

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

В. Андрійчук Б. Забавський

11 червня 2009 р.

ВСТУП

Алгебра належить до основних частин математики і поряд з теорією множин та топологією складає базу, на якій будуються всі інші розділи математики. Всюди там, де ми що-небудь додаємо чи множимо, присутня алгебра. Жодна з будь-яких інших математичних дисциплін неможлива без алгебри.

Предметом вивчення алгебри є множини із заданими на них алгебраїчними операціями, причому конкретна природа цих множин для алгебри не суттєва, отже, по-суті, алгебра вивчає самі алгебраїчні операції, незалежно від того на яких множинах вони можуть бути задані.

В залежності від того, які алгебраїчні операції вивчаються, алгебра ділиться на розділи, такі як теорія груп, теорія кілець, теорія універсальних алгебр та інші. На межі алгебри з іншими розділами математики лежать такі її розділи як топологічна алгебра, диференціальна алгебра, гомологічна алгебра, алгебраїчна топологія, алгебраїчна геометрія і багато інших.

Алгебра знаходить застосування в кожному розділі математики, але особливо великою є її роль в теорії чисел.

Алгебра і теорія чисел мають спільне джерело: вони виникли як науки про розв'язування рівнянь та систем рівнянь з натуральними або додатними раціональними коефіцієнтами та про правила дій над натуральними або дробовими числами.

Письмові пам'ятки, що дійшли до нас, свідчать про те, що деякі з цих правил були відомі ще математикам древнього Єгипту та Вавілону.

В III ст. до н.е. в Началах Евкліда, де було систематизовано всю дотогоди математику, ставиться задача обґрунтування цих правил. Зокрема, Евклід наводить доведення комутативності множення дробів. Книга Начала започаткувала і теорію чисел — як науку про натуральні числа. В цій книзі Евклід вперше запропонував систематичну побудову теорії подільності натуральних чисел на основі відкритого ним алгоритму знаходження найбіль-

шого спільногого дільника, дослідив прості числа і довів теорему про нескінченну кількість простих чисел.

Наступною книгою, яку історики математики вважають етапною в становленні як алгебри так і теорії чисел є Арифметика Діофанта (III ст. н.е.). В Арифметиці, зокрема, були обґрунтовані методи розв'язування в натуральних числах алгебраїчних рівнянь 1-го та 2-го степеня з натуральними коефіцієнтами. Звідси беруть свій початок такі важливі розділи сучасної математики як теорія діофантових рівнянь та діофантових наближень і діофантова геометрія.

Приблизно в цей же час в Китаї, в зв'язку з астрономічними та календарними обчисленнями, виникла задача про знаходження найменшого натурального числа, що має задані остаті при діленні на задані натуральні числа. З точки зору елементарної теорії чисел — це задача про розв'язування системи лінійних конгруенцій. Результат про розв'язок цієї задачі та його узагальнення називають тепер китайською теоремою про лишки.

Сам термін алгебра походить з назви книги Мухаммеда аль-Хорезмі Альджебр аль-мукабала (IX ст.), яка була присвячена алгебрі та геометрії. В алгебраїчній частині цієї книги подаються правила дій над алгебраїчними величинами, а також розглядаються рівняння першого і другого степеня.

Незважаючи на те, що ще Діофант запровадив буквенні позначення для невідомих, арифметичні дії над різними величинами на протязі багатьох століть описувалися словесно. Лише в кінці XV ст. з'явилися знаки “+”, та “-”, а в кінці XVI ст. Вієт запровадив буквенні позначення як для невідомих так і для коефіцієнтів рівнянь. Основи алгебраїчної символіки склалися лише в середині XVII століття, починаючи з Р. Декарта (1596 – 1650) алгебраїчні записи майже не відрізняються від сучасних.

У XVI столітті алгебра отримує потужний імпульс для розвитку в зв'язку з відкриттям італійськими математиками Н. Тарталья (1500–1557) та Д. Кардано (1501–1576) формул для розв'язків алгебраїчних рівнянь 3-го та 4-го степеня. В цей час, і далі на протязі XVII та XVIII століття, предметом алгебри є правила

обчислень та тотожних перетворень буквенных виразів і розв'язування алгебраїчних рівнянь.

У XVII столітті Р. Декарт створює аналітичну геометрію, у якій геометричні об'єкти описуються алгебраїчними рівняннями. Це настільки зблизило алгебру і геометрію, що стало можливим розглядати геометрію як частину алгебри. На цей час припадає діяльність французького математика П. Ферма (1601–1665), творчість якого сприяла відновленню інтересу до теорії чисел. П. Ферма, зокрема, довів теорему про те, що якщо p — просте число, то $a^p - a$ ділиться на p для кожного цілого числа a (мала теорема Ферма), довів, що кожне просте число вигляду $4k + 1$ є сумою двох квадратів і сформулював так звану “велику теорему Ферма” про те, що рівняння $x^n + y^n = z^n$ не має розв'язків в натуральних числах, якщо $n > 2$. Спроби довести цю теорему дуже сприяли розвиткові теорії чисел і привели потім до виникнення алгебраїчної теорії чисел. Дуже багато для розвитку теорії чисел зробив Л. Ойлер (1707–1783). Серед наукових праць Ойлера більше, ніж 140 присвячені теорії чисел. Зокрема, Ойлер використовував в теорії чисел методи математичного аналізу і започаткував ще один важливий розділ теорії чисел — аналітичну теорію чисел.

На початку XIX століття К.Ф. Гаус (1777–1855) дає доведення основної теореми алгебри про існування коренів многочленів з комплексними коефіцієнтами. Крім того, у 1801 р. Гаус видає великий твір під назвою “Арифметичні дослідження” присвячений питанням алгебри та теорії чисел. У цьому творі, серед іншого, Гаусом була завершена побудова теорії конгруенцій, доведений квадратичний закон взаємності, досліджені, так звані, гаусові суми та зображення чисел квадратичними формами. Діяльністю Гауса був підведений підсумок попереднього розвитку алгебри і теорії чисел і визначений дальший розвиток цих дисциплін.

У першій половині XIX століття дослідження коренів многочленів залишається основною проблемою алгебри. У 1824 році Н.Х. Абелль (1802–1829) довів, що загальне алгебраїчне рівняння степеня n нерозв'язне в радикалах, а у 1830 році Е. Галуа

(1811–1832) одержав критерій розв'язності конкретних рівнянь. В цей же час виникає поняття групи, вивчаються матриці та визначники. У другій половині XIX століття була створена алгебра логіки (Дж. Буль (1815–1864)), відкриті кватерніони та гіперкомплексні числа (У. Гамільтон (1805–1865), А. Келі (1821–1895)). В теорії чисел інтенсивно розвивається як алгебраїчна теорія чисел (Е. Куммер (1810–1894), Л. Кронекер (1823–1891), Р. Дедекінд (1831–1916)) так і аналітична теорія чисел (П. Діріхле (1805–1859), Г. Ріман (1826–1866), П. Чебишев (1821–1894)).

Сучасна точка зору на алгебру як на науку про алгебраїчні операції сформулювалася на початку ХХ століття під впливом ідей і робіт Д. Гільберта (1862–1943), Е. Штейніца (1871–1928), Е. Артіна (1898–1962), Е. Нетер (1882–1935). Ця точка зору стала загальноприйнятою після виходу у 1931 році монографії Б.Л. ван дер Вардена “Сучасна алгебра”.

У ХХ столітті алгебраїчні поняття і методи все ширше використовуються у всіх галузях математики; появився, навіть, термін “алгебраїзація математики”. З другого боку, багато абстрактних алгебраїчних понять (групи та зображення груп, некомутативні алгебри, скінченні поля, формальні степеневі ряди, лінійні простори та інші) знаходять широкі застосування в квантовій механіці, в конструюванні обчислювальної техніки, в кристалографії, в математичній економіці, в теорії кодування та передачі інформації та в інших галузях людської діяльності.

Теорія чисел теж широко використовується в практичній діяльності, незважаючи на те, що відомий математик Г. Харді у 1940 році написав “Гаус, як і інші математики, мав рацію, коли він казав, що існує лише одна наука (теорія чисел), яка така далека від людської діяльності, що завжди залишається чистою”. Харді помилувся, тепер теорію чисел широко використовують, наприклад, в питаннях зв'язаних з передачею та кодуванням інформації.

Основу цієї книги складають курси лекцій, що на протязі ряду років читалися авторами у першому семестрі на механіко-математичному факультеті та на факультеті прикладної мате-

матики Львівського університету ім. І. Франка.

Автори ризикнули почати виклад з розгляду абстрактних алгебраїчних операцій. В зв'язку з цим, матриці, системи лінійних рівнянь та векторні простори в розділах 2, 3, і 4 розглядаються над довільним полем P , а не над полем дійсних чисел.

Читачеві, якому психологічно важко прийняти відразу цей рівень абстракції, ми рекомендуємо при першому читанні вважати, що термін “поле P ” означає — “поле дійсних чисел \mathbb{R} ”, а термін “ a — елемент поля P ” означає “ a — дійсне число”. Лектор теж може організувати виклад матеріалу, наприклад, у такій послідовності: матриці з дійсними елементами та дії над ними, метод Гауса розв'язування систем лінійних рівнянь з дійсними коефіцієнтами, числовий n -вимірний векторний простір, визначники n -го порядку матриць з дійсними коефіцієнтами, поняття алгебраїчної операції, початкова інформація про групи, кільця та поля, поле комплексних чисел, многочлени над полем, евклідові кільця, факторіальні кільця, кільце класів лишків.

Кожний розділ книги завершується вправами, переважна більшість яких запозичена з різних джерел. Деякі вправи присвячені висвітленню матеріалу, для якого не вистачило місця в основному тексті і для якого лектору не вистачає часу для прочитання його студентам і він залишає цей матеріал на самостійне опрацювання. Наприклад, автори внесли у вправи розклад раціональних функцій на прості дроби, теорему Штурма та теорему про симетричні многочлени. Всі такі вправи супроводжуються вказівками або посиланнями на літературу.

Автори вдячні О. Романіву і А. Телейку за набір рукопису на комп’ютері та терпіння при внесенні в цей набір великої кількості правок.

Розділ 1

Основні алгебраїчні структури

Поняття алгебраїчної операції є основним в алгебрі. Часто на запитання “Що таке алгебра?” відповідають, що це наука про алгебраїчні операції. Основними об’єктами, що вивчаються в алгебрі, є групи, кільця, поля, модулі та інші алгебраїчні структури. Всі ці об’єкти є множинами із заданими на них алгебраїчними операціями. Саме поняття алгебраїчної операції виникло як узагальнення відомих з давнини звичайних операцій множення та додавання (натуральних, додатних раціональних, цілих та раціональних) чисел. Звичайно, у математиці додають та множать не тільки числа. При вивченні математики в середній школі доводиться, наприклад, додавати вектори, додавати та множити многочлени або функції, знаходити композицію двох рухів площини (два рухи, виконані послідовно, дають знову рух) і т.п..

1.1. Множини та відношення

Ми приймаємо точку зору, згідно якої поняття множини є первинним. Під множиною розуміють сукупність деяких об’єктів, які називають елементами. Немає чіткої різниці між елементами та множинами; елементи можуть бути множинами, а множини – елементами. Той факт, що об’єкт a є елементом множини A записують у вигляді $a \in A$. Запис $a \in A$ можна читати і по іншому: “елемент a належить множині A ”. Якщо об’єкт a не належить множині A , то пишуть $a \notin A$. Множину B називають

підмножиною множини A , і пишуть $B \subset A$, якщо кожен елемент множини B є елементом множини A . Дві множини A і B називають рівними, і пишуть $A = B$, якщо ці множини складаються з одних і тих же елементів. Зрозуміло, що $A = B$ тоді й лише тоді, коли $A \subset B$ і $B \subset A$. Зручно вважати, що існує множина, яка не містить жодного елемента. Таку множину називають порожньою і позначають \emptyset . Порожня множина \emptyset є підмножиною кожної множини.

Для деяких важливих множин існують спеціальні позначення. Зокрема, буквами $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ прийнято позначати, відповідно, множини натуральних, цілих, раціональних та дійсних чисел.

Нехай A – деяка множина. Множину B – всіх елементів множини A , які мають деяку властивість P , записують у вигляді

$$B = \{x \in A \mid P(x)\}.$$

У багатьох випадках множину задають переліком елементів, з яких вона складається. Наприклад, $C = \{2, 3, 5, 7\}$ – множина, що складається з чотирьох елементів 2, 3, 5, 7, а

$$\mathbb{N} = \{0, 1, 2, 3, \dots, n, \dots\}$$

– множина всіх натуральних чисел.

Для скорочення записів далі часто використовуються такі вирази:

$\forall x \in A$ означає “для кожного елемента x множини A ”;

$\exists x \in A$ означає “існує елемент x множини A ”;

$P \rightarrow Q$ означає “з властивості P випливає властивість Q ”;

$P \leftrightarrow Q$ означає “властивість P виконується тоді й лише тоді, коли виконується властивість Q ”;

\wedge означає “і”;

\vee означає “або”;

1.1.1. Означення та приклади відношень

Означення 1.1.1. *Бінарним відношенням R між множинами A і B називається підмножина R декартового добутку $A \times B$.*

[htb]

У випадку, коли $A_1 = \dots = A_n = A$, кажуть про n -місне відношення на множині A .

Наведемо декілька прикладів бінарних відношень:

Приклад 1.1.1. 1) $\{(0, 1), (0, 3), (1, 2)\} \subset \{0, 1, 5\} \times \{1, 2, 3\}$.
 $\{(0, 1), (0, 3), (1, 2)\}$ – бінарне відношення між множинами $\{0, 1, 5\}$
 $i \{1, 2, 3\}$.

2) Будь-яка підмножина множини \mathbb{R}^2 є бінарним відношенням на множині дійсних чисел. На мал. 1.1.1 зображене декілька таких відношень

Puc. 1.1.1

Нехай $R \subset A \times B$ – бінарне відношення. Тоді обернене відношення R^{-1} є наступною підмножиною декартового добутку $B \times A$:

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

Для бінарного відношення R пишуть aRb замість $(a, b) \in R$.

1.1.2. Відношення еквівалентності

Означення 1.1.2. Відношення R на множині A називається *відношенням еквівалентності*, якщо воно має наступні властивості:

- 1) $\forall a \in A \quad (a, a) \in R$ (рефлексивність);
- 2) $\forall a, b \in A \quad (a, b) \in R \rightarrow (b, a) \in R$ (симетричність);
- 3) $\forall a, b, c \in A \quad (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$ (транзитивність).

Відношення еквівалентності є одним з дуже важливих відношень у математиці. Наведемо декілька прикладів відношень еквівалентності:

Приклад 1.1.2. 1) Нехай A — довільна множина. Приймемо $(x, y) \in R$, якщо $x = y$. Легко переконатися у тому, що відношення $x = y$ є рефлексивним, симетричним і транзитивним. Отже, рівність є відношенням еквівалентності. Тому еквівалентність можна вважати узагальненням рівності.

2) Нехай M — множина всіх опуклих многокутників на площині. Для $x, y \in M$ розглянемо наступні 5 відношень:

- a) xR_1y тоді і тільки тоді, коли многокутники x та y конгруентні;
- б) xR_2y тоді і тільки тоді, коли многокутники x та y мають однакову площину;
- в) xR_3y тоді і тільки тоді, коли x та y мають однакові периметри;
- г) xR_4y тоді і тільки тоді, коли вони мають однакові кількості сторін;
- д) xR_5y тоді і тільки тоді, коли x та y подібні.

Всі відношення R_1, \dots, R_5 є відношеннями еквівалентності. Зауважимо, що $R_5 \subset R_4$.

3) \mathbb{N} — множина натуральних чисел, $R \subset \mathbb{N}^2$

$$R = \{(m, n) \in \mathbb{N}^2 \mid m \text{ ділиться на } n\}.$$

Відношення R не симетричне, тому воно не є відношенням еквівалентності.

Відношення еквівалентності на множині A часто позначають символом \sim , тобто замість $(a, b) \in R$ пишуть $a \sim_R b$ або $a \sim b$.

1.1.3. Розбиття та відношення еквівалентності

Означення 1.1.3. Якщо множина A є об'єднанням скінченної або нескінченної родини множин $\{A_i\}_{i \in I}$, причому $A_i \cap A_j = \emptyset$ для $i \neq j$, то кажуть, що задане *розділення* множини A .

Наведемо декілька прикладів розбиттів.

1) Нехай \mathbb{Z} — множина цілих чисел, $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$ — множина парних чисел. Тоді $2\mathbb{Z} \cup (\mathbb{Z} \setminus 2\mathbb{Z})$ — розбиття множини \mathbb{Z} . Об'єднання

$$\{0\} \cup \{1, -1\} \cup \{2, -2\} \cup \dots \cup \{n, -n\} \cup \dots$$

є також розбиттям множини \mathbb{Z} .

2) \mathbb{R} — множина дійсних чисел. $A_i = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = i^2\}$, де $i \in \mathbb{R}$, $i \geq 0$. Тоді $\mathbb{R}^2 = \bigcup_{i \in \mathbb{R}, i \geq 0} A_i$ — розбиття множини \mathbb{R}^2 (див. мал. ??).

Означення 1.1.4. Нехай R — відношення еквівалентності на множині A і $a \in A$. Множина $\bar{a} = \{b \in A \mid b \sim_R a\}$ називається *суміжним класом* з представником a .

1) Назовемо два цілих числа x і y еквівалентними, якщо $x - y$ ділиться на 5. Суміжний клас з представником -12 є наступною множиною цілих чисел:

$$\overline{-12} = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} = \{3 + 5k \mid k \in \mathbb{Z}\}.$$

2) Нехай M — множина точок площини. Для $P, Q \in M$ скажемо, що $P \sim Q$, якщо відрізки OP та OQ рівні, де O — фіксована точка площини. Легко переконатися, що в такий спосіб ми одержуємо відношення еквівалентності на множині всіх точок площини. На мал. ?? зображені три суміжні класи A_0, A_1 і $A_{\sqrt{2}}$ з представниками, відповідно, O, A і B .

Теорема 1.1.1 (критерій рівності суміжних класів). *Два суміжні класи \bar{a}_1 і \bar{a}_2 збігаються тоді й лише тоді, коли їх представники еквівалентні:*

$$\bar{a} = \bar{a}_1 \iff a \sim a_1.$$

Доведення. Імплікація $\bar{a} = \bar{a}_1 \Rightarrow a \sim a_1$ очевидно випливає з означень. Доведемо обернену імплікацію. Нехай $b \in \bar{a}$. Тоді $b \sim a$. Але $a \sim a_1$. Тому за транзитивністю відношення \sim маємо $b \sim a_1$. Отже, $b \in \bar{a}_1$, і ми довели, що $\bar{a} \subset \bar{a}_1$. Так само доводиться і протилежне включення $\bar{a}_1 \subset \bar{a}$. Отже, $\bar{a} = \bar{a}_1$. \square

Теорема 1.1.2. *Кожне розбиття $A = \bigcap_{i \in I} A_i$ множини A визначає відношення еквівалентності на цій множині: $a \sim b$, якщо існує $i \in I$ для якого $a, b \in A_i$. Навпаки, якщо на множині A задане відношення еквівалентності, то воно визначає розбиття множини A , елементами якого є суміжні класи. Зокрема, різні суміжні класи не перетинаються.*

Доведення. Якщо $A = \bigcup_{i \in \mathcal{I}} A_i$ — розбиття і $a, b \in A$, то скажемо, що $a \sim b$, якщо існує $i \in \mathcal{I}$ таке, що $a \in A_i$ і $b \in B_i$. Легко перевірити, що так означене відношення є відношенням еквівалентності. Навпаки, нехай на множині A задане відношення еквівалентності \sim . Розглянемо множину всіх суміжних класів. Ясно, що кожний елемент a множини A міститься у суміжному класі \bar{a} . Тому $A = \bigcup_{a \in A} \bar{a}$. Але об'єднання $\bigcup_{a \in A} \bar{a}$, взагалі кажучи, не є розбиттям, тому що для різних $a, a' \in A$ ми можемо мати $\bar{a} = \bar{a}'$. Щоб одержати розбиття, розглянемо множину всіх різних суміжних класів і в кожному з них виберемо по представнику (тут ми використовуємо аксіому вибору). Нехай C — множина представників всіх різних суміжних класів, тобто така підмножина множини A , що для різних $a, b \in C$ маємо $\bar{a} \neq \bar{b}$ і для кожного суміжного класу \bar{a} знайдеться $c \in C$, для якого $\bar{c} = \bar{a}$.

