C_1^p b^{p-1} cp^t + d,$$

де

$$d = C_2^p b^{p-2} (cp^t)^2 + \dots + C_{p-1}^p b (cp^t)^{p-1} + (cp^t)^p,$$

і $C_k^p = (p!)/((k!)(p-k)!)$ — біноміальні коефіцієнти. Як ми вже бачили у розділі 22, C_k^p ділиться на p , $1 \leq k \leq p$. Розглядаючи довільний член $C_k^p b^{p-k} (cp^t)^k$ з розкладу числа d , де $2 \leq k \leq p$, бачимо, що він ділиться на $pp^{tk} = p^{tk+1}$ і p^{t+1} . Останній член $(cp^t)^p$ розкладу числа d також ділиться на p^{t+1} , оскільки $pt - (t+1) = pt - t - 1 = t(p-1) - 1 \geq t-1 \geq 0$.

Таким чином, d ділиться на p^{t+1} і маємо

$$a^p = b^p + pb^{p-1}cp^t + d = b^p + p^{t+1}b^{p-1}c + p^{t+1}d_1,$$

так що дійсно $a^p \equiv b^p \pmod{p^{t+1}}$.

24.10. Лема. Нехай t — натуральне число, a — ціле число, p — непарне просте число. Якщо $t \geq 2$, $s = p^{t-2}$, то $(1+ap)^s \equiv 1 + ap^{t-1} \pmod{p^t}$.

Доведення. Застосуємо індукцію за числом t . Якщо $t = 2$, то твердження є очевидним. Нехай тепер $t \geq 2$ і припустимо, що твердження є справедливим для t . З леми 24.9 отримуємо, що

$$(1+ap)^{sp} \equiv (1+ap^{t-1})^p \pmod{p^{t+1}},$$

де $sp = p^{t-2}p = p^{t-1}$.

Далі

$$(1+ap^{t-1})^p = 1 + C_1^p ap^{t-1} + d,$$

де

$$d = C_2^p (ap^{t-1})^2 + \dots + C_{p-1}^p b (ap^{t-1})^{p-1} + (ap^{t-1})^p,$$

і $C_k^p = (p!)/((k!)(p-k)!)$ — біноміальні коефіцієнти.

Як ми бачили у розділі 22, C_k^p ділиться на p , $1 \leq k \leq p$. Розглядаючи довільний член $C_k^p (ap^{t-1})^k$ з розкладу числа d , де $2 \leq k \leq p$, бачимо, що він ділиться на $pp^{(t-1)k} \geq p^{t+1}$, оскільки

$$tk - k - t - 1 = tk - k - t = t(k-1) - k \geq 2k - 2 - k = k - 2 \geq 0.$$

Останній член $(ap^{t-1})^p$ розкладу числа d також ділиться на p^{t+1} , оскільки $(t-1)p - t - 1 \geq 3(t-1) - t - 1 = 2t - 4 \geq 0$. Таким чином, d ділиться на p^{t+1} і маємо

$$(1 + ap^{t-1})^p = 1 + pap^{t-1} + d = 1 + ap^t + p^{t+1}d_1,$$

так що дійсно $(1 + ar)^m \equiv 1 + ar^t \pmod{p^{t+1}}$, де $m = p^{t-1}$.

24.11. Наслідок. Нехай t — натуральне число, a — ціле число, p — непарне просте число. Якщо a не ділиться на p , то порядок числа $1 + ar$ за модулем p^t дорівнює p^{t-1} .

Доведення. З леми 24.10 отримуємо, що $(1 + ar)^m \equiv 1 + ar^t \pmod{p^{t+1}}$, де $m = p^{t-1}$, так що $(1 + ar)^m \equiv 1 \pmod{p^t}$. Інакше кажучи, порядок $1 + ar + p^tZ$ як елемент групи $U(Z/p^tZ)$ ділить число p^{t-1} . З іншого боку, якщо $s = p^{t-2}$, то за лемою 24.10 $(1 + ar)^s \equiv 1 + ar^{t-1} \pmod{p^t}$. Оскільки a не ділиться на p , то $(1 + ar)^s + p^tZ \neq 1 + p^tZ$. Це і означає, $|1 + ar + p^tZ| = p^{t-1}$.

24.12. Теорема. Нехай t — натуральне число, p — непарне просте число. Тоді $U(Z/p^tZ)$ — циклічна група. Інакше кажучи, число p^t має примітивні корені.