Переконаємося у тому, що $\bigcup_{a \in C} \bar{a}$ є розбиттям множини A . Для цього досить показати, що коли $a, b \in C$ і $a \neq b$, то $\bar{a} \cap \bar{b} = \emptyset$. Справді, якби існував елемент $d \in \bar{a} \cap \bar{b}$, то $d \sim a$ і $d \sim b$, тому $a \sim b$ і за критерієм рівності суміжних класів $\bar{a} = \bar{b}$. Одержані суперечність з вибором множини C . Тому $\bigcup_{a \in C} \bar{a}$ є розбиттям множини A . \square

Наслідок 1.1.3. *Якщо два суміжні класи мають спільний елемент, то вони збігаються: $\bar{a} \cap \bar{b} \neq \emptyset \Rightarrow \bar{a} = \bar{b}$.*

Означення 1.1.5. Якщо на множині A задане відношення еквівалентності E , то множина всіх суміжних класів для цього відношення еквівалентності називається *фактор-множиною* множини A відносно E і позначається A/E .

1.1.4. Функціональні відношення та відображення

Означення 1.1.6. Відношення $R_f \in A \times B$ називається функціональним відношенням між множинами A і B , якщо R_f задовольняє таку умову:

$$(x, y_1) \in R_f \wedge (x, y_2) \in R_f \implies y_1 = y_2, \text{ де } x \in A, y_1, y_2 \in B. \quad (1.1.1)$$

Якщо $R_f \subset A \times B$ — функціональне відношення, то пишуть $y = f(x)$ замість $(x, y) \in R_f$ і кажуть, що задана функція f з множини A у множину B . Отже, за означенням, поняття функціонального відношення R_f та поняття функції є просто різні назви однієї і тієї ж множини $R_f \subset A \times B$, що задовольняє умові (1.1.1).

Означення 1.1.7. Множину

$$D(f) = \{x \in A \mid \exists y \in B, y = f(x)\}$$

називають *областю визначення функції* f , а множину

$$\text{Im}f = \{y \in B \mid \exists x \in A, y = f(x)\}$$

називають *областю значень* цієї функції. Якщо $y = f(x)$, то y називають *образом* елемента x , а x — *прообразом* елемента y . Множина $f^{-1}(y) = \{x \in A \mid f(x) = y\}$ називається *повним прообразом* елемента y .

Приклад 1.1.3. Наприклад, множина $\{(x, \sin x) \mid x \in \mathbb{R}\}$ є функціональним відношенням на множині \mathbb{R} . Відповідною цівому відношенню функцією є $f(x) = \sin x$. Повний прообраз дійсного числа 0 для цієї функції — це множина $\{\pi k \mid k \in \mathbb{Z}\}$, а

повним прообразом числа -3 є порожня множина. Множина $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ не є функціональним відношенням, тому що, наприклад, обидві пари $(0, 1)$ і $(0, -1)$ належать цій множині, отже, умова (1.1.1) не виконується.

Означення 1.1.8. Функція f з множини A у множину B називається *відображенням* з A в B , якщо $D(f) = A$. Відображення f з множини A в множину B позначають

$$f: A \rightarrow B.$$

Означення 1.1.9. Відображення $f: A \rightarrow B$ називається:

- 1) *ін'єктивним*, якщо для всіх $x_1, x_2 \in A$ з $f(x_1) = f(x_2)$ випливає $x_1 = x_2$;
- 2) *сюр'єктивним*, якщо $\text{Im } f = B$;
- 3) *біективним*, якщо воно ін'єктивне і сюр'єктивне.

1) Функція f з множини \mathbb{R} в \mathbb{R} , для якої $f(x) = x^{-1}$, не є відображенням, оскільки $D(f) \neq \mathbb{R}$. Ця функція є відображенням з множини $\mathbb{R} \setminus \{0\}$ у множину $\mathbb{R} \setminus \{0\}$. Це останнє відображення біективне.

2) Відображення $f: \mathbb{N} \rightarrow \mathbb{N}$, для якого $f(n) = n^3 + 1$, є ін'єктивним, але не є сюр'єктивним.

3) Відображення $f: \mathbb{R} \rightarrow \mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$, $f(x) = x^2$ є сюр'єктивним, але не є ін'єктивним.

1.1.5. Добуток відображень

Означення 1.1.10. *Добутком відображень* $f: A \rightarrow B$ і $g: B \rightarrow C$ називається відображення $g \circ f: A \rightarrow C$, для якого $(g \circ f)(x) = g(f(x))$.

Теорема 1.1.4. *Нехай $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$ – три відображення. Тоді*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Інакше кажучи, множення відображень асоціативне.

Доведення. Потрібно довести, що $\forall x \in A (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$. Маємо:

$$(h \circ (g \circ f))(x) = h((g \circ f))(x) = h((gf(x))),$$

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h((gf(x))).$$

Порівнюючи ці рівності, бачимо, що теорему доведено. \square

Завдання 1.1.1. У випадку, коли визначені обидва добутки $g \circ f$ і $f \circ g$ відображені f і g , не можна стверджувати, що $g \circ f = f \circ g$, тобто множення відображень, взагалі кажучи, не комутативне. Щоб переконатися у цьому, розглянемо відображення $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x + 1$ і $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = 2x$. Тоді

$$(g \circ f)(x) = g(x + 1) = 2x + 2,$$

$$(f \circ g)(x) = f(2x) = 2x + 1.$$

Тому $g \circ f \neq f \circ g$.

Теорема 1.1.5. 1) Добуток двох ін'єктивних відображень є ін'єктивним відображенням.

2) Добуток двох сюр'єктивних відображень є сюр'єктивним відображенням.

3) Добуток двох біективних відображень – біективне відображення.

Доведення. 1) Нехай $f: A \rightarrow B$, $g: B \rightarrow C$ – ін'єктивні відображення. Тоді, якщо $(g \circ f)(x_1) = (g \circ f)(x_2)$ для $x_1, x_2 \in A$, то $g(f(x_1)) = g(f(x_2))$. Звідси, за ін'єктивністю відображення g , одержуємо $f(x_1) = f(x_2)$, і, отже, $x_1 = x_2$, тому що f ін'єктивне. Це означає, що відображення $g \circ f$ ін'єктивне.

2) Нехай $f: A \rightarrow B$, і $g: B \rightarrow C$ – сюр'єктивні. Покажемо, що для кожного $z \in C$ знайдеться $x \in A$, що $(g \circ f)(x) = z$. Перш за все, знайдеться елемент $y \in B$ такий, що $g(y) = z$. Це випливає з сюр'єктивності відображення g . Тоді, за сюр'єктивністю відображення f , для цього y знайдеться $x \in A$, що $f(x) = y$. В результаті $g(f(x)) = z$, тобто $(g \circ f)(x) = z$ і добуток $g \circ f$ сюр'єктивний.

3) Твердження про бієктивність випливає з уже доведених перших двох частин теореми. \square

1.1.6. Однічне та обернене відображення

Означення 1.1.11. Відображення $i: A \rightarrow A$ називається *однічним відображенням* множини A , якщо $i(x) = x$ для кожного елемента $x \in A$. Однічне відображення множини A позначають 1_A .

Означення 1.1.12. Відображення $g: B \rightarrow A$ називається *оберненим відображенням* до відображення $f: A \rightarrow B$, якщо

$$g \circ f = 1_A \text{ i } f \circ g = 1_B.$$

Якщо g — відображення обернене до f , то пишуть f^{-1} замість g .

1) Нехай $f: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$, $f(x) = \frac{1}{x}$. Тоді $f^{-1} = f$ тому, що $(f \circ f)(x) = f(\frac{1}{x}) = (x^{-1})^{-1}$. Це означає, що $f \circ f = 1_{\mathbb{R} \setminus \{0\}}$ і обидві умови з другого означення виконуються.

2) Нехай $A = (\frac{\pi}{2}, \frac{\pi}{2})$, $B = \mathbb{R}$. Відображення $f: (\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$, $f(x) = \operatorname{tg} x$ і $g: \mathbb{R} \rightarrow (\frac{\pi}{2}, \frac{\pi}{2})$, $g(x) = \operatorname{arctg} x$ є взаємно обернені.

Теорема 1.1.6. Для відображення $f: A \rightarrow B$ існує обернене відображення тоді і тільки тоді, коли f бієктивне.

Доведення. \Rightarrow . Нехай $g: B \rightarrow A$ обернене відображення до f . Покажемо, що f — бієктивне. Якщо $f(x_1) = f(x_2)$, то і $g(f(x_1)) = g(f(x_2))$, тобто $(g \circ f)(x_1) = (g \circ f)(x_2)$ або $x_1 = x_2$, оскільки $g \circ f = 1_A$. Це означає, що f — ін'єктивне. Далі, ми маємо $f \circ g = 1_B$. Це означає, що для кожного $y \in B$ $(f \circ g)(y) = y$ або $f(g(y)) = y$. Елемент $x = g(y)$ і є прообразом елемента y для відображення f , тобто f — сюр'єктивне.

\Leftarrow . Нехай f — бієктивне. Побудуємо за відображенням f відображення $g: B \rightarrow A$, означивши

$$g(y) = x \Leftrightarrow f(x) = y. \quad (1.1.2)$$

Перевіримо, що одержиться відображення. Нехай

$$R_g = \{(y, x) \in B \times A \mid g(y) = x\} = \{(y, x) \in B \times A \mid f(x) = y\}.$$

Якщо $(y, x_1) \in R_g$ і $(y, x_2) \in R_g$, то $f(x_1) = f(x_2) = y$, отже, $x_1 = x_2$ тому, що f ін'єктивне відображення. Це означає, що R_g — функціональне відношення. Знайдемо область визначення $\mathcal{D}(g)$ функції g . $\mathcal{D}(g) = \{y \in B \mid \exists x \in A, g(y) = x\} = \{y \in B \mid \exists x \in A, f(x) = y\} = B$ тому, що f сюр'єктивне відображення. Ми довели, що відповідність g , визначена за правилом (1.1.2), є відображенням. Покажемо, що $g = f^{-1}$. Беручи до уваги (1.1.2), маємо для $x \in A, y \in B$:

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g(y) = x, \\ (f \circ g)(y) &= f(g(y)) = f(x) = y. \end{aligned}$$

Це означає, що $g \circ f = 1_A$ і $f \circ g = 1_B$, що і потрібно було довести. \square

1.2. Алгебраїчна операція

1.2.1. Означення та приклади алгебраїчних операцій

Означення 1.2.1. *Бінарною алгебраїчною операцією* на множині G називається відображення $\circ: G \times G \rightarrow G$ з декартового добутку $G \times G$ в G . Якщо $(x, y) \in G \times G$, то образ $\circ((x, y))$ пари (x, y) називають *композицією* (добутком чи, в деяких випадках, сумою) елементів x і y , і позначають $x \circ y$ (або xy , $x + y$; використовують й інші позначення, наприклад, $x * y$, $x \ominus y$, $x \otimes y$ і т.п.).

Приклад 1.2.1. 1) Додавання та множення на множинах натуральних чисел \mathbb{N} , цілих чисел \mathbb{Z} , раціональних чисел \mathbb{Q} та дійсних чисел \mathbb{R} є алгебраїчними операціями на цих множинах.

2) Віднімання є алгебраїчною операцією на множині \mathbb{Z} , але не є алгебраїчною операцією на множині \mathbb{N} ($3 - 5 \notin \mathbb{N}$). Ділення

не є алгебраїчною операцією на множині дійсних чисел, але є алгебраїчною операцією на множині ненульових дійсних чисел (поясніть, чому?).

3) Об'єднання та перетин підмножин множини X є алгебраїчними операціями на множині 2^X – всіх підмножин множини X .

4) Нехай A – будь-яка непорожня множина. Позначимо через $\text{End}A$ множину всіх відображенень множини A в себе. Тоді для кожної спорядкованої пари відображень $f, g \in \text{End}A$ визначений їх добуток $g \circ f: A \rightarrow A$, $(g \circ f)(x) = g(f(x))$ для $x \in A$. Множення відображень є алгебраїчною операцією на множині $M = \text{End}A$.

1.2.2. Асоціативність. Напівгрупа та моноїд

Означення 1.2.2. Алгебраїчна операція \circ на множині G називається асоціативною, якщо $(x \circ y) \circ z = x \circ (y \circ z)$ для всіх елементів $x, y, z \in G$.

Приклад 1.2.2. 1) Додавання і множення на множинах $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ є асоціативними алгебраїчними операціями. Перевірте, що правило $a * b = a + b - ab$ задає асоціативну алгебраїчну операцію на кожній з множин \mathbb{Z}, \mathbb{Q} , і \mathbb{R} .

2) Віднімання є неасоціативною алгебраїчною операцією на кожній з множин \mathbb{Z}, \mathbb{Q} , і \mathbb{R} (наприклад, $(1 - 2) - 3 \neq 1 - (2 - 3)$). Перевірте, що правило $a * b = a^b$ задає неасоціативну алгебраїчну операцію на множині \mathbb{R}_+ додатних дійсних чисел.

3) Об'єднання та перетин множин є асоціативними алгебраїчними операціями на множині 2^X всіх підмножин множини X . Перевірте, що правило $A \oplus B = (A \cup B) \setminus (A \cap B)$ теж задає асоціативну операцію на множині 2^X .

4) Відомо, що множення відображень асоціативне. Тому множення відображень є асоціативною операцією на множині $V = \text{End}A$ всіх відображень множини A в себе.

Означення 1.2.3. Елемент $e \in G$ називається *нейтральним* відносно алгебраїчної операції \circ на множині G , якщо $e \circ x = x \circ e = x$ для всіх елементів $x \in G$.

Приклад 1.2.3. 1) Число 0 є нейтральним елементом для алгебраїчної операції додавання на множинах $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, і \mathbb{R} , а число 1 є нейтральним елементом відносно звичайного множення на цих множинах.

2) Порожня множина \emptyset є нейтральним елементом для алгебраїчної операції об'єднання підмножин на множині 2^X , а вся множина X є нейтральним елементом для алгебраїчної операції перетину підмножин.

3) Однічне відображення 1_A множини A є нейтральним елементом для операції добутку відображень множини $M = \text{End}A$.

Зауваження 1.2.1. Якщо нейтральний елемент для алгебраїчної операції \circ існує, то він єдиний. Справді, якщо e_1 та e_2 два нейтральні елементи, то з означення 1.2.3 випливає, що $e_1 = e_1 \circ e_2 = e_2$.

Позначення. Множину G із заданою на ній алгебраїчною операцією \circ будемо позначати (G, \circ) . Нас може цікавити декілька алгебраїчних операцій \circ_1, \dots, \circ_n на множині G . У цьому випадку будемо писати $(G, \circ_1, \dots, \circ_n)$. Так, запис $(\mathbb{Z}, +, \cdot)$ означає, що розглядається множина \mathbb{Z} разом з алгебраїчними операціями додавання і множення, а запис (\mathbb{R}_+, \cdot) означає, що розглядається множина додатних чисел \mathbb{R}_+ разом з алгебраїчною операцією множення. Для скорочення записів часто пишуть xy замість $x \circ y$.

Означення 1.2.4. Множина (G, \circ) називається *напівгрупою*, якщо алгебраїчна операція \circ є асоціативною. Якщо для алгебраїчної операції \circ існує нейтральний елемент, то напівгрупа (G, \circ) називається *моноїдом*.

Приклад 1.2.4. 1) Всі множини з прикладів 1, 2 і 3 після означення 1.2.3 є моноїдами відносно вказаних у цих прикладах алгебраїчних операцій на цих множинах.

2) Множина $2\mathbb{Z}$ парних цілих чисел є моноїдом відносно алгебраїчної операції додавання і не є моноїдом, а лише напівгрупою, відносно алгебраїчної операції множення.

Нехай (G, \circ) — моноїд, $x_1, x_2, \dots, x_n \in G$. Визначимо добуток елементів x_1, x_2, \dots, x_n за правилом

$$\prod_{i=1}^n x_1 x_2 \dots x_n = (x_1 x_2 \dots x_{n-1}) x_n. \quad (1.2.1)$$

Властивість асоціативності алгебраїчної операції дозволяє розставляти дужки в добутку (1.2.1) будь-яким способом. Наприклад,

$$x_1 x_2 x_3 x_4 = x_1 ((x_2 x_3) x_4) = (x_1 x_2) (x_3 x_4).$$

1.2.3. Обернений елемент.Група

Нехай (G, \cdot) — множина з алгебраїчною операцією. Припустимо, що в множині G існує для цієї операції нейтральний елемент e .

Означення 1.2.5. Елемент $b \in G$ називається правим (лівим) оберненим до елемента $a \in G$, якщо $ab = e$ ($ba = e$).

Приклад 1.2.5. 1) Нехай $f \in \text{End}\mathbb{N}$, $f(n) = 2n$, $g_1, g_2 \in \text{End}\mathbb{N}$,

$$g_1(n) = \begin{cases} \frac{n}{2} & n \text{ — парне}, \\ 1 & n \text{ — непарне}, \end{cases} \quad g_2(n) = \begin{cases} \frac{n}{2} & n \text{ — парне}, \\ 2 & n \text{ — непарне}. \end{cases}$$

Тоді $g_1 \circ f = g_2 \circ f = 1_{\mathbb{N}}$, тобто g_1 і g_2 є лівими оберненими до f . Легко зрозуміти, що тут існує безліч лівих обернених до f . В той же час не існує жодного правого оберненого до f . Спробуйте довести це самостійно.

2) Більш загально, виявляється, що відображення $f \in \text{End}A$, де A будь-яка непорожня множина, має обернене зліва (справа) тоді і тільки тоді, коли воно ін'єктивне (сюр'єктивне). Переконайтесь в цьому самостійно.

Означення 1.2.6. Елемент $b \in G$ називається *оберненим* до елемента $a \in G$, якщо $ba = ab = e$. Елемент $a \in G$, для якого існує обернений, називається *оборотним*. Обернений до a елемент позначають a^{-1} (або $-a$, якщо операцію в G позначають $+$).

Твердження 1.2.1. *Нехай (G, \cdot) – моноїд. Якщо для елемента $a \in G$ існують лівий і правий обернені, то вони збігаються. Для кожного елемента існує не більше одного оберненого.*

Доведення. Нехай b і c , відповідно, лівий і правий обернені до a . Тоді, використовуючи асоціативність, маємо:

$$c = (ba)c = b(ac) = b.$$

Цей же ланцюжок рівностей показує і єдиність оберненого елемента. \square

Нехай a довільний оборотний елемент моноїда G , тобто елемент, який має обернений $a^{-1} \in G$. Позначимо для $k \in \mathbb{Z}$

$$a^k = \begin{cases} \underbrace{a \cdots a}_k, & \text{якщо } k > 0, \\ e, & \text{якщо } k = 0, \\ (a^{-1})^{|k|}, & \text{якщо } k < 0. \end{cases}$$

Елемент a^k назовемо *k-им степенем* елемента a групи G .

Твердження 1.2.2. *Нехай a оборотний елемент моноїда G . Тоді для всіх $m, n \in \mathbb{Z}$ вірні такі рівності*

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

Доведення. Якщо $m, n \in \mathbb{N}$, то все очевидно. Якщо $m < 0, n < 0$, то $a^m a^n = (a^{-1})^{|m|} (a^{-1})^{|n|} = (a^{-1})^{|m|+|n|} = (a^{-1})^{|m+n|} = a^{m+n}$. Якщо $m < 0, n > 0$, то

$$\begin{aligned} a^m a^n &= (a^{-1})^{|m|} a^n = \underbrace{a^{-1} \cdots a^{-1}}_{|m| \text{ разів}} \cdot \underbrace{a \cdots a}_n \\ &= \begin{cases} a^{n-|m|}, & \text{якщо } n \geq |m|, \\ (a^{-1})^{|m|-n}, & \text{якщо } n < |m|. \end{cases} = a^{m+n}. \quad (1.2.2) \end{aligned}$$

Аналогічно розглядаються інші випадки. \square

Зауваження 1.2.2. Якщо алгебраїчна операція в G позначається $+$, то рівності твердження 1.2.2 набувають вигляду

$$ma + na = (m + n)a, \quad n(ma) = (nm)a,$$

де $m, n \in \mathbb{Z}$.

Приклад 1.2.6. Розглянемо ще один приклад моноїда. Нехай маємо квадрат на площині (див. мал. ??), вершини якого занумеровані проти годинникової стрілки числами 1, 2, 3, 4. Нехай O — центр квадрата. Позначимо через e, a, b, c повороти квадрата навколо точки O , відповідно, на $0^\circ, 90^\circ, 180^\circ, 270^\circ$ проти годинникової стрілки. Якщо повернути квадрат навколо центру O

на 90° , тоді вершина 1 перейде у вершину 2, 2 — у 3, 3 — у 4, 4 — у 1. В результаті квадрат перейде сам в себе. Це перетворення квадрата можна задати як відображення вершин $\{1, 2, 3, 4\}$ в себе, яке, як звичайно, записують у вигляді таблиці з двох рядків $(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix})$, де у верхньому рядку вписані всі вершини, а в нижньому — їх образи. Множина всіх поворотів складається з чотирьох елементів:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Введемо на множині $G = \{e, a, b, c\}$ поворотів квадрата алгебраїчну операцію \circ — множення цих поворотів. Тоді (G, \circ) — моноїд з одиничним елементом e , в якому кожний елемент e оборотним: $e^{-1} = e$, $a^{-1} = c$, $b^{-1} = b$, $c^{-1} = a$. Рухи площин (тобто біективні відображення площини в себе, що зберігають відстань), які переводять задану геометричну фігуру в

себе, називають симетріями цієї фігури. Так, e, a, b, c є симетріями квадрата. Крім цих симетрій, квадрат має і інші симетрії, а саме симетрії d і f відносно діагоналей d і f , а також симетрії h і g відносно прямих, які проходять через центр квадрата паралельно сторонам. Легко переконатися, що множина $S = \{e, a, b, c, d, f, g, h\}$ теж є прикладом моноїда, в якому кожний елемент є оборотним. Цей моноїд називається групою симетрій квадрата.

Означення 1.2.7. Групою називається моноїд, в якому кожний елемент є оборотним.

Означення 1.2.8. Група (G, \cdot) називається абелевою, якщо $x \cdot y = y \cdot x$ для всіх $x, y \in G$.

Абелеві групи, як правило, записують адитивно: запис $(G, +)$ — група означає $(G, +)$ — абелева група.

Приклад 1.2.7. 1) Повороти квадрата утворюють групу, яка є абелевою. Група симетрій квадрата не є абелевою. Справді,

$$ag = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = f,$$

$$ga = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = d.$$

Отже, $ag \neq ga$.

2) Важливим прикладом групи є група $\text{Aut } A$ — група всіх бієктивних відображенень множини A в себе відносно алгебраїчної операції добутку відображень. Справді, ми знаємо, що добуток відображень асоціативний, 1_A є нейтральним елементом в $\text{Aut } A$ і для кожного бієктивного відображення існує обернене.

3) Нехай $\mathbb{Q}^*, \mathbb{R}^*$ — множини ненульових раціональних та дійсних чисел, а $\mathbb{Q}_+, \mathbb{R}_+$ — множини додатних раціональних та додатних дійсних чисел. Тоді $(\mathbb{Z}, +)$, $(2\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, (\mathbb{R}^*, \cdot) , (\mathbb{R}_+, \cdot) , (\mathbb{Q}_+, \cdot) , $(\{-1, 1\}, \cdot)$ є абелевими групами відносно вказаних операцій.

Твердження 1.2.3 (наслідки з аксіом груп). *Нехай G — група. Вірні такі твердження:*

- 1) *нейтральний елемент в G єдиний;*
- 2) *для кожного елемента $a \in G$ існує єдиний обернений;*
- 3) *з кожної з рівностей $ab = ac$ і $ba = ca$ випливає рівність $b = c$ (закон скорочення);*
- 4) *кожне з двох рівнянь $ax = b$ і $xa = b$ має в G єдиний розв'язок.*

Доведення. Перші дві властивості вже були доведені раніше для моноїдів. Якщо ми маємо рівність $ab = ac$, то, домноживши її зліва на a^{-1} , одержуємо $a^{-1}(ab) = (a^{-1}a)b = eb = b$ і $a^{-1}(ac) = c$, тобто $b = c$. Правий закон скорочення доводиться за допомогою домноження справа на a^{-1} . Розв'язком рівняння $ax = b$ є $x = a^{-1}b$. Цей розв'язок єдиний за законом скорочення. \square

1.2.4. Підгрупа. Критерій підгрупи

Означення 1.2.9. Підгрупою H групи G називається непорожня підмножина $H \subset G$, яка сама є групою відносно тієї ж операції, що і G .

Приклад 1.2.8. 1) У наступних ланцюжках груп кожна група є підгрупою кожної більшої групи:

$$\begin{aligned} (2\mathbb{Z}, +) &\subset (\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +), \\ (\{1, -1\}, \cdot) &\subset (\mathbb{Q}^*, \cdot) \subset (\mathbb{R}^*, \cdot), \\ (\mathbb{Q}_+, \cdot) &\subset (\mathbb{R}_+, \cdot). \end{aligned}$$

2) Група поворотів квадрата є підгрупою його групи симетрій.

Твердження 1.2.4 (критерій підгрупи). *Підмножина H групи G є підгрупою групи G тоді і тільки тоді, коли для кожних двох елементів $x, y \in H$ добуток xy міститься в H і для кожного $x \in H$ обернений елемент x^{-1} теж міститься в H .*

Доведення. Необхідність очевидна. Доведемо достатність. Нехай $h \in H$. Тоді $h^{-1} \in H$ і $hh^{-1} = e \in H$. Асоціативність алгебраїчної операції на H очевидна, адже вона є обмеженням на H алгебраїчної операції в G , а G — група. \square

Підгрупу $\{e\}$ групи G , що складається лише з нейтрального елемента групи G , називають *тривіальною*. Всю групу G теж називають *тривіальною підгрупою* групи G . Всі інші підгрупи (якщо вони існують) називають *нетривіальними*.

Твердження 1.2.5. *Перетин довільної родини підгруп групи G є підгрупою групи G .*

Доведення. Нехай $(H_i)_i \in \mathcal{I}$ скінчена чи нескінчена родина підгруп і $H = \bigcap_{i \in \mathcal{I}} H_i$. Якщо $x, y \in H$, то $x, y \in H_i$ для всіх i . Тому $xy \in H_i$ і $x^{-1} \in H_i$ для всіх i . Це означає, що $xy, x^{-1} \in \bigcap_{i \in \mathcal{I}} H_i$ і H є підгрупою за критерієм підгрупи. \square

1.2.5. Циклічні підгрупи та групи

Нехай G — група і $a \in G$. Розглянемо підмножину $(a) = \{a^n \mid n \in \mathbb{Z}\}$. З рівностей $a^n a^m = a^{n+m}$ і $(a^n)^{-1} = a^{-n}$ випливає, що $((a), \cdot)$ є підгрупою групи (G, \cdot) .

Означення 1.2.10. *Циклічною підгрупою*, породженою елементом $a \in G$, називається підгрупа (a) , що складається з усіх степенів елемента a . Елемент a називається *твірною циклічної групи* (a) . Група G називається *циклічною*, якщо вона збігається з однією із своїх циклічних підгруп.

Покажемо, що всі підгрупи групи \mathbb{Z} є циклічними. Очевидно, що тривіальні підгрупи цієї підгрупи є циклічними і твірною однієї з них є 0, а твірною іншої є -1 . Нехай H — нетривіальна підгрупа групи \mathbb{Z} . Тоді H містить ненульові елементи, а, отже, і додатні елементи: якщо $0 \neq b \in H$, то і $-b \in H$ і один з елементів $b, -b$ є додатним. Нехай a — найменший додатний елемент з H і нехай $x \in H$. Якщо $x > 0$, то розділимо x з остачею на a ,

$x = na + r$, $0 \leq r < a$. Тоді $r = x - na \in H$, бо H підгрупа. Звідси $r = 0$ і $x = na$. Якщо $x < 0$, то $-x > 0$ і знову $-x = ma$, тобто $x = -ma$. Це й означає, що $H = \{ma \mid n \in \mathbb{Z}\}$, тобто $(H, +)$ — циклічна група.

Зauważення 1.2.3. Очевидно, що кожна циклічна група є абелевою.

1.2.6. Порядок елемента групи

Означення 1.2.11. Групу G називають скінченою, якщо множина її елементів є скінченою, в іншому випадку групу G називають нескінченою. Порядком $|G|$ скінченої групи G називають кількість її елементів. Нехай a елемент групи G . Якщо існує додатне натуральне число k таке, що $a^k = e$ — нейтральний елемент групи G , то кажуть, що елемент a має скінчений порядок. Найменше з усіх таких чисел k називають порядком елемента a і позначають через $o(a)$. Якщо не існує додатного натурального числа k з властивістю $a^k = e$, то елемент a називають елементом нескінченого порядку.

Приклад 1.2.9. Розглянемо групу $S = \{e, a, b, c, d, f, g, h\}$ симетрій квадрата з п. 1.2.2. Легко переконатися, що елементи цієї групи мають такі порядки: $o(e) = 1$, $o(a) = o(c) = 4$, $o(b) = o(d) = o(f) = o(g) = o(h) = 2$.

Теорема 1.2.6. Порядок елемента скінченої групи дорівнює порядку циклічної підгрупи, породженої цим елементом.

Доведення. Перш за все, не всі елементи з послідовності $e = a^0, a^1, a^2, \dots, a^k, \dots$ є різними, бо група G скінчена. Знайдуться $i, j \in \mathbb{N}$, $0 \leq i < j$, для яких $a^i = a^j$, тобто $a^{j-i} = e$. Отже, a має скінчений порядок. Нехай $o(a) = n$. Тоді елементи $e = a^0, a^1, \dots, a^{n-1}$ всі різні, бо якби $a^i = a^j$ для $0 \leq i < j \leq n-1$, то $a^{j-i} = e$ і $0 < j-i < n$, що суперечить тому, що $o(a) = n$. Покажемо, що кожний цілий степінь a^m елемента a дорівнює одному з елементів e, a, \dots, a^{n-1} . Це й означатиме, що $o(a) = |(a)| = n$.

Якщо m додатне, то, розділивши m з остачею на n , одержимо $m = dn + r$, $0 \leq r \leq n - 1$ і $a^m = a^{dn+r} = (a^n)^d a^r = e^d a^r = a^r$, що й стверджується. Якщо m від'ємне, то $m = -l$, де $l > 0$, і $a^m = a^{-l} = (a^{-1})^l = (a^{n-1})^l = a^{(n-1)l}$; це означає, що від'ємні степені елемента a зводяться до додатних (тут ми використовуємо рівність $a^{-1} = a^{n-1}$, яка випливає з рівності $a^n = e$). \square

1.3. Групи підстановок

1.3.1. Найпростіші властивості групи підстановок

Нехай M — скінчenna множина, що має n елементів. Ми вже знаємо (див. приклад 2 після означення 1.2.7), що множина $\text{Aut } M$ всіх бієктивних відображень множини M в себе утворює групу відносно множення відображень. Цю групу прийнято позначати S_n . Оскільки природа елементів множини M для нас несуттєва, то будемо вважати, що $M = \{1, 2, \dots, n\}$ — множина перших n додатних натуральних чисел. Елемент σ групи S_n є відображенням скінченної множини в себе, тому його зручно записувати у вигляді таблиці

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

або

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad (1.3.1)$$

де $i_k = \sigma(k)$. Зауважимо, що група S_n неабельєва, якщо $n \geq 3$. Справді, якщо, наприклад,

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}, \quad \text{то} \\ \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix}, \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}, \end{aligned}$$

і тому $\sigma \circ \tau \neq \tau \circ \sigma$.

Елементи групи S_n називають *підстановками*. Зауважимо, що кожну підстановку можна однозначно записати у вигляді (1.3.1). Очевидно, що коли в записі (1.3.1) довільним способом переставити стовпчики, то одержимо запис тієї самої підстановки. Переставивши в (1.3.1) рядки, одержимо підстановку $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$, обернену до підстановки σ . Знайдемо кількість $|S_n|$ елементів групи S_n .

Твердження 1.3.1. $|S_n| = n!$.

Доведення. Кожну підстановку $\sigma \in S_n$ можна однозначно записати у вигляді (1.3.1). Для i_1 в (1.3.1) маємо n можливостей. Для кожної з цих n можливостей маємо $n - 1$ можливість для $i_2 = \sigma(2)$. Якщо ми вже вибрали $i_1 = \sigma(1)$ та $i_2 = \sigma(2)$, то для кожного з $n(n - 1)$ можливих виборів цих двох елементів існує $n - 2$ можливостей для i_3 . І так далі, продовжуючи цей процес, ми отримуємо, що існує $n \cdot (n - 1) \cdot (n - 2) \cdots 2 \cdot 1$ підстановок $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, тобто $|S_n| = n!$. \square

1.3.2. Цикли та орбіти

Підстановка може деякі елементи переміщувати, а деякі залишати на місці. Існують підстановки, які деякі елементи переміщують, так би мовити, по колу, а інші залишають без змін. Наприклад, підстановка

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

залишає без змін елементи 2 і 5, а інші переміщує так: $1 \rightarrow 3 \rightarrow \rightarrow 4 \rightarrow 6 \rightarrow 1$. Останню послідовність чисел і стрілок зображенено на мал. ???. Підстановки такого вигляду будемо називати *циклами*. Не всі підстановки є циклами. Наприклад, підстановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ не є циклом. Введемо скорочений запис для циклів. Нехай $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$. Такий цикл скорочено запишемо у вигляді $(1, 3, 5, 2)$. Множину елементів $\{1, 3, 5, 2\}$, що входять у скорочений запис циклу, називають *орбітою* підстановки, відповідною циклу $(1, 3, 5, 2)$. Перейдемо до строгого означення циклу.

Означення 1.3.1. Циклом (i_1, i_2, \dots, i_k) , де i_1, i_2, \dots, i_k — деякі числа з множини $\{1, 2, \dots, n\}$, називається підстановка $\tau \in S_n$ така, що

$$\tau(i) = \begin{cases} i, & \text{якщо } i \notin \{i_1, \dots, i_k\}, \\ i_{t+1}, & \text{якщо } i = i_t \text{ де } t \neq k, \\ i_1, & \text{якщо } i = i_k. \end{cases}$$

Множину елементів $\{i_1, i_2, \dots, i_k\}$ назовемо *орбітою* підстановки, яка відповідає циклу (i_1, i_2, \dots, i_k) . Два цикли з S_n назовемо *незалежними*, якщо відповідні їм орбіти не мають спільних елементів. Двоелементний цикл назовемо *транспозицією*.

Зauważення 1.3.1. При $k = 1$ з попереднього означення одержується одинична підстановка, тобто цикл довжини 1 є одиничною підстановкою.

Твердження 1.3.2. Якщо ρ і τ незалежні цикли, то $\rho \circ \tau = \tau \circ \rho$.

Доведення. Позначимо через $\tilde{\rho}$ і $\tilde{\tau}$ орбіти, які відповідають циклам ρ і τ . Якщо $i \in \tilde{\rho}$, то $\rho(i) \in \tilde{\rho}$ і $i \notin \tilde{\tau}$. Так само $\tau(i) \in \tilde{\tau}$ і $i \notin \tilde{\rho}$, якщо $i \in \tilde{\tau}$. Тому

$$(\tau \circ \rho)(i) = (\rho \circ \tau)(i) = \begin{cases} \rho(i) = i, & \text{якщо } i \notin \tilde{\rho} \cup \tilde{\tau}, \\ \rho(i), & \text{якщо } i \in \tilde{\rho}, \\ \tau(i), & \text{якщо } i \in \tilde{\tau}. \end{cases}$$

Отже, $(\rho \circ \tau)(i) = (\tau \circ \rho)(i)$ для всіх $i \in \{1, 2, \dots, n\}$, тобто $\rho \circ \tau = \tau \circ \rho$. \square

1.3.3. Розклад підстановки в добуток циклів

Твердження 1.3.3. Кожна підстановка розкладається в добуток незалежних циклів.

Доведення. Для підстановки $\sigma \in S_n$ через $k(\sigma)$ позначимо кількість неінваріантних елементів множини $M = \{1, 2, \dots, n\}$

відносно σ , тобто кількість тих $i \in M$, для яких $\sigma(i) \neq i$. Якщо $k(\sigma) = 0$, то доведення очевидне. Нехай $k(\sigma) = m > 0$. Припускаємо, що твердження доведене для всіх $\sigma' \in S_n$ таких, що $k(\sigma') < m$. Існує $i_1 \in M$ з властивістю $\sigma(i_1) \neq i_1$. Нехай i_1 переходить в i_2 , i_2 в i_3 і так далі. Нехай i_r перший елемент, який повторюється. Якщо $i_r = i_k$, де $2 \leq k \leq r - 1$, то отримаємо два різних елементи i_{r-1} та i_{k-1} , які підстановка σ переводить в один і той же елемент i_k . Це неможливо, бо σ біективне відображення. Тому $i_r = i_1$ і ми отримуємо цикл

$$\tau_1 = (i_1, i_2, \dots, i_{r-1}).$$

Розглянемо тепер підстановку σ_1 , для якої

$$\sigma_1(j) = \begin{cases} j, & \text{якщо } j \in \tilde{\tau}_1 = \{i_1, \dots, i_{r-1}\}, \\ \sigma(j), & \text{якщо } j \notin \tilde{\tau}_1. \end{cases}$$

Легко перевірити, що $\sigma = \tau_1 \sigma_1 = \sigma_1 \tau_1$. Далі $k(\sigma_1) = k(\sigma) - r < k(\sigma)$. Тому, за припущенням, підстановка σ_1 розкладається в добуток незалежних циклів $\sigma_1 = \tau_2 \cdot \dots \cdot \tau_s$. Отже, $\sigma = \tau_1 \sigma_1 = \tau_1 \tau_2 \cdot \dots \cdot \tau_s$ теж розкладається в добуток незалежних циклів. \square

Зауваження 1.3.2. Можна перевірити, що розклад, про який йдеться у твердженні 1.3.3, єдиний з точністю до порядку циклів (вправа!). В той же час, якщо не вимагати умови незалежності циклів, то розклад не є єдиним. Наприклад, $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (1, 2)(2, 3) = (1, 3)(1, 2)$.