Доведення. З наслідку 23.12 отримуємо, що $U(Z/pZ)$ — циклічна група. Нехай m — ціле число, що має властивість $\langle m + pZ \rangle = U(Z/pZ)$. Припустимо, що $m^{p-1} \equiv 1 \pmod{p^2}$ і розглянемо у цьому випадку число $m + p$. Маємо

$$(m + p)^{p-1} = m^{p-1} + (p-1)m^{p-2}p + p^2d,$$

і оскільки $(p-1)m^{p-2}$ не ділиться на p , то $(m + p)^{p-1} - 1$ не ділиться на p^2 . В той же час $m + p + pZ = m + pZ$. Таким чином, якщо $m^{p-1} \equiv 1 \pmod{p^2}$, то замінюємо m на $m + p$. Тому, щоб не вводити далі нових позначень, будемо вважати, що $m^{p-1} - 1$ не ділиться на p^2 . Нехай порядок $m + p^tZ$ як елемент групи $U(Z/p^tZ)$ дорівнює n . За наслідком 23.7 $m^{p-1} \equiv 1 + ar$, де a не ділиться на p . Далі

$$\begin{aligned} (1 + ar + p^tZ)^n &= (m^{p-1} + p^tZ)^n = ((m + p^tZ)^{p-1})^n = \\ &= ((m + p^tZ)^n)^{p-1} = (1 + p^tZ)^{p-1} = 1 + p^tZ. \end{aligned}$$

Наслідок 24.11 показує, що $1 + ar + p^tZ$ як елемент групи $U(Z/p^tZ)$ має порядок p^{t-1} . Звідси випливає, що n ділиться на $s = p^{t-1}$: $n = p^{t-1}k = sk$. Далі $(m + pZ)^n = (m + pZ)^{sk}$. За наслідком 23.7 $(m + pZ)^{p-1} = 1 + pZ$, а тому

$$(m + pZ)^p = (m + pZ)^{p-1}(m + pZ) = (1 + pZ)(m + pZ) = m + pZ.$$

За допомогою звичайної індукції отримаємо звідси рівність $(m + pZ)^s = (m + pZ)$. Отже,

$$(m + pZ)^n = (m + pZ)^{sk} = (m + pZ)^k.$$

З рівності $(m + p^tZ)^n = 1 + p^tZ$ отримуємо, що і $(m + pZ)^n = 1 + pZ$, отже $(m + pZ)^k = 1 + pZ$. У свою чергу, рівність $\langle m + pZ \rangle = U(Z/pZ)$ показує, що $|m + pZ| = |\langle m + pZ \rangle| = |U(Z/pZ)|$,

а за теоремою 23.5 $|U(Z/pZ)| = \varphi(p) = p - 1$. Отже, маємо $|m + pZ| = p - 1$.

Отримана вище рівність $(m + pZ)^k = 1 + pZ$ показує, що k ділиться на $p - 1$, а тому $n = p^{t-1}k$ ділиться на $p^{t-1}(p - 1) = \varphi(p^t)$. З іншого боку, з наслідку 12.6 випливає, що n ділить $|U(Z/p^tZ)| = \varphi(p^t)$. Таким чином, $n = \varphi(p^t)$. Застосування пропозиції 24.8 завершує доведення.

Як ми могли бачити з доведення цієї теореми, вона ще й указує, як знаходити примітивний корінь. Більш конкретно, вона показує, що його можна знайти, якщо є знайденим хоча б один примітивний корінь за модулем простого числа p . У загальному випадку ця задача є досить непростою. Наступна теорема показує, як можна суттєво зменшити можливий перебір усіх варіантів.

24.13. Теорема. Нехай q — непарне просте число, $q - 1 = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ — його розклад на прості множники, де $p_i \neq p_j$ при $i \neq j$. Ціле число g , взаємно просте з q , тоді і тільки тоді буде примітивним коренем за модулем q , коли воно не є розв'язком жодної з наступних конгруенцій

$$x^{(q-1)/p_j} \equiv 1 \pmod{q}, \quad 1 \leq j \leq t.$$

Доведення. Дійсно, якщо g — примітивний корінь за модулем q , то згідно з пропозицією 24.8 $|g + qZ| = q - 1$. Таким чином, якщо p — довільний простий дільник числа $q - 1$, то $(g + qZ)^{(q-1)/p} \neq 1 + qZ$, зокрема, g не може задовольняти ні одну з виписаних вище конгруенцій.

Навпаки, нехай ціле число g , взаємно просте з q , не є розв'язком жодної з наступних конгруенцій $x^{(q-1)/p_j} \equiv 1 \pmod{q}$, $1 \leq j \leq t$. Припустимо, що в той же час g не є примітивним коренем за модулем q . Інакше кажучи, $\langle g + qZ \rangle \neq U(Z/qZ)$.

З наслідку 12.6 отримуємо, що $|g + qZ| = m$, де m — власний дільник числа $q - 1$. Але тоді $m = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, де $r_j \leq k_j$, $1 \leq j \leq t$, й існує такий індекс s , що $r_s \neq k_s$. Зокрема, m є дільником числа $(q - 1)/p_s$, тому $1 + qZ = (g + qZ)^m = (g + qZ)^{(q-1)/p_s}$.