1.3.4. Розклад підстановки в добуток транспозицій

Твердження 1.3.4. *Будь-який цикл розкладається в добуток транспозицій.*

Доведення. Для доведення досить перевірити рівність

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_3)(i_1, i_2). \quad (1.3.2)$$

\square

Твердження 1.3.5. *Кожна підстановка розкладається в добуток транспозицій.*

Доведення. Розкладаємо спочатку підстановку в добуток незалежних циклів (твердження 1.3.3), а тоді кожний цикл, що входить в цей розклад, розкладаємо в добуток транспозицій за правилом (1.3.2). \square

1.3.5. Парні та непарні підстановки

Для дальнього дослідження групи S_n нам необхідне поняття перестановки. Під *перестановкою* i_1, i_2, \dots, i_n чисел $1, 2, \dots, n$ розуміють запис цих чисел в деякому порядку. Взагалі, перестановки і підстановки тісно між собою зв'язані. Якщо i_1, i_2, \dots, i_n — перестановка, то $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ підстановка. Навпаки, якщо $\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$ — підстановка, то обидва її рядки є перестановками.

Означення 1.3.2. Кажуть, що числа i_k та i_l утворюють *інверсію* в перестановці $i_1, \dots, i_k, \dots, i_l, \dots, i_n$, якщо $i_k > i_l$, а $k < l$. Якщо i_k та i_l не утворюють інверсії, то кажуть, що вони утворюють *порядок*.

Кількість всіх інверсій даної перестановки характеризує, наскільки вона відрізняється від перестановки $1, 2, \dots, n$. Але нас буде цікавити не так число інверсій, як його парність.

Означення 1.3.3. Перестановка називається *парною*, якщо число її інверсій парне, і *непарною* в протилежному випадку.

Наприклад, число інверсій перестановки $3, 5, 7, 1, 4, 2, 6$ дорівнює 10. Отже, ця перестановка парна. Перестановка $2, 1, 4, 3, 5, 7, 6$ непарна: її елементи утворюють 3 інверсії.

Означення 1.3.4. *Транспозицією* перестановки назовемо заміну місцями двох її елементів.

Твердження 1.3.6. *Транспозиція змінює парність перестановки.*

Доведення. Розглянемо спочатку випадок, коли маємо транспозицію сусідніх елементів i_k та i_{k+1} . Число інверсій, які утворюють i_k та i_{k+1} з іншими елементами, при їх транспозиції не змінюється. Якщо i_k, i_{k+1} утворюють порядок, то їх транспозиція дає інверсію. Якщо ж ці елементи утворюють інверсію, то після їх перестановки вона пропаде. В обох випадках загальне число інверсій змінюється на 1, тобто парність перестановки змінюється на протилежну. Нехай транспозиція здійснюється над числами i_k та i_l , між якими є ще числа j_1, \dots, j_s . Цю транспозицію можна виконувати, переставивши i_k з кожним j_1, \dots, j_s , тоді переставивши i_k та i_l і, нарешті, переставивши i_l з кожним j_1, \dots, j_s , отже, зробивши всього $2s+1$ перестановок сусідніх елементів. Знаючи, що при транспозиції сусідніх елементів парність змінюється, ми одержуємо звідси, що це вірно і при транспозиції будь-яких елементів. \square

Означення 1.3.5. Підстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ називається *парною*, якщо перестановка i_1, i_2, \dots, i_n парна. В іншому випадку підстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ називається *непарною*.

1.3.6. Розклад і парність підстановок

Теорема 1.3.7. Коєсна парна підстановка розкладається в добуток парного числа транспозицій, а непарна — в добуток непарного числа транспозицій.

Доведення. Спочатку доведемо, що при множенні підстановки справа на транспозицію одержимо підстановку протилежної парності. Справді,

$$\begin{pmatrix} \dots r \dots s \dots \\ \dots i_r \dots i_s \dots \end{pmatrix} (r, s) = \begin{pmatrix} \dots r \dots s \dots \\ \dots i_s \dots i_r \dots \end{pmatrix}.$$

Бачимо, що множення підстановки на транспозицію (r, s) дає транспозицію елементів i_r, i_s в нижньому рядку підстановки. Застосувавши твердження 1.3.6, одержуємо, що отримана і початкова підстановки мають різну парність. За твердженням 1.3.5

кожна підстановка π розкладається в добуток транспозицій $\pi = \sigma_1 \cdots \sigma_k$. Перепишемо цю рівність у вигляді $\pi = \varepsilon\sigma_1 \cdots \sigma_k$, де ε — одинична підстановка. Бачимо, що підстановка π одержується з одиничної підстановки ε домноженням справа на транспозиції $\sigma_1, \dots, \sigma_k$. Оскільки домноження на транспозицію змінює парність, а ε — парна підстановка, то π — парна підстановка тоді і тільки тоді, коли k — парне число. \square

Легко бачити, що квадрат будь-якої транспозиції дорівнює одиничній підстановці: $(r, s)^2 = \varepsilon$. Звідси випливає, що $\pi^{-1} = \sigma_k \cdots \sigma_1$, якщо $\pi = \sigma_1 \dots \sigma_k$. Це означає, що підстановки π і π^{-1} мають однукову парність. Тому підстановка, обернена до парної, є парною. Крім цього, добуток підстановок однакової парності є парною підстановкою. Тому, за критерієм підгрупи, множина парних підстановок утворює підгрупу A_n групи всіх підстановок S_n .

Означення 1.3.6. Якщо підстановка $\sigma \in S_n$ розкладається в добуток t транспозицій, то t називають *сигнатурою* підстановки σ і позначають $\text{sgn}\sigma$. Сигнатура $\text{sgn}\sigma$ визначається підстановкою σ однозначно з точністю до парного доданка.

1.4. Гомоморфізми, суміжні класи та фактор-групи

1.4.1. Гомоморфізми півгруп та груп

Нехай (G_1, \cdot) і (G_2, \circ) — дві півгрупи або групи.

Означення 1.4.1. Відображення $\varphi: G_1 \rightarrow G_2$ називається *гомоморфізмом*, якщо $\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$ для всіх $x, y \in G_1$. Сюр'ективний гомоморфізм називається *епіморфізмом*, ін'ективний гомоморфізм називається *мономорфізмом* груп, а бієктивний гомоморфізм називається *ізоморфізмом*. Якщо існує ізоморфізм півгруп (груп) G_1 і G_2 , то ці півгрупи (групи) називаються

ізоморфними. Той факт, що півгрупи (групи) G_1 і G_2 ізоморфні, будемо записувати $G_1 \simeq G_2$.

Приклад 1.4.1. 1) *Множина \mathbb{R}_+ всіх додатних дійсних чисел є групою відносно звичайного множення чисел. Кожне додатне число $r \neq 1$ визначає гомоморфізм адитивної групи \mathbb{R} дійсних чисел в групу \mathbb{R}_+ за правилом $a \xrightarrow{\exp} r^a$. Справді, $\exp(a+b) = r^{a+b} = r^a r^b = \exp a \cdot \exp b$. Відображення $\exp: \mathbb{R} \rightarrow \mathbb{R}^+$ має обернене $\log: \mathbb{R}^+ \rightarrow \mathbb{R}$, отже, воно біективне. Тому групи $\{\mathbb{R}_+, \cdot\}$ і $\{\mathbb{R}, +\}$ – ізоморфні.*

2) Позначимо через C_2 групу з елементами $1, -1$ і звичайним множенням. Розглянемо відображення $\varepsilon: S_n \rightarrow C_2$, для якого

$$\varepsilon(\pi) = \begin{cases} 1, & \pi - \text{парна}, \\ -1, & \pi - \text{непарна}. \end{cases}$$

Тоді

$$\varepsilon(\sigma\tau) = \begin{cases} 1, & \sigma \text{ і } \tau \text{ мають однакову парність}, \\ -1, & \text{в іншому випадку} \end{cases} = \varepsilon(\sigma)\varepsilon(\tau).$$

Отже, ε – гомоморфізм груп S_n і C_2 .

3) Якщо група G абелева, то відображення $\varepsilon: G \rightarrow G$, $\varepsilon(a) = a^{-1}$, є ізоморфізмом групи G в себе.

Означення 1.4.2. Гомоморфізм групи G в себе називається *ендоморфізмом* груп. Множину всіх ендоморфізмів групи G в себе позначають $\text{End}G$.

Зauważення 1.4.1. Оскільки $1_G \in \text{End}G$, то $\text{End}G \neq \emptyset$.

Твердження 1.4.1. Якщо $\phi: G_1 \rightarrow G_2$ – гомоморфізм груп, то:

- a) образ $\phi(e_1)$ нейтрального елемента групи G_1 є нейтральним елементом групи G_2 ;
- б) образ $\phi(G_1)$ є підгрупою групи G_2 .

Доведення. а) Нехай e_1 та e_2 — нейтральні елементи груп G_1 та G_2 відповідно, $a_1 \in G_1$. Маємо

$$e_2\phi(a_1) = \phi(e_1a_1) = \phi(e_1)\phi(a_1).$$

Застосувавши до рівності $e_2\phi(a_1) = \phi(e_1)\phi(a_1)$ закон скорочення, одержимо $\phi(e_1) = e_2$.

б) Спочатку покажемо, що $\phi(G_1)$ задовольняє умови критерію підгрупи. Нехай $a_2, b_2 \in \phi(G_1)$. Тоді існують $a_1, b_1 \in G_1$, такі що $a_2 = \phi(a_1)$, $b_2 = \phi(b_1)$. $a_2b_2 = \phi(a_1)\phi(b_1) = \phi(a_1b_1)$. Отже, $a_2b_2 \in \phi(G_1)$. Далі, за доведеним, $e_2 = \phi(e_1) = \phi(a_1a_1^{-1}) = \phi(a_1)\phi(a_1^{-1})$. Звідси $a_2^{-1} = \phi(a_1)^{-1} = \phi(a_1^{-1}) \in \phi(G_1)$. \square

Твердження 1.4.2. а) Якщо ϕ — ізоморфізм груп G_1 і G_2 , то ϕ^{-1} є ізоморфізмом груп G_2 і G_1 .

б) Якщо ψ — ізоморфізм груп G_2 і G_3 , то добуток $\psi \circ \phi$ є ізоморфізмом груп G_1 і G_3 .

Доведення. а) Досить показати, що $\phi^{-1}(a_2b_2) = \phi^{-1}(a_2)\phi^{-1}(b_2)$ для всіх $a_2, b_2 \in G_2$. Оскільки, ϕ — біективне відображення, то для елементів $a_2, b_2 \in G_2$ існують елементи $a_1, b_1 \in G_1$ такі, що $\phi(a_1) = a_2$, $\phi(b_1) = b_2$. Тоді $\phi^{-1}(a_2b_2) = \phi^{-1}(\phi(a_1)\phi(b_1)) = \phi^{-1}(\phi(a_1b_1)) = a_1b_1 = \phi^{-1}(a_2)\phi^{-1}(b_2)$.

б) Добуток $\psi \circ \phi$ є біективним відображенням групи G_1 у групу G_3 . Крім цього, для $a, b \in G_1$ маємо $(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = (\psi\phi)(a)(\psi\phi)(b)$. \square

Враховуючи той факт, що одиничне відображення 1_G є ізоморфізмом групи G , з твердження 1.4.2 випливає, що відношення ізоморфізму груп задовольняє умовам відношення еквівалентності. Це дозволяє вивчати групи з точністю до ізоморфізму, тобто не розрізняти ізоморфні групи.

1.4.2. Суміжні класи

Означення 1.4.3. Нехай G — група, а H — її підгрупа. Множину елементів $Hx = \{hx \mid h \in H\}$ називають *правим сумі-*

жним класом групи G за підгрупою H . Множина $xH = \{xh \mid h \in H\}$ називається лівим суміжним класом.

Виявляється, що праві (ліві) суміжні класи групи G за підгрупою H є класами еквівалентних відносно відношення еквівалентності на множині елементів групи G , які визначаються за допомогою підгрупи H . А саме, задамо на групі G відношення еквівалентності \sim_H . Вважатимемо, що $a \sim_H b$, якщо $ab^{-1} \in H$. Переконаємося, що \sim_H — відношення еквівалентності:

- а) $a \sim_H a$, бо $aa^{-1} = e \in H$.
- б) Якщо $a \sim_H b$, то $ab^{-1} \in H$. Отже, $(ab^{-1})^{-1} = ba^{-1} \in H$, тому $b \sim_H a$.
- в) Нехай $a \sim_H b$ і $b \sim_H c$. Тоді $ab^{-1} \in H$ і $bc^{-1} \in H$. Звідси $ab^{-1}bc^{-1} = ac^{-1} \in H$. Отже, $a \sim_H c$.

Таким чином, \sim_H — відношення еквівалентності на G . Тому група G розбивається на класи еквівалентних елементів, причому різні класи попарно не перетинаються. кожний такий клас \bar{x} складається із елементів $z \in G$ таких, що $zx^{-1} \in H$, тобто $zx^{-1} = h \in H$, $z = hx$. Отже, клас еквівалентності \bar{x} елемента x — це множина $Hx = \{hx \mid h \in H\}$. Очевидно, що $G = \bigcup_{x \in G} Hx$. Ми бачимо, що праві суміжні класи є класами еквівалентних елементів відносно відношення еквівалентності \sim_H . Так само можна показати, що ліві суміжні класи одержуються з відношення еквівалентності $H \sim$, для якого: $a \sim b \Leftrightarrow a^{-1}b \in H$. Тому група G є об'єднанням як лівих, так і правих суміжних класів:

$$G = \bigcup_{x \in G} Hx = \bigcup_{x \in G} xH.$$

Твердження 1.4.3. *Множина лівих суміжних класів групи G за підгрупою H рівнопотужна множині правих суміжних класів.*

Доведення. Розглянемо відображення f , яке лівому суміжному класу xH ставить у відповідність правий суміжний клас Hx^{-1} , $f(xH) = Hx^{-1}$. Маємо

$$xH = yH \Leftrightarrow x^{-1}y \in H \Leftrightarrow x^{-1} \in Hy^{-1} \Leftrightarrow Hx^{-1} = Hy^{-1}.$$

Звідси випливає як коректність означення відображення f , так і його ін'єктивність. Нарешті, $f(y^{-1}H) = Hy$ для кожного $y \in G$, тобто відображення f сюр'єктивне. \square

Означення 1.4.4. Якщо кількість різних лівих (правих) суміжних класів групи G за підгрупою H скінчена, то кажуть, що підгрупа H має скінчений індекс в групі G . У протилежному випадку кажуть, що H має нескінчений індекс. *Індекс* підгрупи H у групі G позначають $(G : H)$.

Приклад 1.4.2. 1) Нехай $G = S_n$, а $H = A_n$ – підгрупа парних підстановок. Нехай $\pi \in S_n$. Тоді πA_n складається з усіх парних підстановок, якщо підстановка π – парна, і з усіх непарних підстановок в іншому випадку. З таких самих підстановок (всіх парних або непарних) складається і правий суміжний клас $A_n\pi$. Тому в цьому випадку

$$\pi A_n = A_n\pi = \begin{cases} A_n, & \text{якщо } \pi \text{ – парна підстановка,} \\ S_n \setminus A_n, & \text{в іншому випадку.} \end{cases}$$

Бачимо, що тут ліві суміжні класи збігаються з правими. Наступний приклад показує, що так трапляється не завжди.

2) Нехай $G = S_3$, $H = \{e, (1, 2)\}$. Тоді $(2, 3)H = \{(2, 3), (1, 3, 2)\}$, а $H(2, 3) = \{(2, 3), (1, 2, 3)\}$.

Зауваження 1.4.2. Множина елементів будь-якого правого (лівого) суміжного класу Hx (xH) групи G за підгрупою H рівнопотужна множині H , тобто існують біективні відображення $H \rightarrow Hx$ та $H \rightarrow xH$. Справді, відображення $f: H \rightarrow Hx$, для якого $f(h) = hx$, є біективним, бо для нього існує обернене $f^{-1}: Hx \rightarrow H$, $f^{-1}(hx) = (hx)x^{-1} = h$. Так само відображення $g: H \rightarrow xH$, $g(h) = xh$, є біективним. Зокрема, якщо H є скінченою групою, що має t елементів, то кожний правий (лівий) суміжний клас теж має t елементів.

1.4.3. Теорема Лагранжа

Нагадаємо, що порядком скінченної групи G називають кількість елементів множини G .

Теорема 1.4.4 (Лагранж). *Порядок будь-якої підгрупи H скінченної групи G є дільником порядку групи G .*

Доведення. Група G є об'єднанням правих суміжних класів Hx . Вони є класами еквівалентності відносно відношення еквівалентності \sim_H , розглянутого в п. 1.4.2. Різні класи не мають спільних елементів. Далі, якщо підгрупа H складається з t елементів, то, згідно зауваження 1.4.2, кожний суміжний клас Hx містить t елементів. Тому порядок n групи G дорівнює tk , де k — кількість різних суміжних класів Hx . \square

Наслідок 1.4.5. *Порядок кожного елемента скінченної групи G є дільником порядку групи G .*

Доведення. Порядок елемента за теоремою 1.2.6 дорівнює порядку циклічної підгрупи, породженої цим елементом. \square

Наслідок 1.4.6. *Якщо порядок групи G є простим числом, то вона має лише тривіальні підгрупи.*

Доведення. Єдиними дільниками простого числа $p \in \{1, p\}$. \square

1.4.4. Розбиття групи, узгоджені з операцією

Серед відношень еквівалентності, заданих на групі G , особливе значення мають ті відношення еквівалентності, які узгоджені з груповою операцією.

Означення 1.4.5. Відношення еквівалентності \sim на групі G називається *узгодженим з операцією*, якщо для будь-яких елементів $g_1, g_2, g'_1, g'_2 \in G$ з $g_1 \sim g_2$ і $g'_1 \sim g'_2$ випливає $g_1g'_1 \sim g_2g'_2$.

Інакше кажучи, відношення еквівалентності на групі узгоджене з груповою операцією, якщо добуток довільних елементів по одному з двох заданих суміжних класів завжди належить до одного і того ж суміжного класу. Розглянемо, наприклад, підгрупу A_n парних підстановок в групі S_n . Ця підгрупа визначає розбиття $S_n = A_n \cup (S_n \setminus A_n)$ групи S_n (нагадаємо, що задання розбиття множини рівносильне заданню відношення еквівалентності на цій множині). Очевидно, добуток двох довільних парних підстановок є парною підстановкою, добуток двох непарних підстановок є парною, а добуток парної і непарної підстановок є непарною підстановкою. Тому ми маємо тут розбиття S_n (відношення еквівалентності на S_n), яке узгоджене з операцією.

Означення 1.4.6. Підгрупа H групи G називається *нормальною*, якщо для будь-якого $g \in G$ справедлива рівність $gH = Hg$ (ліві суміжні класи збігаються з правими).

Приклад 1.4.3. 1) Якщо G абелева група, то кожна підгрупа групи G є нормальною.

2) Ми бачили в п. 1.4.2, що A_n є нормальною підгрупою групи S_n .

3) Легко зрозуміти, що якщо $(G : H) = 2$, то розбиття групи як на ліві, так і на праві суміжні класи має вигляд $G = H \cup (G \setminus H)$, тобто в цьому випадку ліві суміжні класи збігаються з правими і H є нормальною підгрупою групи G . Зокрема, група поворотів квадрата є нормальною підгрупою всіх симетрій квадрата.

Твердження 1.4.7. Підгрупа H групи G є нормальною в G тоді і тільки тоді, коли $ghg^{-1} \in H$ для всіх $h \in H$, $g \in G$.