Таким чином, число g задовольняє конгруенцію $x^{(q-1)/p_s} \equiv 1 \pmod{q}$, що суперечить нашій умові. Отримане протиріччя доводить, що g є примітивним коренем за модулем q .

На черзі розгляд випадку, коли $p = 2$.

24.14. Теорема. Нехай t — натуральне число. Тоді $U(Z/2Z) \neq U(Z/4Z)$ — циклічні групи. Якщо $t \geq 3$, то

$$U(Z/2^tZ) = \{(-1)^a 5^b + 2^tZ \mid a \in \{0, 1\}, 0 \leq b \leq 2^{t-2}\}.$$

Доведення. Очевидно $U(Z/2Z) = \{1 + 2Z\} = \langle 1 + 2Z \rangle$, $U(Z/4Z) = \{1 + 4Z, 3 + 4Z\} = \langle 3 + 4Z \rangle$.

Нехай $t \geq 3$. Покажемо спочатку, що має місце конгруенція $5^s \equiv 1 + 2^{t-1} \pmod{2^t}$, де $s = 2^{t-3}$. Для $t = 3$ вона є очевидною. Припустимо, що вона має місце для $t \geq 3$ і покажемо, що

вона має місце для числа $t + 1$. Застосовуючи до конгруенції $5^s \equiv 1 + 2^{t-1} \pmod{2^t}$ лему 24.9, маємо $(5^s)^2 \equiv (1 + 2^{t-1})^2 \pmod{2^{t+1}}$. Далі $2s = 2(2^{t-2}) = 2^{t-1}$ та

$$(1 + 2^{t-1})^2 = 1 + 2 \cdot 2^{t-1} + (2^{t-1})^2 = 1 + 2^t + 2^{2t-2}.$$

Оскільки $t \geq 3$, то $2t - 2 \geq t + 1$, отже отримуємо $5^m \equiv 1 + 2^t \pmod{2^{t+1}}$, де $m = 2^{t-2}$. З доведеної конгруенції отримуємо рівність

$$(5 + 2^t Z)^m = 5^m + 2^t Z = 1 + 2^t Z,$$

де $m = 2^{t-2}$, тобто порядок $5 + 2^t Z$ як елемента групи $U(Z/2^t Z)$ ділить число 2^{t-2} .

З іншого боку, якщо $s = 2^{t-3}$, то $5^s \equiv 1 + 2^{t-1} \pmod{2^t}$ і $5^s + 2^t Z \neq 1 + 2^t Z$. Це і означає, $|5 + 2^t Z| = 2^{t-2}$.

Розглянемо множину $\{(-1)^a 5^b + 2^t Z \mid a \in \{0, 1\}, 0 \leq b \leq 2^{t-2}\}$. Припустимо, що $(-1)^a 5^b + 2^t Z = (-1)^c 5^d + 2^t Z$ для деяких $a, c \in \{0, 1\}$, $0 \leq b, d \leq 2^{t-2}$. Тоді, очевидно, $(-1)^a + 4Z = (-1)^c + 4Z$, а це можливо тільки при $a = c$. Звідси випливає рівність $5^b + 2^t Z = 5^d + 2^t Z$, яка тягне за собою рівність $(5 + 2^t Z)^{b-d} = 1 + 2^t Z$. Оскільки $|5 + 2^t Z| = 2^{t-2}$, то це означає, що $b - d$ ділиться на 2^{t-2} , а це, зважаючи на їх вибір, означає, що $b - d = 0$ і $b = d$.

Таким чином, всі елементи множини $\{(-1)^a 5^b + 2^t Z \mid a \in \{0, 1\}, 0 \leq b \leq 2^{t-2}\}$ є попарно різними, а тому

$$|\{(-1)^a 5^b + 2^t Z \mid a \in \{0, 1\}, 0 \leq b \leq 2^{t-2}\}| = 2 \cdot 2^{t-2} = 2^{t-1} = \varphi(2^t).$$

За теоремою 23.5 $|U(Z/2^t Z)| = \varphi(2^t)$, отже,

$$U(Z/2^t Z) = \{(-1)^a 5^b + 2^t Z \mid a \in \{0, 1\}, 0 \leq b \leq 2^{t-2}\}.$$

Перейдемо до розгляду конгруенцій більш високих степенів. Спочатку розглянемо конгруенції, що мають вигляд $x^k \equiv a \pmod{n}$.

Нехай n, k — натуральні числа, a — таке ціле число, що $\text{GCD}(a, n) = 1$. Будемо говорити, що $a - k$ — степеневий лишок за модулем n , якщо конгруенція $x^k \equiv a \pmod{n}$ має розв'язок y , для якого $\text{GCD}(y, n) = 1$.

24.15. Теорема. Нехай n, k — натуральні числа, a — таке ціле число, що $\text{GCD}(a, n) = 1$. Припустимо також, що n має примітивні корені. Число a буде k -степеневим лишком за модулем n тоді і тільки тоді, коли $a^{(\varphi(n)/d)} \equiv 1 \pmod{n}$, де $d = \text{GCD}(k, \varphi(n))$. Більш того, якщо конгруенція $x^k \equiv a \pmod{n}$ має розв'язки, то вона має рівно d розв'язків.

Доведення. Нехай g — примітивний корінь за модулем n , $\langle g + nZ \rangle = U(Z/nZ)$. Припустимо, що y — один з розв'язків конгруенції $x^k \equiv a \pmod{n}$, для якого $\text{GCD}(y, n) = 1$. З теореми 23.5 випливає, що $y + nZ, a + nZ \in U(Z/nZ)$. Тоді $a + nZ = (y + nZ)^k = g^b + nZ$, та $y + nZ = (g + nZ)^z = g^z + nZ$, для деяких $b, z \in Z$. Маємо

$$g^b + nZ = a + nZ = (y + nZ)^k = (g^z + nZ)^k = g^{zk} + nZ.$$

З цієї рівності отримуємо

$$(g + nZ)^{kz} = (g + nZ)^b \cdot 1 + nZ = (g + nZ)^{kz-b} = g^{kz-b} + nZ.$$

Рівність $\langle g + nZ \rangle = U(Z/nZ)$ разом з теоремою 23.5 дає рівність $|g + nZ| = \varphi(n)$, з якої випливає, що $kz - b$ ділиться на $\varphi(n)$. Отже, приходимо до конгруєнції $kz \equiv b \pmod{\varphi(n)}$. За теоремою 24.1 d мусить ділити число b , тобто $b = cd$ для деякого натурального числа c . Маємо

$$(a + nZ)^{(\varphi(n)/d)} = (g + nZ)^{(b\varphi(n)/d)} = (g + nZ)^{\varphi(n)c} = ((g + nZ)^{\varphi(n)})^c = 1 + nZ,$$

тобто отримали конгруєнцію $a^{(\varphi(n)/d)} \equiv 1 \pmod{n}$.

Навпаки, нехай остання конгруєнція має місце. Тоді має місце рівність $(g + nZ)^{(b\varphi(n)/d)} = 1 + nZ$. Оскільки $|g + nZ| = \varphi(n)$, то це означає, що $b\varphi(n)/d$ ділиться на $\varphi(n)$, а це означає, що d ділить b .

Слід також відзначити, що конгруєнція $kz \equiv b \pmod{\varphi(n)}$ має рівно d розв'язків за тією ж теоремою 24.1. З аргументів, що були наведені вище, можна побачити, що різним розв'язкам конгруєнції $kz \equiv b \pmod{\varphi(n)}$ відповідають різні розв'язки конгруєнції $x^k \equiv a \pmod{n}$ і навпаки. Таким чином, вказана конгруєнція має рівно d розв'язків.

Нехай n — натуральне число та $n = 2^{k_1} p_2^{k_2} \dots p_t^{k_t}$ — його розклад на прості множники, де $p_i \neq p_j$ при $i \neq j$, k — натуральне число, a — таке ціле число, що $\text{GCD}(a, n) = 1$. Розглянемо систему конгруєнцій

$$x^m \equiv a \pmod{2^{k_1}}, x^m \equiv a \pmod{p_2^{k_2}}, \dots, x^m \equiv a \pmod{p_t^{k_t}}.$$

Припустимо, що ці конгруєнції мають своїми розв'язками числа $y_1, \dots, y_t$ відповідно. З теореми 24.5 випливає існування такого цілого числа y , що

$$y + 2^{k_1}Z = y_1 + 2^{k_1}Z, y + p_2^{k_2}Z = y_2 + p_2^{k_2}Z, \dots, y + p_t^{k_t}Z = y_t + p_t^{k_t}Z.$$

Тоді маємо

$$y^m + 2^{k_1}Z = (y + 2^{k_1}Z)^m = (y_1 + 2^{k_1}Z)^m = y_1^m + 2^{k_1}Z = a + 2^{k_1}Z.$$

Аналогічно $y^m + p_j^{k_j}Z = a + p_j^{k_j}Z$, $2 \leq j \leq t$. Інакше кажучи, $y^m - a \in 2^{k_1}Z$ і $y^m - a \in p_j^{k_j}Z$, $2 \leq j \leq t$, тобто $y^m - a$ ділиться на 2^{k_1} та на $p_j^{k_j}$, $2 \leq j \leq t$, отже, $y^m - a$ ділиться на їх добуток $n = 2^{k_1} p_2^{k_2} \dots p_t^{k_t}$. Ми бачимо, що y є розв'язком конгруєнції $x^m \equiv a \pmod{n}$. Повторюючи ті ж самі аргументи, але в зворотному порядку, з'ясуємо, що кожен розв'язок конгруєнції $x^m \equiv a \pmod{n}$ буде і розв'язком системи конгруєнцій $x^m \equiv a \pmod{2^{k_1}}$, $x^m \equiv a \pmod{p_2^{k_2}}$, $\dots$, $x^m \equiv a \pmod{p_t^{k_t}}$.