Доведення. Нехай H нормальна в G . Тоді $gH = Hg$, тобто для кожного $h \in H$ і кожного $g \in G$ існує $s \in H$ такий, що $gh = sg$. Звідси $ghg^{-1} = s \in H$. Навпаки, якщо для всіх $h \in H$, $g \in G$ $ghg^{-1} = s \in H$, то $gh = sg$, звідки $gH \subset Hg$. Оскільки $g^{-1}h(g^{-1})^{-1} \in H$ для всіх $h \in H$, то і $Hg \subset gH$, а тому $gH = Hg$. \square

Теорема 1.4.8 (про розбиття групи). *Розбиття групи G на класи еквівалентності узгоджене з груповою операцією тоді і тільки тоді, коли воно є розбиттям на суміжні класи за діякою нормальнюю підгрупою H .*

Доведення. *Необхідність.* Нехай $G = \bigcup_i G_i$ — розбиття, узгоджене з операцією. Припустимо, що нейтральний елемент e групи G належить до G_1 . Покажемо, що G_1 — підгрупа групи G . Нехай $g_1, g_2 \in G_1$. Тоді $g_1 \sim e$, $g_2 \sim e$, отже, $g_1 g_2 \sim e$. Це означає, що $g_1 g_2 \in G_1$. Далі, якщо $g \sim e$ і, очевидно, $g^{-1} \sim g^{-1}$, то $g g^{-1} \sim e g^{-1}$, тобто $g^{-1} \sim e$. Це означає, що $g^{-1} \in G_1$. Отже, за критерієм підгрупи, G_1 є підгрупою групи G .

Покажемо, що G_1 — нормальна підгрупа. Нехай $g \in G$, $g_1 \in G_1$. Тоді $g_1 \sim e$ і $g g_1 g^{-1} \sim g e g^{-1} = e$, тобто $g g_1 g^{-1} \in G_1$ і, в силу твердження 1.4.7, G_1 — нормальна підгрупа.

Переконаємося, нарешті, що кожен клас G_i є суміжним класом за підгрупою G_1 . Зафіксуємо елемент $g_i \in G_i$. Нехай g — довільний елемент множини G_i . Тоді з $g \sim g_i$ випливає $g_i^{-1}g \sim \sim g_i^{-1}g_i = e$. Отже, елемент $h = g_i^{-1}g$ міститься в G_1 , тому $g = g_i h \in g_i G_1$, тобто $G_i \subset g_i H$. Крім цього, якщо $h \in G_1$, то $h \sim e$ і тому $g_i h \sim g_i$. Це означає, що $g_i h \in G_i$, тобто $g_i G_1 \subset G_i$ і, остаточно, $G_i = g_i G_1$.

Достатність. Нехай H — нормальна підгрупа групи G , $G = \bigcup gH$ — розбиття G на суміжні класи. Доведемо, що це розбиття узгоджене з операцією. Нам потрібно показати, що коли $g_1 H \sim g_2 H$, $g'_1 H \sim g'_2 H$, то $g_1 g'_1 H \sim g_2 g'_2 H$. Оскільки $g_1 H \sim g_2 H$, $g'_1 H \sim g'_2 H$, то існують такі елементи $h_1, h_2 \in H$, що $g_1 = g_2 h_1$, $g'_1 = g'_2 h_2$. З нормальності підгрупи H випливає, що знайдеться елемент $h_3 \in H$, такий що $h_1 g'_2 = g'_2 h_3$. Звідси $g_1 g'_1 = g_2 h_1 g'_2 h_2 = = g_2 g'_2 h_3 h_2 = g_2 g'_2 h_4$, де $h_4 = h_3 h_2 \in H$. Отже, $g_1 g'_1 H \sim g_2 g'_2 H$ і наше розбиття узгоджене з операцією. \square

1.4.5. Фактор-група

Нехай G — група, $G = \bigcup_{i \in I} G_i$ — розбиття групи G , узгоджене з операцією. Нагадаємо, що коли задане розбиття (відношен-

ня еквівалентності) деякої множини G , то множину, елементами якої є суміжні класи G_i , називають *фактор-множиною*.

Означимо на фактор-множині $\{G_i \mid i \in I\}$ наступну алгебраїчну операцію: *додутком класів* G_i та G_j назовемо клас G_k ($G_i \cdot G_j = G_k$), в якому лежать добутки $g_i g_j$ для всіх $g_i \in G_i$, $g_j \in G_j$. Оскільки розбиття узгоджене з операцією, то G_k не залежить від конкретного вибору елементів g_i та g_j , а залежить лише від вибору класів G_i та G_j , тобто наша алгебраїчна операція на фактор-множині $\{G_i \mid i \in I\}$ означена коректно.

У п. 1.4.4 ми бачили, що розбиття групи, узгоджене з операцією, є обов'язково розбиттям за деякою нормальнюю підгрупою H , і суміжні класи G_i є суміжними класами групи G за підгрупою H : $G_i = g_i H = H g_i$.

Позначимо фактор-множину $\{G_i \mid i \in I\} = \{gH \mid g \in G\}$ символом G/H . Означення алгебраїчної операції в G/H можна записати в іншому, більш зручному, вигляді.

Означення 1.4.7. $aH \cdot bH = abH$.

Твердження 1.4.9. G/H є групою відносно щойно означеної алгебраїчної операції над її елементами.

Доведення. Дано операція асоціативна:

$$aH(bHcH) = aH(bcH) = a(bc)H = (ab)cH = abHcH = (aHbH)cH.$$

Нейтральним елементом є суміжний клас $eH = H$. Нарешті, $(aH)^{-1} = a^{-1}H$. \square

Означення 1.4.8. Група G/H називається *фактор-групою* групи G за нормальнюю підгрупою H . Легко перевірити, що відображення $\varphi: G \rightarrow G/H$, $\varphi(a) = aH$, є гомоморфізмом груп. Цей гомоморфізм називають *канонічним*.

Приклад 1.4.4. 1) Нехай $G = S_n$, $H = A_n$. Ми бачили, що A_n — нормальнa підгрупа групи S_n . Фактор-група S_n/A_n складається з двох елементів A_n і $S_n \setminus A_n$. Розглянемо групу

$C_2 = (\{-1, 1\}, \cdot)$, що складається з двох елементів 1 і -1 зі звичайним множенням. Відображення $\phi: S_n/A_n \rightarrow C_2$, для якого $\phi(A_n) = 1$, $\phi(S_n \setminus A_n) = -1$ є, як легко бачити, ізоморфізмом груп S_n/A_n і C_2 .

2) Розглянемо підгрупу \mathbb{Z} групи \mathbb{Q} . \mathbb{Q} — абелевова група, тому \mathbb{Z} є її нормальним підгрупою. Фактор-група \mathbb{Q}/\mathbb{Z} складається з суміжних класів $\frac{m}{n} = \frac{m}{n} + \mathbb{Z}$, де $\frac{m}{n} \in \mathbb{Q}$. У кожному такому суміжному класі $\frac{m}{n}$ міститься єдине раціональне число $\frac{a}{b}$ з властивістю $0 \leq \frac{a}{b} < 1$. ($\frac{a}{b} = \frac{m}{n} - [\frac{m}{n}]$, $[\frac{m}{n}]$ — ціла частина $\frac{m}{n}$). Це означає, що елементи групи \mathbb{Q}/\mathbb{Z} перебувають у біекційній відповідності з раціональними числами $\frac{a}{b}$, $0 \leq \frac{a}{b} < 1$. Знайдемо, наприклад, суму елементів $\frac{3}{8}$ і $\frac{5}{7}$ групи \mathbb{Q}/\mathbb{Z} : $\frac{3}{8} + \frac{5}{7} = \frac{61}{56} = \frac{5}{56}$.

1.4.6. Теорема про гомоморфізми

Нехай $\varphi: G \rightarrow G'$ — гомоморфізм груп. Ми вже знаємо (див. твердження 1.4.1), що образ $\varphi(G)$ гомоморфізму φ є підгрупою групи G' . Для позначення образу гомоморфізму використовують також символ $\text{Im}\varphi$, тобто $\text{Im}\varphi = \varphi(G)$. Введемо ще одне важливе поняття, зв'язане з гомоморфізмами, — **ядро гомоморфізму** φ .

Означення 1.4.9. Множину $\text{Ker}\varphi = \{g \in G \mid \varphi(g) = e\}$ (e — нейтральний елемент групи G') називають **ядром гомоморфізму** φ .

Твердження 1.4.10. $\text{Ker}\varphi$ є нормальною підгрупою групи G .

Доведення. Використаємо критерій підгрупи. Якщо $g_1, g_2 \in \text{Ker}\varphi$, то $\varphi(g_1g_2) = \varphi(g_1) \cdot \varphi(g_2) = e \cdot e = e$ і $\varphi(g_1^{-1}) = \varphi(g_1)^{-1} = e^{-1} = e$. Отже, $\text{Ker}\varphi$ — підгрупа. Якщо тепер $g \in G$, $h \in \text{Ker}\varphi$, то $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e$; тому, за твердженням 1.4.7, $\text{Ker}\varphi$ — нормальнa підгрупа. \square

Теорема 1.4.11. Якщо $\varphi: G \rightarrow G'$ — гомоморфізм груп і $H = \text{Ker}\varphi$, то існує ізоморфізм $\bar{\varphi}: G/H \xrightarrow{\sim} \text{Im}\varphi$.

Доведення. Нехай $\bar{g} = gH \in G/H$. Означимо $\bar{\varphi}(\bar{g}) = \varphi(g)$ і перевіримо, що $\bar{\varphi}$ — біективний гомоморфізм. Спочатку пересвідчуємося, що $\bar{\varphi}$ є відображенням: якщо $\bar{g}_1 = \bar{g}_2$, то $g_1g_2^{-1} \in \text{Ker}\varphi$, а тому $\varphi(g_1)\varphi(g_2)^{-1} = e$, і $\varphi(g_1) = \varphi(g_2)$.

Очевидно, що $\bar{\varphi}$ — сюр'єктивне відображення. Перевіримо, що воно також ін'єктивне. Якщо $\bar{\varphi}(\bar{g}_1) = \bar{\varphi}(\bar{g}_2)$, то $\varphi(g_1) = \varphi(g_2)$, отже, $g_1g_2^{-1} \in \text{Ker}\varphi$, тому $\bar{g}_1 = \bar{g}_2$ за критерієм рівності суміжних класів.

Таким чином, ми довели, що $\bar{\varphi}$ — біективне відображення. Залишається перевірити, що $\bar{\varphi}$ — гомоморфізм, а це випливає з наступної низки рівностей:

$$\bar{\varphi}(\bar{g}_1\bar{g}_2) = \bar{\varphi}(\bar{g}_1\bar{g}_2) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \bar{\varphi}(\bar{g}_1)\bar{\varphi}(\bar{g}_2).$$

□

1.5. Кільця та поля

1.5.1. Означення та приклади кілець. Наслідки з аксіом

Означення 1.5.1. *Кільцем* називається множина R з двома алгебраїчними операціями “+” — додавання і “.” — множення, якщо ці операції задовольняють наступним властивостям:

- 1) R — абеліова група відносно додавання;
- 2) множення асоціативне: $\forall a, b, c \in R \quad a(bc) = (ab)c$;
- 3) множення зв’язане з додаванням законами дистрибутивності:

$$\forall a, b, c \in R \quad (a + b)c = ac + bc, \quad c(a + b) = ca + cb.$$

Якщо множення в кільці R комутативне, то R називають *комутативним* кільцем. Якщо існує елемент $1 \in R$, такий що $1a = a1 = a$ для кожного $a \in R$, то R називають *кільцем з одиничним елементом* або *кільцем з 1*.

Приклад 1.5.1. 1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ є комутативними кільцями з 1, $2\mathbb{Z}$ — комутативне кільце без 1.

2) Мноожина дійсних функцій від дійсної змінної, визначених на проміжку (a, b) , є комутативним кільцем з 1 відносно звичайних операцій додавання та множення функцій.

3) Нехай A — непорожня мноожина, $M = 2^A$ — мноожина всіх підмноожин мноожини A . Визначимо на 2^A операції: $X \oplus Y = (X \cup Y) \setminus (X \cap Y)$ і $X \odot Y = X \cap Y$ — перетин X і Y . M є кільцем відносно цих операцій.

У кільці обов'язково існує нейтральний елемент відносно додавання, який ми будемо позначати 0 і називати нулем. Абелеву групу $(R, +)$ кільця R називають *адитивною групою кільця R* .

Твердження 1.5.1. У кожному кільці R виконуються такі властивості (a, b — будь-які елементи із R):

- 1) $a \cdot 0 = 0 \cdot a = 0$;
- 2) $a(-b) = (-a)b = -ab$;
- 3) $(-a)(-b) = ab$. ($-a, -b, -ab$ означають обернені елементи до a, b, ab відносно операції додавання).

Доведення. 1) З рівностей $0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a$ і $0 + 0 \cdot a = 0 \cdot a$ за законом скорочення випливає, що $0 \cdot a = 0$. Так само доводиться, що й $a \cdot 0 = 0$. 2) $a(-b) + ab = a(-b + b) = a \cdot 0 = 0$ за доведеним. Отже, $a(-b) = -ab$. Так само доводиться, що і $(-a)b = -ab$. 3) $(-a)(-b) + (-ab) = (-a)(-b) + (-a)b = = (-a)(-b + b) = -a \cdot 0 = 0$. З іншого боку, $ab + (-ab) = 0$. За законом скорочення звідси випливає, що $(-a)(-b) = ab$. \square

Надалі ми будемо писати $a - b$ замість $a + (-b)$.

1.5.2. Підкільця та ідеали. Суміжні класи за ідеалом

Означення 1.5.2. Підмноожина R_1 кільця R називається *підкільцем* кільця R , якщо R_1 є кільцем відносно тих же операцій, що і в R .

Приклад 1.5.2. 1) У ланцюжку $6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ кожне попереднє кільце є підкільцем кожного наступного (операції тут звичайні додавання і множення).

2) Кільце неперервних дійсних функцій, визначених на проміжку (a, b) , є підкільцем кільця всіх дійсних функцій, визначених на цьому проміжку.

Означення 1.5.3. Підмножина \mathcal{I} кільця R називається *правим (лівим) ідеалом* в R , якщо вона має наступні властивості:

- 1) $\forall a, b \in \mathcal{I} \quad a - b \in \mathcal{I};$
- 2) $\forall a \in \mathcal{I}, \forall c \in R \quad ac \in \mathcal{I} (ca \in \mathcal{I}).$

У випадку комутативного кільця праві і ліві ідеали, очевидно, збігаються, тому в цьому випадку вживають термін *ідеал*.

Приклад 1.5.3. 1) $n\mathbb{Z}$ є ідеалом в кільці \mathbb{Z} , бо різниця двох цілих чисел, кратних n , є цілим числом, кратним n , і добуток цілого числа, кратного n , на довільне ціле число є цілим числом, кратним n .

2) Нехай R — комутативне кільце з 1, $a \in R$. Розглянемо множину $(a) = \{ac \mid c \in R\}$. Очевидно, (a) є ідеалом (це узагальнення прикладу 1). Цей ідеал (a) називають *головним ідеалом*, *породженим елементом* a , і часто позначають aR .

Твердження 1.5.2. *коєсний ідеал \mathcal{I} в кільці R є підкільцем кільця R .*

Доведення. Якщо $b \in \mathcal{I}$, то $0 = b - b \in \mathcal{I}$, $-b = 0 - b \in \mathcal{I}$ і $a + b = a - (-b) \in \mathcal{I}$. Це означає, що множина \mathcal{I} є підгрупою групи R відносно додавання. Крім того, з означення ідеалу випливає, що \mathcal{I} замкнена відносно множення. Для \mathcal{I} справедливі всі аксіоми з означення кільця. Це випливає з того, що вони справедливі для всього R . \square

Зauważення 1.5.1. Невірно, що підкільце зобов'язане бути ідеалом. Наприклад, підкільце \mathbb{Z} кільця \mathbb{Q} не є ідеалом в \mathbb{Q} .

До кінця цього параграфа розглядаються лише комутативні кільця.

1.5.3. Фактор-кільце

Нехай \mathcal{I} — ідеал в кільці R . Тоді \mathcal{I} — підгрупа адитивної групи R . Тому так само, як і у випадку груп, можна означити відношення еквівалентності: $a \sim_{\mathcal{I}} b$ тоді і тільки тоді, коли $a - b \in \mathcal{I}$ (порівняйте з п. 1.4.4). Зауважимо, що в даному випадку ситуація більш проста, ніж у п. 1.4.4, оскільки адитивна група R є комутативною. Отже, так само, як у п. 1.4.4, ми одержимо розбиття кільця R на суміжні класи $a + \mathcal{I}$ за ідеалом \mathcal{I} . Ми пишемо $a \sim a'$, якщо елементи a і a' належать до одного і того ж суміжного класу, тобто $a - a' \in \mathcal{I}$.

Означення 1.5.4. Розбиття кільця R (відношення еквівалентності на R) називається *узгодженним з операціями*, якщо для будь-яких елементів $a, b, a', b' \in R$ з $a \sim a'$ і $b \sim b'$ випливає $a + b \sim a' + b'$ і $ab \sim a'b'$.

Теорема 1.5.3 (про розбиття кільця). *Розбиття кільця R узгоджене з операціями тоді і тільки тоді, коли воно є розбиттям на суміжні класи за деяким ідеалом.*

Доведення. Якщо розбиття кільця R узгоджене з операціями, то з теореми 1.4.8 (про розбиття групи) випливає, що воно є розбиттям за деякою підгрупою \mathcal{I} адитивної групи кільця R . Покажемо, що ця підгрупа \mathcal{I} є ідеалом. Якщо $a, b \in \mathcal{I}$, то $-b \in \mathcal{I}$ і $a - b = a + (-b) \in \mathcal{I}$ за критерієм підгрупи. Далі, для будь-яких $c \in R$ і $a \in \mathcal{I}$ маємо $a \sim 0$, $c \sim c$, тому (розбиття узгоджене з операцією множення) $c \cdot a \sim c \cdot 0 = 0$, тобто $ca \in \mathcal{I}$. Отже, \mathcal{I} є ідеалом кільця R . Навпаки, якщо \mathcal{I} — ідеал кільця R , то розбиття групи R на суміжні класи за підгрупою \mathcal{I} узгоджене з операцією додавання за теоремою 1.4.8. Покажемо, що це розбиття узгоджене і з операцією множення. Нехай $a \sim a'$, $b \sim b'$. Тоді $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in \mathcal{I}$, бо $a - a', b - b' \in \mathcal{I}$. Це означає, що $ab \sim a'b'$, тобто розбиття узгоджене і з операцією множення. \square

Означення 1.5.5. Нехай $R/\mathcal{I} = \{a + \mathcal{I} \mid a \in R\}$ — множина

всіх суміжних класів кільця R за ідеалом \mathcal{I} . Позначимо (для скорочення) суміжний клас $a + \mathcal{I}$ через \bar{a} . Означимо на множині R/\mathcal{I} операції додавання і множення суміжних класів:

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Зауваження 1.5.2. З теореми 1.5.3 випливає, що ці означення додавання і множення суміжних класів є коректними: сума і добуток суміжних класів означаються за допомогою представників у цих класах, а теорема 1.5.3 гарантує, що ці операції залежать лише від суміжних класів, а не від конкретного вибору представників.

Твердження 1.5.4. *Множина R/\mathcal{I} є кільцем відносно визначених вище операцій додавання і множення суміжних класів.*

Доведення. Ми вже знаємо (тврдження 1.4.9), що R/\mathcal{I} є абелевою групою відносно додавання. Асоціативність множення та дистрибутивність в R/\mathcal{I} випливають з асоціативності множення та дистрибутивності в R . Обмежимося доведенням дистрибутивності: $(\bar{a} + \bar{b})\bar{c} = (\overline{a+b})\bar{c} = \overline{(a+b)c} = \overline{ac + bc} = \overline{ac} + \overline{bc} = \bar{a}\cdot\bar{c} + \bar{b}\cdot\bar{c}$. Зауважимо, що коли R — кільце з одиничним елементом 1, то й R/\mathcal{I} є кільцем з одиничним елементом $\bar{1} = 1 + \mathcal{I}$. \square

Означення 1.5.6. Кільце R/\mathcal{I} , елементами якого є суміжні класи кільця R за ідеалом \mathcal{I} , називається *фактор-кільцем* кільця R за ідеалом \mathcal{I} .

1.5.4. Кільце $\mathbb{Z}/n\mathbb{Z}$

Важливим прикладом фактор-кільця є так зване кільце класів лішків $\mathbb{Z}/n\mathbb{Z}$ — фактор-кільце кільця \mathbb{Z} за ідеалом $n\mathbb{Z}$, де $n > 1$. Поки що обмежуємося лише найелементарнішими властивостями цього фактор-кільця і розглядаємо його лише для того, щоб мати конкретний приклад фактор-кільця. Пізніше ми будемо вивчати фактор-кільце $\mathbb{Z}/n\mathbb{Z}$ більш детально, оскільки воно

відіграє важливу роль у теорії чисел. Елементами кільця класів лишків $\mathbb{Z}/n\mathbb{Z}$ є суміжні класи $\bar{a} = a + n\mathbb{Z}$, де $a \in \mathbb{Z}$. Позначимо через $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$ суміжні класи з представниками $0, 1, 2, \dots, n-1$. Виявляється, що ці суміжні класи вичерпують всі елементи кільця $\mathbb{Z}/n\mathbb{Z}$. Справді, з означення суміжних класів випливає, що для $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$. $\bar{a} = \bar{b}$ тоді і тільки тоді, коли $a - b \in n\mathbb{Z}$, тому суміжні класи $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$ всі різні. Далі, якщо $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ будь-який суміжний клас, то, розділивши a з остачею на n , одержимо $a = nd + r$ (тут $d = \left[\frac{a}{n} \right]$ — ціла частина дробу $\frac{a}{n}$, $r = a - nd$, $0 \leq r < n$), і $\bar{a} = \bar{nd+r} = \bar{nd} + \bar{r} = \bar{0} + \bar{r} = \bar{r} \in \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$. Розглянемо таблички додавання і множення для кільця класів лишків $\mathbb{Z}/5\mathbb{Z}$ і $\mathbb{Z}/6\mathbb{Z}$:

a) $\mathbb{Z}/5\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

б) $\mathbb{Z}/6\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$						
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Зауважимо, що в кільці $\mathbb{Z}/5\mathbb{Z}$ кожний ненульовий елемент має обернений відносно множення: $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{2} \cdot \bar{3} = \bar{1}$, $\bar{4} \cdot \bar{4} = \bar{1}$. У кільці $\mathbb{Z}/6\mathbb{Z}$ елементи $\bar{2}, \bar{3}$ і $\bar{4}$ не мають обернених відносно множення. Крім того, в $\mathbb{Z}/6\mathbb{Z}$ добуток ненульових елементів може

давати нульовий елемент ($\bar{2} \cdot \bar{3} = \bar{0}$), квадрат ненульового елемента, що не дорівнює $\bar{1}$, може давати цей самий елемент: $\bar{3}^2 = \bar{3}$. Є їй інші незвичні властивості множення в $\mathbb{Z}/6\mathbb{Z}$. Той факт, що в $\mathbb{Z}/5\mathbb{Z}$ кожний ненульовий елемент має обернений відносно множення, допускає узагальнення.

Твердження 1.5.5. *Нехай p — просте число, $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$, $\bar{a} \neq \bar{0}$. Тоді існує елемент $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$ такий, що $\bar{a} \cdot \bar{b} = \bar{1}$.*

Доведення. Розглянемо головний ідеал $(\bar{a}) = \bar{a} \cdot \mathbb{Z}/p\mathbb{Z}$, породжений елементом \bar{a} (пригадайте приклад 3 з п. 1.5.1). Цей ідеал містить ненульові елементи ($\bar{a} \in (\bar{a})$) і за твердженням 1.5.2 є підкільцем кільця $\mathbb{Z}/p\mathbb{Z}$, отже, є підгрупою адитивної групи $\mathbb{Z}/p\mathbb{Z}$. За наслідком 1.4.6 з теореми Лагранжа (п. 1.4.3) $(\bar{a}) = \mathbb{Z}/p\mathbb{Z}$. Звідси випливає, що знайдеться $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$, для якого $\bar{a} \cdot \bar{b} = \bar{1}$. \square

1.5.5. Поле

Означення 1.5.7. Комутативне кільце P з одиничним елементом $1 \neq 0$ називається *полем*, якщо для кожного ненульового елемента з P існує обернений відносно множення.

Приклад 1.5.4. 1) Множина \mathbb{Q} раціональних чисел і множина \mathbb{R} дійсних чисел є полями відносно звичайних операцій додавання і множення.

2) Кільце класів лишків $\mathbb{Z}/p\mathbb{Z}$ є полем тоді і тільки тоді, коли p -просте число. Якщо p — просте число, то згідно твердження 1.5.5 фактор-кільце $\mathbb{Z}/p\mathbb{Z}$ є полем. Якщо p не є простим числом, то $\mathbb{Z}/n\mathbb{Z}$ не є полем. Справді, у цьому випадку $n = n_1 \cdot n_2$, де $1 < n_1, n_2 < n$. $\bar{n} = \bar{n}_1 \cdot \bar{n}_1 = \bar{0}$ і $\bar{n}_1 \neq \bar{0}$, $\bar{n}_2 \neq \bar{0}$. Якби для \bar{n}_1 існував обернений \bar{n}_1^{-1} , то ми мали б $\bar{n}_1^{-1} \cdot \bar{n}_1 \cdot \bar{n}_2 = \bar{n}_1^{-1} \cdot \bar{0} = \bar{0}$, тобто $\bar{1} \cdot \bar{n}_2 = \bar{n}_2 = \bar{0}$ — суперечність.

Таким чином, вірне наступне твердження:

Твердження 1.5.6. $\mathbb{Z}/n\mathbb{Z}$ — поле тоді і тільки тоді, коли n — просте число.

1.5.6. Гомоморфізми кілець та полів

Означення 1.5.8. Нехай R_1 і R_2 — кільця. Відображення $f: R_1 \rightarrow R_2$ називається *гомоморфізмом* кілець, якщо $f(a + b) = f(a) + f(b)$ і $f(ab) = f(a)f(b)$.

З означення випливає, що $f(0_1) = 0_2$, де 0_1 і 0_2 , відповідно, нульові елементи кілець R_1 і R_2 (див. твердження 1.4.1).

Означення 1.5.9. *Гомоморфізмом полів* P_1 і P_2 називають відображення $f: P_1 \rightarrow P_2$, для якого $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ і $f(1_1) = 1_2$, де 1_1 та 1_2 одиничні елементи в P_1 та P_2 відповідно.

Приклад 1.5.5. 1) Нехай R — кільце, \mathcal{I} — ідеал в R . Розглянемо відображення $f: R \rightarrow R/\mathcal{I}$ кільця R у фактор-кільце R/\mathcal{I} , для якого $f(a) = \bar{a}$. Тоді $f(a + b) = \overline{a + b} = \bar{a} + \bar{b} = f(a) + f(b)$ і $f(ab) = \overline{ab} = \bar{a} \cdot \bar{b} = f(a)f(b)$. Отже, відображення f є гомоморфізмом кілець R і R/\mathcal{I} . Цей гомоморфізм називають *канонічним гомоморфізмом*.

2) Відображення кільця цілих чисел в поле раціональних чисел $f: \mathbb{Z} \rightarrow \mathbb{Q}$ таке, що $f(n) = n$, є, очевидно, гомоморфізмом.

Означення 1.5.10. *Ізоморфізмом кілець (полів)* називають біективний гомоморфізм.

Приклад 1.5.6. 1) Однічне відображення будь-якого кільця (поля) в себе є, очевидно, ізоморфізмом.

2) Відображення $f: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$, для якого $f(a + b\sqrt{2}) = a - b\sqrt{2}$, є ізоморфізмом поля $\mathbb{Q}(\sqrt{2})$ в себе. Справді, біективність тут очевидна. $f((a + b\sqrt{2})(c + d\sqrt{2})) = f(ac + 2bd + (ad + bc)\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = f(a - b\sqrt{2})f(c - d\sqrt{2})$. Ще легше перевіряється, що $f((a + b\sqrt{2}) + (c + d\sqrt{2})) = f(a + b\sqrt{2}) + f(c + d\sqrt{2})$.

Ідеали кілець тісно пов'язані з гомоморфізмами.

Означення 1.5.11. Нехай $f: R_1 \rightarrow R_2$ — гомоморфізм кільцець. Підмножина $\text{Ker } f = \{x \in R_1 \mid f(x) = 0\}$ кільця R_1 називається *ядром гомоморфізму* f .

Твердження 1.5.7. а) Ядро гомоморфізму кільцець $f: R_1 \rightarrow R_2$ є ідеалом кільця R_1 .

б) Якщо \mathcal{I} — ідеал кільця R , то \mathcal{I} є ядром канонічного гомоморфізму $f: R \rightarrow R/\mathcal{I}$, $f(a) = \bar{a}$.

Доведення. а) Якщо $a, b \in \text{Ker } f$, то $f(a - b) = f(a) - f(b) = 0 - 0 = 0$, тому $a - b \in \text{Ker } f$. Якщо, крім цього, $c \in R$, то $f(ca) = f(c)f(a) = f(c) \cdot 0 = 0$. Це означає, що $ca \in \text{Ker } f$.

б) $\text{Ker } f = \{a \in R \mid \bar{a} = \bar{0}\} = \{a \in R \mid a \in \mathcal{I}\} = \mathcal{I}$. \square

Твердження 1.5.8. Гомоморфізм полів є завжди ін'єктивним відображенням.

Доведення. Перш за все, ядро гомоморфізму полів $f: P_1 \rightarrow P_2$ є ідеалом в полі P_1 . Але ми знаємо, що в P_1 є лише два ідеали (0) і P_1 . $\text{Ker } f \neq P_1$ тому, що $f(1) = 1$ і $1 \notin \text{Ker } f$. Отже, ядро гомоморфізму полів складається лише з 0 . Тепер, якщо $f(a_1) = f(a_2)$, то, оскільки f — гомоморфізм, $f(a_1 - a_2) = 0$, $a_1 - a_2 \in \text{Ker } f = (0)$ і $a_1 = a_2$. Отже, f — ін'єктивне відображення. \square

1.6. Матриці

1.6.1. Означення

Нехай R — кільце. *Матрицею* з елементами з кільця R називається прямокутна таблиця

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad (1.6.1)$$

де $a_{ij} \in R$, $1 \leq i \leq m$, $1 \leq j \leq n$. Матриця (1.6.1) має m рядків і n стовпчиків; кажуть ще, що вона має розмір $m \times n$. Матриці прийнято позначати великими буквами латинського алфавіту $A, B, \dots, A_1, A_2, \dots, X, Y, Z$. Елементи $a_{ij} \in R$, що входять в матрицю (1.6.1), називають *елементами матриці*. Елемент a_{ij} розміщений на перетині i -го рядка і j -го стовпчика матриці (1.6.1). Матрицю вигляду (1.6.1) позначають ще $[a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$, або коротше $[a_{ij}]$. Множину всіх матриць розміру $m \times n$ з елементами кільця R позначають $M_{m,n}(R)$:

$$M_{m,n}(R) = \{[a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n} \mid a_{ij} \in R\}.$$

Якщо $m = 1$, то матриця (1.6.1) складається з одного рядка; її називають *матрицею-рядком* або просто *рядком*. Аналогічно при $n = 1$ маємо *матрицею-стовпчик* або просто *стовпчик*. Якщо $m = n$, то матрицю (1.6.1) називають *квадратною матрицею порядку n* . Множину всіх квадратних матриць порядку n з елементами з кільця R позначають $M_n(R)$. Дві матриці A і B називаються *рівними*, якщо вони мають однакові розміри і однакові відповідні елементи:

$$[a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n} = [b_{ij}]_{1 \leq i \leq k, 1 \leq j \leq l},$$

якщо $m = k$, $n = l$ і $a_{ij} = b_{ij}$ для всіх значень i та j .

1.6.2. Лінійні операції над матрицями

Означимо на множині матриць $M_{m,n}(R)$ алгебраїчну операцію додавання матриць і операцію множення матриць на елементи з кільця R (операцію множення на скаляри). Нехай $A = [a_{ij}]$, $B = [b_{ij}]$; $A, B \in M_{m,n}(R)$, $\lambda \in R$.

Означення 1.6.1. *Сумою* матриць $[a_{ij}]$ та $[b_{ij}]$ називається матриця, на перетині i -го рядка та j -го стовпчика якої стоїть елемент $a_{ij} + b_{ij}$:

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}].$$

Добутком матриці $[a_{ij}]$ на скаляр $\lambda \in R$ називається матриця, на перетині i -го рядка та j -го стовпчика якої стоїть елемент λa_{ij} :

$$\lambda[a_{ij}] = [\lambda a_{ij}].$$

Додавання матриць та множення матриць на скаляри називають *лінійними операціями над матрицями*. *Нульовою матрицею* $O \in M_{m,n}(R)$ назовемо матрицю, всі елементи якої дорівнюють нулю кільця R . Для матриці $A = [a_{ij}]$ через $-A$ позначимо матрицю $[-a_{ij}]$, елементи якої є оберненими відносно додавання до елементів $a_{ij} \in R$.

Нехай $A, B, C \in M_{m,n}(R)$; $\lambda, \mu \in R$.

Твердження 1.6.1. *Лінійні операції над матрицями мають такі властивості:*

- 1) $A + B = B + A$,
- 2) $(A + B) + C = A + (B + C)$,
- 3) $A + O = A$,
- 4) $A + (-A) = O$,
- 5) $\lambda(\mu A) = (\lambda\mu)A$,
- 6) $(\lambda + \mu)A = \lambda A + \mu A$,
- 7) $\lambda(A + B) = \lambda A + \lambda B$,
- 8) $1 \cdot A = A$, якщо кільце R є кільцем з одиничним елементом

1.

Доведення. Обмежимося доведенням, наприклад, властивості 7):

$$\begin{aligned}\lambda(A + B) &= \lambda([a_{ij}] + [b_{ij}]) = \lambda[a_{ij} + b_{ij}] = [\lambda(a_{ij} + b_{ij})] = \\ &= [\lambda a_{ij} + \lambda b_{ij}] = [\lambda a_{ij}] + [\lambda b_{ij}] = \lambda[a_{ij}] + \lambda[b_{ij}] = \lambda A + \lambda B.\end{aligned}$$

Пропонуємо інші властивості довести самостійно. □

1.6.3. Добуток матриць

Нехай $A = (a_1, a_2, \dots, a_n)$ — матриця-рядок, а $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ — матриця-стовпчик, $A \in M_{1,n}(R)$, $B \in M_{n,1}(R)$. Тоді добутком

матриць A і B називають елемент $a_1b_1 + a_2b_2 + \dots + a_nb_n = \sum_{k=1}^n a_k b_k \in R$ (цей елемент можна вважати квадратною матрицею порядку 1). Далі ми будемо використовувати символ суми $\sum_{i=1}^k a_i$ для позначення суми $a_1 + a_2 + \dots + a_k$ декількох елементів кільця R . У наступній лемі наведені корисні рівності, що містять символ \sum .

Лема 1.6.1. Нехай $a, a_i, a_{ij} \in R$. Тоді

- 1) $a \sum_{i=1}^k a_i = \sum_{i=1}^k aa_i;$
- 2) $\sum_{j=1}^l (\sum_{i=1}^k a_{ij}) = \sum_{i=1}^k (\sum_{j=1}^l a_{ij}).$

Доведення. Рівність 1) є узагальненням властивості дистрибутивності в кільці R і може бути доведена методом математичної індукції (доведіть самостійно). Для доведення рівності 2) розглянемо матрицю

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{21} & a_{22} & \dots & a_{2l} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kl} \end{pmatrix} \in M_{k,l}(R).$$

Суму $\sum_{j=1}^l (\sum_{i=1}^k a_{ij})$ можна трактувати як суму сум елементів всіх стовпчиків матриці A . Вона дорівнює сумі всіх елементів матриці A . Так само, сума $\sum_{i=1}^k (\sum_{j=1}^l a_{ij})$ є сумою сум елементів всіх рядків матриці A ; вона теж дорівнює сумі всіх елементів матриці A . \square

Означення 1.6.2. Нехай $A = [a_{ij}] \in M_{m,l}(R)$, $B = [b_{ij}] \in M_{l,n}(R)$. Матриця $C = [c_{ij}] \in M_{m,n}(R)$ називається *добутком матриць* A і B (її позначають $C = AB$), якщо $c_{ij} = \sum_{k=1}^l a_{ik} b_{kj}$.

Зауваження 1.6.1. Не кожні дві матриці A і B можна перемножити. Добуток AB матриці A і B визначений лише тоді, коли матриці A і B мають підходжі розміри, а саме, кількість стовпчиків матриці A повинна дорівнювати кількості рядків матриці B . Матриця-добуток AB має стільки рядків, скільки їх має A і стільки стовпчиків, скільки їх має B . Схематично це зображенено на мал. ??

Приклад 1.6.1.

$$1) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 & ay_1 + by_2 & az_1 + bz_2 \\ cx_1 + dx_2 & cy_1 + dy_2 & cz_1 + dz_2 \end{pmatrix},$$

де $a, b, c, d, x_1, x_2, y_1, y_2, z_1, z_2$ — елементи деякого кільцева R .

Добуток цих матриць у зворотному порядку не визначений.

$$2) \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} (2, 3, 4, 5) = \begin{pmatrix} 1 \cdot 2 & 1 \cdot 3 & 1 \cdot 4 & 1 \cdot 5 \\ 2 \cdot 2 & 2 \cdot 3 & 2 \cdot 4 & 2 \cdot 5 \\ 3 \cdot 2 & 3 \cdot 3 & 3 \cdot 4 & 3 \cdot 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 4 & 6 & 8 & 10 \\ 6 & 9 & 12 & 15 \end{pmatrix},$$

$$(2, 3, 4, 5) \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 2 + 6 + 4 + 15 = 27.$$

$$3) A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 2 & -1 \\ 5 & 4 \end{pmatrix}, AB = \begin{pmatrix} 7 & 3 \\ 19 & 10 \end{pmatrix}, BA = \begin{pmatrix} 0 & -1 \\ 13 & 17 \end{pmatrix}.$$

Приклад 1) показує, що коли добуток AB визначений, то добуток BA визначений не завжди. Крім цього, приклади 2) і 3) показують, що коли навіть обидва добутки AB і BA визначені, то, взагалі кажучи, $AB \neq BA$.