Таким чином, питання про знаходження розв'язків конгруєнції $x^m \equiv a \pmod{n}$ зводиться до випадку, коли $n = p^k$, де p — просте число. Якщо $p \neq 2$, то з теореми 24.12 випливає, що p^k має примітивні корені, так що можна застосувати теорему 24.15. Випадок $p = 2$ знову потребує окремого розгляду. Якщо $k \leq 2$, то 2^k має примітивні корені, так що можна застосувати теорему 24.15. Отже, основним буде випадок, коли $k \geq 3$.

24.16. Теорема. Нехай n, t — натуральні числа, $t \geq 3$, a — непарне ціле число. Якщо n є непарним, то конгруенція $x^n \equiv a \pmod{2^t}$ має єдиний розв'язок. Якщо n є парним, то число a буде n -степеневим лишком за модулем 2^t тоді і тільки тоді, коли $a \equiv 1 \pmod{4}$, $a^{s/d} \equiv 1 \pmod{2^t}$, де $s = 2^{t-2}$, $d = \text{GCD}(n, 2^{t-2})$. Більш того, якщо вказана конгруенція має розв'язки, то вона має рівно $2d$ розв'язків.

Доведення. Нехай n є непарним. З результатів розділу 23 отримуємо рівність $m = \varphi(2^t) = 2^{t-1}(2-1) = 2^{t-1}$. За наслідком 20.7 існують такі цілі числа u, v , що $un + mv = 1$. Для довільного цілого числа x введемо позначення $\hat{x} = x + 2^t\mathbb{Z}$. Будемо мати

$$\hat{a} = \hat{a}^1 = \hat{a}^{un + mv} = (\hat{a}^{un})(\hat{a}^{mv}) = (\hat{a}^u)^n(\hat{a}^m)^v.$$

З наслідку 23.6 випливає, що $(\hat{a}^m) = 1$. Таким чином, ми бачимо, що число $y = \hat{a}^u$ буде розв'язком конгруенції $x^n \equiv a \pmod{2^t}$. Слід також зазначити, що число u можна знайти, застосовуючи алгоритм Евкліда (див. розділ 21).

Розглянемо випадок, коли число n є парним. Припустимо, що y — непарне ціле число, яке є одним з розв'язків конгруенції $x^n \equiv a \pmod{2^t}$. З теореми 23.5 випливає, що $y + 2^t\mathbb{Z}$, $a + 2^t\mathbb{Z} \in U(\mathbb{Z}/2^t\mathbb{Z})$. Враховуючи теорему 24.13, отримуємо

$$a + 2^t\mathbb{Z} = (-1)^b 5^c + 2^t\mathbb{Z}, y + 2^t\mathbb{Z} = (-1)^r 5^z + 2^t\mathbb{Z}$$

для деяких $b, c, z, r \in \mathbb{Z}$. Тепер будемо мати

$$\begin{aligned} (-1)^b 5^c + 2^t\mathbb{Z} &= a + 2^t\mathbb{Z} = (y + 2^t\mathbb{Z})^n = ((-1)^r 5^z + 2^t\mathbb{Z})^n = \\ &= (-1)^{rn} 5^{zn} + 2^t\mathbb{Z} = 5^{zn} + 2^t\mathbb{Z}. \end{aligned}$$

Зокрема, $b = 0$, а це означає, що $a \equiv 1 \pmod{4}$ і $a + 2^t\mathbb{Z} = 5^c + 2^t\mathbb{Z}$. Нехай $n = dw$, тоді маємо

$$\begin{aligned} (a + 2^t\mathbb{Z})^{s/d} &= (5^c + 2^t\mathbb{Z})^{s/d} = (5^{kn} + 2^t\mathbb{Z})^{s/d} = (5 + 2^t\mathbb{Z})^{kns/d} = \\ &= (5 + 2^t\mathbb{Z})^{skdw/d} = (5 + 2^t\mathbb{Z})^{skw}. \end{aligned}$$

З доведення теореми 24.13 випливає, що порядок числа 5 дорівнює s , тобто $(a + 2^t\mathbb{Z})^{s/d} = 1 + 2^t\mathbb{Z}$ або $a^{s/d} \equiv 1 \pmod{2^t}$. Рівняння

$$(5 + 2^t\mathbb{Z})^c = 5^c + 2^t\mathbb{Z} = 5^{zn} + 2^t\mathbb{Z} = (5 + 2^t\mathbb{Z})^{zn}$$

приводить до конгруенції $nz \equiv c \pmod{2^{t-2}}$. За теоремою 24.1 ця конгруенція має рівно d розв'язків. Нарешті, слід сказати, що разом з числом y число $-y$ буде розв'язком конгруенції $x^n \equiv a \pmod{2^t}$.