Твердження 1.6.2. Нехай A, B і C — три матриці підходящих розмірів, тобто $A \in M_{m,p}(R)$, $B \in M_{p,q}(R)$, $C \in M_{q,n}(R)$. Тоді

$$(AB)C = A(BC). \quad (1.6.2)$$

Доведення. Оскільки $A \in M_{m,p}(R)$, $B \in M_{p,q}(R)$, $C \in M_{q,n}(R)$, то $AB \in M_{m,q}(R)$, $BC \in M_{p,n}(R)$, і всі добутки, що входять в (1.6.2), визначені. Рівність (1.6.2) випливає з такого обчислення:

$$\begin{aligned} (AB)C &= ([a_{ij}] \cdot [b_{ij}])[c_{ij}] = \left[\sum_{k=1}^p a_{ik} b_{kj} \right] \cdot [c_{ij}] = \\ &= \left[\sum_{l=1}^q \left(\left(\sum_{k=1}^p a_{ik} b_{kl} \right) c_{lj} \right) \right] = \left[\sum_{l=1}^q \left(\sum_{k=1}^p a_{ik} b_{kl} c_{lj} \right) \right] = \\ &= \left[\sum_{k=1}^p \left(\sum_{l=1}^q a_{ik} b_{kl} c_{lj} \right) \right] = \left[\sum_{k=1}^p a_{ik} \left(\sum_{l=1}^q b_{kl} c_{lj} \right) \right] = A(BC). \end{aligned}$$

Тут четверта і передостання рівності випливають з твердження 1) леми 1.6.1, п'ята — з твердження 2) цієї ж леми, а решта — з означення добутку матриць (крім першої рівності, яка вводить позначення для елементів наших матриць). \square

Твердження 1.6.3. Нехай $A \in M_{m,p}(R)$, $B, C \in M_{p,n}(R)$, $D \in M_{n,r}(R)$. Тоді

$$A(B + C) = AB + AC, \quad (1.6.3)$$

$$(B + C)D = BD + CD. \quad (1.6.4)$$

Доведення. Обмежимося доведенням властивості (1.6.3), а властивість (1.6.4) пропонуємо довести читачеві. Нехай $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}]$.

$$\begin{aligned} A(B + C) &= \left[\sum_{k=1}^p a_{ik}(b_{kj} + c_{kj}) \right] = \left[\sum_{k=1}^p (a_{ik}b_{kj} + a_{ik}c_{kj}) \right] = \\ &= \left[\sum_{k=1}^p a_{ik}b_{kj} + \sum_{k=1}^p a_{ik}c_{kj} \right] = \left[\sum_{k=1}^p a_{ik}b_{kj} \right] + \left[\sum_{k=1}^p a_{ik}c_{kj} \right] = AB + BC. \end{aligned}$$

\square

1.6.4. Одинична та транспонована матриці

Нехай R — кільце з 1.

Означення 1.6.3. Одиничною матрицею $E_n \in M_n(R)$ називається матриця вигляду

$$E_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

На головній діагоналі цієї матриці стоїть одиничний елемент кільця R , а на всіх інших місцях — нуль кільця R . Як правило,

індекс n в позначенні одиничної матриці пропускають і пишуть просто E . Одиничну матрицю зручно записувати за допомогою символу Кронекера δ_{ij} :

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

Отже, $E_n = [\delta_{ij}]$.

Твердження 1.6.4. Нехай $A \in M_{m,n}(R)$. Тоді

$$AE_n = A, \quad E_m A = A. \quad (1.6.5)$$

Доведення. Доведемо першу з рівностей (1.6.5), а другу залишимо читачеві. $AE_n = [\sum_{k=1}^n a_{ik} \delta_{kj}]$. Тепер $\delta_{kj} = 1$ при $k = j$ і $\delta_{kj} = 0$ у всіх інших випадках. Тому сума $\sum_{k=1}^n a_{ik} \delta_{kj}$ зводиться до одного доданка a_{ij} і $AE_n = [a_{ij}] = A$. \square

Означення 1.6.4. Нехай $A = [a_{ij}] \in M_{m,n}(R)$. Матриця $A' = [a'_{ij}] \in M_{n,m}(R)$ називається *транспонованою* до A , якщо $a'_{ij} = a_{ji}$.

Приклад 1.6.2. $\begin{pmatrix} 1 & 9 & 9 & 5 \\ 1 & 7 & 0 & 1 \end{pmatrix}' = \begin{pmatrix} 1 & 1 \\ 9 & 7 \\ 9 & 0 \\ 5 & 1 \end{pmatrix}.$

Твердження 1.6.5. Нехай $A \in M_{m,p}(R)$, $B \in M_{p,n}(R)$. Тоді $(AB)' = B'A'$ за умови, що кільце R комутативне.

Доведення. Перш за все ясно, що матриці $(AB)'$ і $B'A'$ мають однакові розміри: $(AB)' \in M_{n,m}(R)$. Залишається перевірити, що їх відповідні елементи рівні між собою. Нехай $(AB)' = [c_{ij}]$. За означенням транспонування c_{ij} дорівнює добутку j -го рядка матриці A на i -ий стовпчик матриці B : $c_{ij} = \sum_{k=1}^p a_{jk} b_{ki}$. Якщо $B'A' = [d_{ij}]$, то елемент d_{ij} дорівнює добутку i -го стовпчика матриці B на j -ий рядок матриці A : $d_{ij} = \sum_{k=1}^p b_{ki} a_{jk} = \sum_{k=1}^p a_{jk} b_{ki}$. Отже, $c_{ij} = d_{ij}$, що й потрібно було довести. \square

1.6.5. Кільце матриць

Нехай R — будь-яке кільце. Розглянемо множину $M_n(R)$ квадратних матриць порядку n з елементами з кільця R . Сума і добуток двох матриць з $M_n(R)$ знову належать до $M_n(R)$, тому операції додавання і множення матриць є алгебраїчними операціями на множині $M_n(R)$.

Твердження 1.6.6. *Множина $M_n(R)$ квадратних матриць з коефіцієнтами з кільця R є кільцем відносно операцій додавання і множення матриць.*

Доведення. З твердження 1.6.1 випливає, що $M_n(R)$ є абелевою групою відносно додавання. Множення матриць асоціативне за твердженням 1.6.2, і множення зв'язане з додаванням законами дистрибутивності за твердженням 1.6.3. Якщо R — кільце з 1, то $M_n(R)$ — теж кільце з 1. Роль одиничного елемента в кільці $M_n(R)$ відіграє одинична матриця. \square

1.7. комплексні числа

1.7.1. Поле комплексних чисел

Спочатку означимо комплексні числа як множину, тоді введемо на цій множині дві алгебраїчні операції і доведемо, що множина комплексних чисел є полем відносно введених операцій, і це поле містить підполе, ізоморфне полю дійсних чисел.

Означення 1.7.1. Назовемо множиною комплексних чисел \mathbb{C} множину всіх впорядкованих пар дійсних чисел:

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Отже, комплексне число $z \in \mathbb{C}$ — це впорядкована пара дійсних чисел $z = (a, b)$. комплексне число ще можна трактувати як матрицю-рядок з дійсними елементами: $(a, b) \in M_{1,2}(\mathbb{R})$.

Введемо на множині \mathbb{C} операції додавання і множення.

Означення 1.7.2. Якщо $(a, b), (c, d) \in \mathbb{C}$, то

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d), \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc).\end{aligned}$$

Твердження 1.7.1. *Множина комплексних чисел \mathbb{C} є полем відносно означеных вище алгебраїчних операцій. Поле \mathbb{C} містить підполе R' , ізоморфне полю дійсних чисел \mathbb{R} .*

Доведення. Множина \mathbb{C} є абелевою групою відносно додавання. Це випливає з того, що комплексні числа додаються по-компонентно (як матриці), а за твердженням 1.6.1 матриці заданого розміру утворюють абелеву групу відносно додавання. Покажемо, що множення комплексних чисел асоціативне. Нехай $z_1 = (a, b), z_2 = (c, d), z_3 = (e, f)$ — три комплексні числа. Тоді

$$\begin{aligned}(z_1 z_2) z_3 &= ((a, b)(c, d))(e, f) = (ac - bd, ad + bc)(e, f) = \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce) \\ z_1(z_2 z_3) &= (a, b)((c, d)(e, f)) = (a, b)(ce - df, cf + de) = \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce).\end{aligned}$$

Порівнюючи результати цих обчислень, бачимо, що $(z_1 z_2) z_3 = z_1(z_2 z_3)$. З означення множення комплексних чисел легко видно, що множення комутативне. Для множення існує нейтральний елемент — комплексне число $(1, 0)$. Справді, $(a, b)(1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b)$. Перевіримо, що множення зв'язане з додаванням законом дистрибутивності. Нехай $z_1, z_2, z_3 \in \mathbb{C}$.

$$\begin{aligned}(z_1 + z_2) z_3 &= ((a, b) + (c, d))(e, f) = (a + c, b + d)(e, f) = \\ &= ((a + c)e - (b + d)f, (a + c)f + (b + d)e) = \\ &= (ae + ce - bf - df, af + cf + be + de) = \\ &= (ae - bf, af + be) + (ce - df, cf + de) = \\ &= (a, b)(e, f) + (c, d)(e, f) = z_1 z_3 + z_2 z_3.\end{aligned}$$

Отже, перевірено, що множина \mathbb{C} є комутативним кільцем з одиничним елементом. Щоб довести, що \mathbb{C} є полем, залишилося перевірити, що кожний ненульовий елемент $z \in \mathbb{C}$ має обернений відносно множення. Нехай $z = (a, b) \in \mathbb{C}$, $z \neq 0$, отже, a і b не дорівнюють нулю одночасно. Тоді $a^2 + b^2 \neq 0$. Розглянемо комплексне число $z' = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ і обчислимо добуток zz' .

$$\begin{aligned} zz' &= (a, b) \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) = \\ &= \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ab}{a^2+b^2} \right) = (1, 0). \end{aligned}$$

Отже, елемент $z' = z^{-1}$ — обернений до z . Залишається довести, що поле \mathbb{C} містить підполе R' , ізоморфне полю дійсних чисел. Позначимо через R' наступну підмножину множини \mathbb{C} : $R' = \{(a, 0) \mid a \in \mathbb{R}\}$. Операції додавання і множення в \mathbb{C} , застосовані до елементів з R' , не виводять за межі множини R' :

$$\begin{aligned} (a_1, 0) + (a_2, 0) &= (a_1 + a_2, 0), \\ (a_1, 0)(a_2, 0) &= (a_1 a_2, 0). \end{aligned}$$

Нейтральні елементи $(0, 0)$ відносно додавання і $(1, 0)$ відносно множення належать до R' . Так само елементи $(-a, 0)$ і $(a^{-1}, 0)$ ($a \neq 0$), які обернені до елементів з R' , знову належать до R' . Звідси випливає, що множина R' є полем. Перевіримо, що поле R' ізоморфне полю дійсних чисел \mathbb{R} . Для цього розглянемо відображення $f: \mathbb{R} \rightarrow R'$, для якого $f(a) = (a, 0)$. Очевидно, відображення f — біективне, переводить 0 в $(0, 0)$ і 1 в $(1, 0)$. Крім того,

$$\begin{aligned} f(a_1 + a_2) &= (a_1 + a_2, 0) = (a_1, 0) + (a_2, 0) = f(a_1) + f(a_2), \\ f(a_1 a_2) &= (a_1 a_2, 0) = (a_1, 0)(a_2, 0) = f(a_1)f(a_2). \end{aligned}$$

Отже, відображення f є ізоморфізмом \mathbb{R} і R' , і це завершує доказування. \square

1.7.2. Алгебраїчна форма комплексних чисел

В процесі доведення твердження 1.7.1 був побудований ізоморфізм поля дійсних чисел \mathbb{R} і підполя $R' = \{(a, 0) \mid a \in \mathbb{R}\}$ поля комплексних чисел \mathbb{C} . Використовуючи цей ізоморфізм, ототожнимо кожне комплексне число вигляду $(a, 0)$ з дійсним числом a . В результаті такого ототожнення можна вважати, що саме поле дійсних чисел \mathbb{R} є підполем поля \mathbb{C} (кажуть також, що поле \mathbb{C} є розширенням поля \mathbb{R}). Позначимо комплексне число $(0, 1)$ через i . Знайдемо квадрат числа i : $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$ (остання рівність справедлива в силу нашої домовленості ототожнювати комплексні числа $(a, 0)$ з дійсними числами a). Бачимо, що $i^2 = -1$. Звичайно, $(-i)^2$ теж дорівнює -1 . Це означає, що в полі комплексних чисел многочлен $x^2 + 1$ має два корені $\pm i$. Зауважимо, що *основна теорема алгебри*, яку буде доведено пізніше, стверджує, що кожний многочлен степеня більшого або рівного 1 з комплексними (зокрема з дійсними) коефіцієнтами має хоч один комплексний корінь.

Розглянемо тепер будь-яке комплексне число $z = (a, b) \in \mathbb{C}$. Очевидно, що $z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$. Нагадаємо, що ми домовилися ототожнювати $(a, 0)$ з a , $(b, 0)$ з b , а $(0, 1)$ позначили буквою i . Запис комплексного числа (a, b) у вигляді $a + bi$, де $a, b \in \mathbb{R}$, називають *звичайною (або алгебраїчною) формою комплексного числа*. Дії над комплексними числами, записаними у звичайній формі, виконують за такими ж правилами, як у середній школі над алгебраїчними виразами. Іні правила, по-суті, випливають з аксіом поля. Звичайно, крім цього, використовується ще той факт, що $i^2 = -1$.

Приклад 1.7.1.

$$\begin{aligned} \frac{(3+5i)^3}{1-2i} &= \frac{3^3 + 3 \cdot 3^2 \cdot 5i + 3 \cdot 3 \cdot 25i^2 + 125i^3}{1-2i} = \frac{27 + 135i - 225 - 125i}{1-2i} = \\ &= \frac{-198 + 10i}{1-2i} = \frac{(-198 + 10i)(1+2i)}{(1-2i)(1+2i)} = \frac{-198 + 10i - 296i - 20}{5} = \\ &= \frac{-218 - 286i}{5} = -\frac{2}{5}(109 + 143i). \end{aligned}$$

Означення 1.7.3. Нехай $z = a + bi$. Тоді a називають *дійсною частиною* числа z , а bi — *уявною частиною*. Дійсну і уявну частину числа z позначають, відповідно, $\operatorname{Re} z$ та $\operatorname{Im} z$.

1.7.3. Геометрична інтерпретація

Розглянемо площину з декартовою системою координат (див. мал. ??). комплексному числу $z = a + bi$ поставимо у відповідність точку площини з координатами a і b (або вектор із початком у початку координат і з кінцем у точці з абсцисою a і ординатою b).

Зрозуміло, що це зображення комплексних чисел точками площини (або векторами) задає біективну відповідність між множиною \mathbb{C} і множиною точок площини (або векторів з початком в точці $(0, 0)$). При такому зображення комплексних чисел точками площини дійсні числа відповідають точкам осі абсцис Ox , яку тому часто називають *дійсною віссю* комплексної площини. Нехай маємо два комплексних числа $z_1 = a_1 + b_1i$ і $z_2 = a_2 + b_2i$. На комплексній площині цим числам відповідають два вектори (див. мал. ??).

Комплексному числу $z_1 + z_2 = a_1 + a_2 + (b_1 + b_2)i$ відповідає вектор-діагональ паралелограма, побудованого на векторах, відповідних числам z_1 і z_2 , як на сторонах. Отже, якщо комплексні числа інтерпретувати векторами, то сума комплексних чисел інтерпретується сумою векторів.

1.7.4. Модуль та аргумент

Означення 1.7.4. Якщо $z = a + bi$ — комплексне число, то комплексне число $\bar{z} = a - bi$ називається *спряженним* до z .

Правило $f(z) = \bar{z}$ задає відображення $f: \mathbb{C} \rightarrow \mathbb{C}$. Легко бачимо, що для відображення f існує обернене $f^{-1} = f$ (справді $f \circ f^{-1} = 1_{\mathbb{C}}$), тому f — біективне відображення. Ізоморфізм будь-якого поля в себе називають *автоморфізмом* цього поля.

Виявляється, що комплексне спряження є автоморфізмом поля \mathbb{C} .

Твердження 1.7.2. *Відображення $f: \mathbb{C} \rightarrow \mathbb{C}$, $f(z) = \bar{z}$ є автоморфізмом поля \mathbb{C} .*

Доведення. Досить показати, що $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ і $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. Перевіримо другу рівність, а перевірку першої залишимо читачеві. Нехай $z_1 = a + bi$, $z_2 = c + di$.

$$\begin{aligned}\overline{z_1 \cdot z_2} &= \overline{(a+bi)(c+di)} = \overline{ac - bd + (ad + bc)i} = \\ &= ac - bd - (ad + bc)i = (a - bi)(c - di) = \overline{z_1} \cdot \overline{z_2}.\end{aligned}$$

□

Нехай $z = a + bi$, тоді $z\bar{z} = (a+bi)(a-bi) = a^2 + b^2$ — невід'ємне дійсне число.

Означення 1.7.5. Дійсне число $|z| = \sqrt{z\bar{z}}$ називається *модулем комплексного числа z* . Ясно, що $|z| = \sqrt{a^2 + b^2}$, якщо $z = a + bi$, тому $|z|$ можна геометрично інтерпретувати як довжину вектора, що відповідає числу z .

Означення 1.7.6. Нехай $z = a + bi$ — ненульове комплексне число. Дійсне число ϕ , для якого $\cos \phi = \frac{a}{\sqrt{a^2+b^2}}$ і $\sin \phi = \frac{b}{\sqrt{a^2+b^2}}$, називається *аргументом комплексного числа z* і позначається $\arg z$.

Зauważення 1.7.1. Число $\phi = \arg z$ можна знайти для будь-якого ненульового числа $z \in \mathbb{C}$. Це випливає з того, що $-1 \leq \frac{a}{\sqrt{a^2+b^2}} \leq 1$, $-1 \leq \frac{b}{\sqrt{a^2+b^2}} \leq 1$ і $\left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1$. Зauważимо також, що $\arg z$ визначається числом z неоднозначно. Існує безліч дійсних чисел ϕ , які задовільняють попередньому означенню. Всі вони відрізняються між собою на число, кратне 2π — періоду функцій $\cos \phi$ і $\sin \phi$. Можна уникнути цієї неоднозначності, якщо домовитися вибирати $\arg z$ у якому-небудь проміжку довжини 2π , наприклад, у проміжку $[0, 2\pi)$. Геометрично $\arg z$ є кутом між додатним напрямком дійсної осі комплексної площини і вектором, що відповідає числу z .

Твердження 1.7.3. Модуль комплексного числа має такі властивості:

- 1) $|z| \geq 0$, $|z| = 0 \Leftrightarrow z = 0$,
- 2) $|z_1 z_2| = |z_1||z_2|$,
- 3) $|z_1 + z_2| \leq |z_1| + |z_2|$,
- 4) $||z_1| - |z_2|| \leq |z_1 + z_2|$.

Доведення. Властивість 1) очевидна, а властивість 2) випливає з такого обчислення:

$$\begin{aligned} |z_1 z_2| &= \sqrt{(z_1 z_2) \overline{z_1 z_2}} = \sqrt{z_1 z_2 \overline{z_1 z_2}} = \sqrt{(z_1 \overline{z_1})(z_2 \overline{z_2})} = \\ &= \sqrt{z_1 \overline{z_1}} \cdot \sqrt{z_2 \overline{z_2}} = |z_1| \cdot |z_2|. \end{aligned}$$

Для доведення нерівності 3 зауважимо, що для всіх дійсних чисел a і b

$$a \leq \sqrt{a^2 + b^2}. \quad (1.7.1)$$

Нерівність (1.7.1) очевидна, якщо $a < 0$ і рівносильна очевидній нерівності $a^2 \leq a^2 + b^2$, якщо $a \geq 0$. Повертаючись до нерівності 3), доведемо спочатку, що

$$|1 + z| \leq 1 + |z|. \quad (1.7.2)$$

Справді, $|1 + z| = \sqrt{(1 + z)(1 + \bar{z})}$. Звідси

$$\begin{aligned} |1 + z|^2 &= (1 + z)(1 + \bar{z}) = 1 + (z + \bar{z}) + |z|^2 = 1 + 2\operatorname{Re} z + |z|^2 \leq \\ &\leq 1 + 2|z| + |z|^2 = (1 + |z|)^2. \end{aligned}$$

В цьому обчисленні використано нерівність $\operatorname{Re} z \leq |z|$, тобто нерівність (1.7.1) для $z = a + bi$. Ми одержали $|1 + z|^2 \leq (1 + |z|)^2$. Добуваючи квадратний корінь з обох частин, одержимо нерівність (1.7.2), яка є частковим випадком властивості 3). Покажемо, що властивість 3 випливає з нерівності (1.7.2). Можемо вважати, що $z_1 \neq 0$. Тоді

$$|z_1 + z_2| = |z_1| \left| 1 + \frac{z_2}{z_1} \right| \leq |z_1| \left(1 + \frac{|z_2|}{|z_1|} \right) = |z_1| + |z_2|$$

і властивість 3) доведена. Залишається довести властивість 4). Маємо $|z_1| = |z_1 + z_2 - z_2| \leq |z_1 + z_2| + |-z_2| = |z_1 + z_2| + |z_2|$. Звідси

$$|z_1| - |z_2| \leq |z_1 + z_2|. \quad (1.7.3)$$

Так само (міняючи ролями z_1 і z_2) показуємо, що

$$|z_2| - |z_1| \leq |z_1 + z_2|. \quad (1.7.4)$$

З (1.7.3) і (1.7.4) випливає те, що потрібно. \square

Зауваження 1.7.2. Якщо комплексне число z є дійсним ($\operatorname{Im} z = 0$), то його модуль $|z|$ збігається з відомим з курсу середньої школи модулем (абсолютною величиною) дійсного числа. Твердження 1.7.3 свідчить про те, що відомі властивості модуля дійсного числа зберігаються і для модуля комплексного числа. Зауважимо ще, що властивість $|z_1 + z_2| \leq |z_1| + |z_2|$ має наступну геометричну інтерпретацію: довжина сторони трикутника не перевищує суми довжин двох його інших сторін.