Навпаки, нехай $a \equiv 1 \pmod{4}$ та конгруенція $a^{s/d} \equiv 1 \pmod{2^t}$ має місце. Зокрема, $b = 0$, тобто $a + 2^t\mathbb{Z} = 5^c + 2^t\mathbb{Z}$. Тоді має місце рівність

$$1 + 2^t\mathbb{Z} = (a + 2^t\mathbb{Z})^{s/d} = (5^c + 2^t\mathbb{Z})^{s/d} = (5 + 2^t\mathbb{Z})^{cs/d}.$$

Доводячи теорему 24.13, ми показали, що $|5 + 2^t Z| = 2^{t-2} = s$, а тому число cs/d мусить ділитися на s , а це означає, що $d | c$. У цьому випадку згідно з теоремою 24.1 конгруенція $nz \equiv c \pmod{2^{t-2}}$ має розв'язок. Як ми вже бачили, у свою чергу з цього випливає, що число y (разом з числом $-y$), для якого $y + 2^t Z = 5^z + 2^t Z$ буде розв'язком конгруенції $x^n \equiv a \pmod{2^t}$.

Розглянемо тепер важливий частинний випадок конгруенції $x^m \equiv a \pmod{2^t}$, коли $n = p$ — непарне просте число, $m = 2$, тобто конгруенцію $x^2 \equiv a \pmod{p}$. Оскільки $p \neq 2$, то

$$-1 + pZ = (p-1) + pZ \neq 1 + pZ,$$

отже, $-1^{\wedge} = -1 + pZ$ та $1^{\wedge} = 1 + pZ$ будуть єдиними розв'язками рівняння $X^2 = 1^{\wedge}$. Використовуючи наслідок 23.7, для довільного цілого числа a , взаємно простого з p , будемо мати

$$((a + pZ)^{(p-1)/2})^2 = (a + pZ)^{p-1} = 1 + pZ,$$

а це, у свою чергу, показує, що або $(a + pZ)^{(p-1)/2} = -1 + pZ$, або $(a + pZ)^{(p-1)/2} = 1 + pZ$.

Нехай a — ціле число, що не ділиться на непарне просте число p . Визначимо символ $\langle a/p \rangle$, за наступним правилом

$$\langle a/p \rangle = \begin{cases} 1, & \text{якщо } a \text{ — квадратичний лишок за модулем } p, \\ -1, & \text{якщо } a \text{ не є квадратичним лишком за модулем } p. \end{cases}$$

(тут термін «квадратичний лишок» означає 2-степеневий лишок).

Символ $\langle a/p \rangle$ називають *символом Лежандра*.

24.17. Тесрема. Нехай p — непарне ціле число, a, b — цілі числа, взаємно прості з p .

- (1) Число a тоді і тільки тоді буде квадратичним лишком за модулем p , коли $a^{(p-1)/2} \equiv 1 \pmod{p}$.
- (2) $a^{(p-1)/2} \equiv \langle a/p \rangle \pmod{p}$.
- (3) $\langle ab/p \rangle \pmod{p} \equiv \langle a/p \rangle \langle b/p \rangle \pmod{p}$.

Д о в е д е н н я . За наслідком 23.12 p має примітивні корні, так що для доведення твердження (1) можна застосувати теорему 24.15. Твердження (1) разом з наведеними перед цією теоремою аргументами доводить (2). Оскільки фактор-кільце (Z/pZ) є комутативним, то

$$((a + pZ)(b + pZ))^k = (a + pZ)^k(b + pZ)^k$$

для будь-якого цілого k . Зокрема,

$$\begin{aligned} \langle ab/p \rangle + pZ &= (ab + pZ)^{(p-1)/2} = ((a + pZ)(b + pZ))^{(p-1)/2} = \\ &= (a + pZ)^{(p-1)/2} (b + pZ)^{(p-1)/2} = (\langle a/p \rangle + pZ)(\langle b/p \rangle + pZ), \end{aligned}$$

що і доводить (3).

Розглянемо питання про розв'язок загальних конгруенцій другого степеня, тобто конгруенцій $ax^2 + bx + c \equiv 0 \pmod{p}$, де p — непарне просте число. Якщо a ділиться на p , то наша конгруенція перетворюється на конгруенцію першого степеня, які вже були раніше розглянуті. Отже, можна припустити, що числа a та p є взаємно простими. З теореми 24.1 випливає, що конгруенції $ax \equiv b \pmod{p}$ та $ax \equiv c \pmod{p}$ мають єдиний розв'язок, і нехай числа b_1 та c_1 — розв'язки цих конгруенцій відповідно. Приходимо до конгруенції $ax^2 + ab_1x + ac_1 \equiv 0 \pmod{p}$, і знову використовуючи взаємну простоту чисел a і p , отримуємо з неї конгруенцію $x^2 + b_1x + c_1 \equiv 0 \pmod{p}$. Оскільки p — непарне просте число, то з теореми 24.1 випливає, що конгруенція $2x \equiv b_1 \pmod{p}$ має єдиний розв'язок, який позначимо через b_2 . Отже, маємо наступну конгруенцію $x^2 + 2b_2x + c_1 \equiv 0 \pmod{p}$. Застосуємо наступні звичайні перетворення

$$x^2 + 2b_2x + c_1 = x^2 + 2b_2x + b_2^2 + (c_1 - b_2^2) = (x + b_2)^2 + c_2,$$

де $c_2 = (c_1 - b_2^2)$.

Нехай $y = x + b_2$, $c_3 = -c_2$, так що отримали конгруенцію $y^2 \equiv c_3 \pmod{p}$. Тепер за допомогою теореми 24.17 залишається з'ясувати, чи є число c_3 квадратичним лишком за модулем p , і якщо це так, то розв'язати конгруенцію $y^2 \equiv c_3 \pmod{p}$, користуючись методом, наведеним у доведенні теореми 24.15.

І, нарешті, останній результат цього розділу.

24.18. Теорема (Вільсона). (1) Якщо p — просте число, то $(p-1)! \equiv -1 \pmod{p}$.

(2) Якщо ціле число n не є простим, то $(n-1)! \equiv 0 \pmod{n}$.

Д о в е д е н н я . Якщо $p = 2$, твердження є вірним, оскільки $-1 \equiv -1 \pmod{p}$. Тому далі будемо вважати, що p — непарне просте число. Як і раніше для довільного цілого числа x введемо позначення $x^\wedge = x + p\mathbb{Z}$. З теореми 23.7 отримуємо конгруенцію $a^{p-1} \equiv 1 \pmod{p}$ для довільного числа цілого числа a , взаємно простого з p . Інакше кажучи, $a^\wedge$ є коренем полінома $X^{p-1} - 1^\wedge$. Оскільки $|U(\mathbb{Z}/p\mathbb{Z})| = p-1$, то всі елементи $U(\mathbb{Z}/p\mathbb{Z})$ будуть коренями полінома $X^{p-1} - 1^\wedge$. З пропозиції 17.5 отримуємо тоді рівність

$$X^{p-1} - 1^\wedge = (X - 1^\wedge)(X - 2^\wedge) \dots (X - (p-1)^\wedge).$$

При $X = 0^\wedge$ будемо мати $-1^\wedge = (-1)^{p-1}((p-1)!)^\wedge = (p-1)!^\wedge$. Переходячи тепер на мову конгруенцій, отримаємо, що $(p-1)! \equiv -1 \pmod{p}$.

Розглянемо випадок, коли n не є простим. Очевидно для $n = 4$ твердження є вірним, тому можна вважати, що $n \geq 6$. Якщо n має розклад $n = km$, де $1 < k < m < n$, то k і m будуть множниками в розкладі $(n-1)!$, а тому $(n-1)!$ ділиться на $km = n$, тобто $(n-1)! \equiv 0 \pmod{n}$. У протилежному разі $n = q^2$, де $q \geq 4$. Але тоді $(n-1)!$ містить множники q і $2q$, тобто знову будемо мати $(n-1)! \equiv 0 \pmod{n}$.

ЛІТЕРАТУРА

1. Александров П.С. Введение в теорию групп. — М.: Наука, 1980.
2. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. — М.: Мир, 1987.
3. Бахтурин Ю.А. Тожества в алгебрах Ли. — М.: Наука, 1985.
4. Борович З.И., Шафаревич И.Р. Теория чисел. — М.: Наука, 1964.
5. Бурбаки Н. Алгебра. Алгебраические структуры. Линейная и полилинейная алгебра. — М.: Изд-во физ.-мат. лит., 1962.
6. Бурбаки Н. Алгебра. Многочлены и поля. Упорядоченные группы. — М.: Наука, 1965.
7. Бурбаки Н. Алгебра. Модули, кольца, формы. — М.: Наука, 1966.
8. Бурбаки Н. Коммутативная алгебра. — М.: Мир, 1971.
9. Бурбаки Н. Группы и алгебры Ли. Алгебры Ли, свободные алгебры Ли и группы Ли. — М.: Мир, 1976.
10. Бурбаки Н. Группы и алгебры Ли. Подалгебры Картана, регулярные элементы, расщепляемые полупростые алгебры Ли. — М.: Мир, 1978.
11. Ван дер Варден Б.Л. Алгебра. — М.: Наука, 1976.
12. Виноградов И.М. Основы теории чисел. — М.: Наука, 1972.
13. Вейль Г. Алгебраическая теория чисел. — М.: Изд-во иностр. лит., 1947.
14. Жевлаков К.А., Слинко А.М., Шестаков И.П., Шишов А.И. Кольца, близкие к ассоциативным. — М.: Наука, 1978.
15. Завало С.Т., Левіченко С.С., Пилаєв В.В., Рокицький І.О. Алгебра і теорія чисел. Практикум. — К.: Вища шк., 1983. — Ч. 1.
16. Завало С.Т., Левіченко С.С., Пилаєв В.В., Рокицький І.О. Алгебра і теорія чисел. Практикум. — К.: Вища шк., 1986. — Ч. 2.
17. Зарисский О., Самюэль П. Коммутативная алгебра. — М.: Изд-во иностр. лит., 1963. — Т. 1.
18. Зарисский О., Самюэль П. Коммутативная алгебра. — М.: Изд-во иностр. лит., 1963. — Т. 2.
19. Калужнин Л.А. Введение в общую алгебру. — М.: Наука, 1973.
20. Калужнин Л.А., Вишенский В.А., Шуб Ц.О. Лінійні простори. — К.: Вища шк., 1971.
21. Калужнин Л.А., Суцанский В.И. Преобразования и перестановки. — М.: Наука, 1985.
22. Кострикин А.И. Введение в алгебру. — М.: Наука, 1977.
23. Кострикин А.И. Введение в алгебру. Основы алгебры. — М.: Наука, 1994.
24. Кострикин А.И., Манин Ю.И. Линейная алгебра и геометрия. — М.: Наука, 1986.
25. Курош А.Г. Курс высшей алгебры. — М.: Наука, 1971.
26. Курош А.Г. Лекции по общей алгебре. — М.: Наука, 1973.
27. Курош А.Г. Общая алгебра. — М.: Наука, 1974.
28. Ленг С. Алгебра. — М.: Мир, 1968.
29. Мальцев А.И. Основы линейной алгебры. — М.: Наука, 1970.
30. Проскураков И.В. Сборник задач по линейной алгебре. — М.: Наука, 1967.
31. Сборник задач по алгебре / Под ред. А.И. Кострикина. — М.: Наука, 1987.
32. Серр Ж.-П. Алгебры Ли и группы Ли. — М.: Мир, 1969.
33. Скорняков Л.А. Элементы алгебры. — М.: Наука, 1980.
34. Скорняков Л.А. Элементы общей алгебры. — М.: Наука, 1983.
35. Ольшанский А.Ю. Геометрия определяющих соотношений в группах. — М.: Наука, 1989.

-
36. *Фаддеев Д.К.* Лекции по алгебре. — М.: Наука, 1984.
37. *Фаддеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. — М.: Наука, 1974.
38. *Федорова Ю.Г.* О бесконечных группах, все нетривиальные подгруппы которых имеют конечный индекс // *Успехи мат. наук.* — 1951. — 6, № 1.— С. 187-189.
39. *Черников С.Н.* О проблеме Шмидта // *Укр. мат. журн.*— 1971.— 23, № 5.— С. 598-603.
40. *Шафаревич И.Р.* Основные понятия алгебры. Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления». — М.: ВИНТИ, 1986. — Т. 11.
41. *Bhattacharya J.* Basic abstract algebra. — Cambridge: Cambridge Univ. Press, 1986.
42. *Dedekind R.* Über Gruppen, deren sammtliche Teiler Normalteiler sind // *Math. Annalen.*— 1897. — 48. — S. 548-561.
43. *Garding L, Tambour T.* Algebra for Computer Science. — New York: Springer, 1988.
44. *Kurdachenko L.A., Otal J. and Subbotin I.Ya.* Groups with prescribed quotient groups and associated module theory. — New Jersey: World Scentific, 2002.
45. *Lang S.* Undergraduate Algebra. — Berlin: Springer, 1987.
46. *Robinson D.J.S.* An Introduction to Abstract Algebra. — Berlin: Springer Walter de Gruyter, 2003.
47. *LeVeque W.J.* Topics in Number Theory. — Reading, Mass.: Addison-Wesley, 1956. — Vol. 2.
48. *Wilson J.C.* A principal ideal ring that is not a Euclidean ring. In book "Selected paper on Algebra" The Mathematical Association of America, 1977.
-

На в ч а л ь н е в и д а н н я

КУРДАЧЕНКО Леонід Андрійович

КИРИЧЕНКО Володимир Васильович

СЕМКО Микола Миколайович

ВИБРАНІ РОЗДІЛИ АЛГЕБРИ ТА ТЕОРІЇ ЧИСЕЛ

СУЧАСНА АЛГЕБРА

Посібник

Редактор Л. М. Овсієнко

Художнє оформлення і оригінал-макет Н.М. Мініної, О.О. Канигіної

Підп. до друку 30.08.05 р. Формат 70×108/16.

Ум. друк. арк. 18,2. Обл.-вид. арк. 21,16.

Наклад 100 пр. Зам. № 120.

Інститут математики НАН України. 01601 Київ 4, вул. Терещенківська, 3

Віддруковано у друкарні Інституту математики НАН України.

01601 Київ 4, вул. Терещенківська, 3