1.7.5. Тригонометрична форма комплексного числа

Нехай $z = a + bi$ — ненульове комплексне число, $\phi = \arg z$. Перепишемо z у вигляді

$$z = \sqrt{a^2 + b^2} \left(\frac{a}{\sqrt{a^2 + b^2}} + \frac{bi}{\sqrt{a^2 + b^2}} \right) = |z|(\cos \phi + i \sin \phi).$$

Означення 1.7.7. Вираз $|z|(\cos \phi + i \sin \phi)$ називають *тригонометричною формою комплексного числа* z ($\phi = \arg z$).

Приклад 1.7.2. $1 + \sqrt{3}i = 2 \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) = 2 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right)$, тому $2 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right)$ — тригонометрична форма числа $1 + \sqrt{3}i$.

Твердження 1.7.4. а) При множенні ненульових комплексних чисел їх модулі перемножаються, а аргументи додаються.

б) При діленні ненульових комплексних чисел їх модулі діляться, а аргументи віднімаються.

Доведення. Нехай $\arg z_1 = \phi_1$, $\arg z_2 = \phi_2$. Тоді $z_1 = |z_1|(\cos \phi_1 + i \sin \phi_1)$, $z_2 = |z_2|(\cos \phi_2 + i \sin \phi_2)$.

a)

$$\begin{aligned} z_1 z_2 &= |z_1|(\cos \phi_1 + i \sin \phi_1)|z_2|(\cos \phi_2 + i \sin \phi_2) = |z_1||z_2| = \\ &= ((\cos \phi_1 \cos \phi_2 - \sin \phi_1 \sin \phi_2) + i(\sin \phi_1 \cos \phi_2 + \cos \phi_1 \sin \phi_2)) = \\ &= |z_1||z_2|(\cos(\phi_1 + \phi_2) + i \sin(\phi_1 + \phi_2)). \end{aligned}$$

б)

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{|z_1|(\cos \phi_1 + i \sin \phi_1)}{|z_2|(\cos \phi_2 + i \sin \phi_2)} = \frac{|z_1|}{|z_2|} \frac{(\cos \phi_1 + i \sin \phi_1)(\cos \phi_2 - i \sin \phi_2)}{\cos^2 \phi_2 + \sin^2 \phi_2} = \\ &= \frac{|z_1|}{|z_2|} ((\cos \phi_1 \cos \phi_2 + \sin \phi_1 \sin \phi_2) + i(\sin \phi_1 \cos \phi_2 - \cos \phi_1 \sin \phi_2)) = \\ &= \frac{|z_1|}{|z_2|} (\cos(\phi_1 - \phi_2) + i \sin(\phi_1 - \phi_2)). \end{aligned}$$

□

1.7.6. Формула Муавра

Твердження 1.7.5. Для всіх цілих чисел n

$$(\cos \phi + i \sin \phi)^n = \cos n\phi + i \sin n\phi. \quad (1.7.5)$$

Доведення. Для $n = 0$ і $n = 1$ формула (1.7.5) очевидна (для $n = 0$ вона зводиться до $1 = 1$). Для $n = -1$ вона зводиться до $(\cos \phi + i \sin \phi)^{-1} = \cos \phi - i \sin \phi$, що теж легко перевіряється. Доведемо методом математичної індукції, що формула (1.7.5) виконується для всіх натуральних чисел n . Отже, припустимо, що вона виконується для натурального $n = k \geq 0$ і покажемо, що тоді вона вірна і для $n = k + 1$. Маємо, використовуючи твердження 1.7.4,

$$\begin{aligned} (\cos \phi + i \sin \phi)^{k+1} &= (\cos \phi + i \sin \phi)^k (\cos \phi + i \sin \phi) = \\ &= (\cos k\phi + i \sin k\phi)(\cos \phi + i \sin \phi) = \cos(k+1)\phi + i \sin(k+1)\phi. \end{aligned}$$

Отже, рівність (1.7.5) виконується для всіх натуральних n . Якщо $n = -k$, де $k > 0$, то

$$\begin{aligned} (\cos \phi + i \sin \phi)^n &= (\cos \phi + i \sin \phi)^{-k} = ((\cos \phi + i \sin \phi)^{-1})^k = \\ &= (\cos(-\phi) + i \sin(-\phi))^k = \cos(-k\phi) + i \sin(-k\phi) = \cos n\phi + i \sin n\phi \end{aligned}$$

і формула (1.7.5) доведена. \square

Формулу (1.7.5) називають *формулою Муавра*.

1.7.7. Корені з комплексних чисел

Нехай z — комплексне число, n — натуральне число, $n \geq 1$.

Означення 1.7.8. Коренем n -го степеня з комплексного числа z називається будь-який розв'язок рівняння

$$x^n = z. \quad (1.7.6)$$

Позначимо через $\sqrt[n]{z}$ множину всіх коренів n -го степеня з числа z :

$$\sqrt[n]{z} = \{u \in \mathbb{C} \mid u^n = z\}.$$

Наступне твердження цілком описує множину $\sqrt[n]{z}$.

Твердження 1.7.6.

$$\sqrt[n]{z} = \left\{ \sqrt[n]{|z|} \left(\cos \frac{\phi + 2\pi k}{n} + i \sin \frac{\phi + 2\pi k}{n} \right) \mid \phi = \arg z, 0 \leq k < n \right\} \quad (1.7.7)$$

Доведення. Щоб знайти множину $\sqrt[n]{z}$, потрібно знайти всі розв'язки рівняння (1.7.6). Припустимо, що розв'язки цього рівняння існують і нехай $u \in \mathbb{C}$ один з розв'язків. Тоді u можна подати в тригонометричній формі $u = \rho(\cos \psi + i \sin \psi)$, де $\rho = |u|$, $\psi = \arg u$. Підставимо u в рівняння (1.7.6). Використовуючи формулу Муавра, одержимо рівність

$$|u|^n (\cos n\psi + i \sin n\psi) = |z| (\cos \phi + i \sin \phi), \quad (1.7.8)$$

де $\phi = \arg z$. Очевидно, два комплексних числа рівні тоді і тільки тоді, коли їх модулі рівні, а аргументи відрізняються на ціле число, кратне періоду 2π . Тому з (1.7.8) одержуємо

$$|u|^n = |z| \text{ або } |u| = \sqrt[n]{|z|},$$

$$n\psi - \phi = 2\pi k \text{ або } \psi = \frac{\phi + 2\pi k}{n}, \text{ де } k \in \mathbb{Z}.$$

Тепер ясно, що для будь-якого k число $\sqrt[n]{|z|}(\cos \frac{\phi+2\pi k}{n} + i \sin \frac{\phi+2\pi k}{n})$ є розв'язком рівняння (1.7.6). Перевіримо, що при $k = 0, 1, \dots, n-1$ одержуються різні розв'язки. Справді, якби для $0 \leq k_1 < k_2 \leq n-1$ розв'язки були однаковими, то $\frac{\phi+2\pi k_2}{n} - \frac{\phi+2\pi k_1}{n} = 2\pi l$ тобто $k_2 - k_1 = nl, l > 1$, що неможливо. Далі, якщо $k \in \mathbb{Z}$, то k можна розділити з остачею на n , $k = dn+r$, де $0 \leq r \leq n-1$ і

$$\begin{aligned} \cos \frac{\phi + 2\pi k}{n} + i \sin \frac{\phi + 2\pi k}{n} &= \cos \frac{\phi + 2\pi(nd+r)}{n} + i \sin \frac{\phi + 2\pi(nd+r)}{n} = \\ &= \cos \left(\frac{\phi + 2\pi r}{n} + 2\pi d \right) + i \sin \left(\frac{\phi + 2\pi r}{n} + 2\pi d \right) = \cos \frac{\phi + 2\pi r}{n} + i \sin \frac{\phi + 2\pi r}{n}. \end{aligned}$$

Це означає, що всі елементи множини $\sqrt[n]{z}$ обчислюються за формuloю (1.7.7). \square

Приклад 1.7.3.

$$\begin{aligned} \sqrt[3]{-8} &= \left\{ \sqrt[3]{8} \left(\cos \frac{\pi + 2\pi k}{3} + i \sin \frac{\pi + 2\pi k}{3} \right) \mid k = 0, 1, 2 \right\} = \\ &= \left\{ 2 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right), 2 \left(\cos \pi + i \sin \pi \right), 2 \left(\cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} \right) \right\} = \\ &= \{1 + \sqrt{3}i, -2, 1 - \sqrt{3}i\}. \end{aligned}$$

1.7.8. Корені з 1. Група C_n

Застосуємо формулу (1.7.7) до випадку $z = 1$. У цьому випадку $|z| = 1, \arg z = 0$ і формула (1.7.7) має вигляд

$$\sqrt[n]{1} = \left\{ \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \mid k = 0, 1, \dots, n-1 \right\}. \quad (1.7.9)$$

Для множини $\sqrt[n]{1}$ — коренів n -го степеня з 1 — прийняте стандартне позначення C_n .

Твердження 1.7.7. *Множина C_n є циклічною групою порядку n відносно операції множення.*

Доведення. Покажемо, що добуток двох елементів з C_n і обернений до елемента з C_n належать до C_n :

$$\begin{aligned} & \left(\cos \frac{2\pi k_1}{n} + i \sin \frac{2\pi k_1}{n} \right) \left(\cos \frac{2\pi k_2}{n} + i \sin \frac{2\pi k_2}{n} \right) = \\ & = \left(\cos \frac{2\pi(k_1 + k_2)}{n} + i \sin \frac{2\pi(k_1 + k_2)}{n} \right) \in C_n, \\ & \left(\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \right)^{-1} = \left(\cos \frac{2\pi(n - k)}{n} + i \sin \frac{2\pi(n - k)}{n} \right) \in C_n. \end{aligned}$$

Тому, за критерієм підгрупи, C_n є підгрупою групи C^* — ненульових комплексних чисел відносно множення, отже, C_n — група. З формули Муавра випливає, що всі елементи групи C_n є степенями елемента $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, тому група C_n — циклічна, що й потрібно було довести. \square

Зауваження 1.7.3. З критерію підгрупи випливає, що множини $U = \{z \in \mathbb{C} \mid |z| = 1\}$ і $T = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}, z^n = 1\}$ є групами відносно множення. Пропонуємо довести це самостійно.

Приклад 1.7.4. *C_6 є циклічною групою, породженою елементом $\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.*

1.7.9. Первісні корені з 1

Означення 1.7.9. Корінь n -го степеня з 1 називається *первісним*, якщо він не є коренем степеня m з 1, де $1 \leq m < n$.

Приклад 1.7.5. *i та $-i$ — первісні корені 4-го степеня з 1, $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ — первісний корінь n -го степеня з 1.*

Наступне твердження описує множину всіх первісних коренів n -го степеня з 1.

Твердження 1.7.8. *Нехай $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. ε^k є первісним коренем n -го степеня з 1 тоді і тільки тоді, коли k і n взаємно прості.*

Доведення. Нехай ε^k первісний корінь, і нехай k і n не взаємно прості. Тоді існує $d > 1$ таке, що $k = k_1 d$ і $n = n_1 d$. $(\varepsilon^k)^{n_1} = (\varepsilon^{k_1 d})^{n_1} = \varepsilon^{k_1 d n_1} = \varepsilon^{k_1 n} = (\varepsilon^n)^{k_1} = 1$. Ми одержали суперечність з тим, що ε^k — первісний корінь, бо $(\varepsilon^k)^{n_1} = 1$, а $n_1 < n$. Навпаки, нехай k і n взаємно прості. Покажемо, що ε^k — первісний корінь n -го степеня з 1. Якщо для деякого $m < n$ $(\varepsilon^k)^m = 1$, тобто $\cos \frac{2\pi km}{n} + i \sin \frac{2\pi km}{n} = 1$, то $\frac{2\pi km}{n} = 2\pi l$, $l \in \mathbb{Z}$ або $km = nl$. Звідси, і з того, що k і n взаємно прості, випливає, що m ділиться на n , що неможливо, оскільки $m < n$. \square

Зauważення 1.7.4. Кількість первісних коренів n -го степеня з 1 дорівнює кількості натуральних чисел k , таких що $1 \leq k < n$ і k взаємно просте з n . Ця кількість позначається $\phi(n)$. $\phi(n)$ — функція від натурального n , вона називається *функцією Ойлера* і відіграє важливу роль в теорії чисел.

1.8. Вправи

- 1) На множині $\mathbb{N} \setminus \{0\}$ ненульових натуральних чисел задані такі алгебраїчні операції:
 - a) $a \circ_1 b = c$, де c — найбільший спільний дільник a і b ;
 - б) $a \circ_2 b = c$, де c — найменше спільне кратне a і b ;
 - в) $a \circ_2 b = a^b$.
 Вияснити, які з цих операцій є асоціативними, комутативними. Чи існують нейтральні елементи (ліві, праві, двосторонні)?
- 2) Елемент a півгрупи G називається *ідемпотентом*, якщо $a^2 = a$. Довести, що в кожній скінченній півгрупі існують ідемпотенти.
- 3) Довести, що в комутативній півгрупі, що містить ідемпотенти, множина всіх ідемпотентів є підпівгрупою.

- 4) Чи утворює групу множина функцій $f_0(x) = x$, $f_1(x) = \frac{1}{x}$, $f_2(x) = 1-x$, $f_3(x) = \frac{x}{x-1}$, $f_4(x) = \frac{x-1}{x}$, $f_5(x) = \frac{1}{1-x}$ відносно суперпозиції функцій?
- 5) Знайти групу симетрій ромба. Чи ізоморфні група симетрій квадрата і група симетрій ромба? Чи ізоморфні група поворотів квадрата і група симетрій ромба?
- 6) Довести, що дві циклічні групи ізоморфні тоді і тільки тоді, коли їх порядки рівні.
- 7) Довести, що кожна нескінченна група має нескінченно багато підгруп.
- 8) Знайти ліві суміжні класи групи A_4 за підгрупою $H = \{e, (1, 2, 3), (1, 3, 2)\}$. Чи є H нормальнюю підгрупою?
- 9) Довести, що коли підмножина K групи G є правим або лівим суміжним класом за якою-небудь підгрупою, то для всіх $x, y, z \in K$ $xy^{-1}z \in K$.
- 10) Довести, що кожна нециклічна група шостого порядку ізоморфна групі S_3 .
- 11) Довести, що кожна підгрупа і кожна фактор-група циклічної групи є циклічною.
- 12) Довести, що група A_n парних підстановок степеня n породжується циклами довжини 3.
- 13) Довести, що група S_n породжується циклом $(1, 2, \dots, n)$ довжини n і транспозицією $(1, 2)$.
- 14) Чи утворюють систему твірних групи S_9 підстановки $(1, 2, 3)$ і $(1, 2, \dots, 9)$?
- 15) Якщо n — просте число, то для кожного k , $0 < k < n$, підстановка $(i_1, i_2, \dots, i_n)^k$ є циклом довжини n . Якщо n — не просте, то ця підстановка буде циклом довжини n для

чисел k , що взаємно прості з n , і добутком циклів однакової довжини в іншому випадку.

- 16) Нехай $\sigma \in S_n$ і нехай s — кількість незалежних циклів у розкладі σ в добуток циклів плюс кількість символів, що переходять у себе. Різниця $n - s$ називається *декрементом* підстановки σ . Довести, що парність підстановки σ збігається з парністю її декременту.
- 17) Довести, що для кільця K з одиницею аксіома комутативності додавання виводиться з інших аксіом. Показати, що це невірно для кілець без одиниці.
- 18) Якщо для довільного елемента x кільця K елемент $x^2 - x$ комутує з кожним елементом кільця K , то K — комутативне кільце.
- 19) Довести, що скінченне комутативне кільце, в якому добуток будь-яких ненульових елементів ненульовий, є полем.
- 20) Показати, що множина $\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ є полем відносно звичайних операцій додавання і множення чисел.
- 21) Показати, що множина всіх матриць вигляду $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, де $a, b \in \mathbb{R}$, є полем, ізоморфним полю комплексних чисел.
- 22) Показати, що множина матриць $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}/3\mathbb{Z} \right\}$ є полем з дев'ятою елементами.
- 23) Довести, що для того, щоб квадратна матриця $A \in M_n(R)$ комутувала з усіма квадратними матрицями $B \in M_n(R)$ того ж порядку, необхідно і достатньо, щоб A була скалярною, тобто $A = cE$, де $c \in R$, E — одинична матриця (R — комутативне кільце з 1).
- 24) Довести, що кільце матриць $M_n(M_m(R))$ і $M_{nm}(R)$ ізоморфні.

25) Показати, що додавання і множення матриць на множині $R = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$ є алгебраїчними операціями на цій множині, і що вони задовольняють всім аксіомам поля, крім комутативності множення (тут \bar{a} — спряжене до a в \mathbb{C}).

26) Використовуючи геометричну інтерпретацію комплексних чисел, доведіть такі геометричні теореми:

а) сума квадратів діагоналей паралелограма дорівнює сумі квадратів всіх його сторін.

б) коло і квадрат $ABCD$ мають спільний центр. Довести, що для кожної точки M кола число $MA^2 \cdot MC^2 + MB^2 \cdot MD^2$ не залежить від розміщення точки M на колі.

в) відстані від будь-якої точки M , взятої в площині трикутника ABC , до вершин A, B, C і точки O перетину медіан зв'язані рівністю

$$MA^2 + MB^2 + MC^2 = AO^2 + BO^2 + CO^2 + 3MO^2.$$

27) Використовуючи формулу Муавра, знайти суми

$$\cos \alpha + \cos 2\alpha + \cdots + \cos n\alpha \quad \text{i} \quad \sin \alpha + \sin 2\alpha + \cdots + \sin n\alpha.$$

28) Обчислити суми

$$A = 1 - \cos 2\alpha + \cos 4\alpha - \cos 6\alpha + \cdots + \cos 2n\alpha,$$

$$B = \cos \alpha - \cos 2\alpha + \cos 3\alpha - \cdots + \cos(2n-1)\alpha,$$

$$C = \sin \alpha - \sin 2\alpha + \sin 3\alpha - \cdots + \sin(2n-1)\alpha.$$

29) а) Обчислити $\sqrt[3]{-i}$, $\sqrt[3]{2+2i}$, $\sqrt[4]{i}$.

б) Розв'язати рівняння $z^2 + i = 0$, $z^3 + 8i = 0$.

Розділ 2

Системи лінійних рівнянь та визначники

2.1. n -вимірний векторний простір

Зафіксуємо яке-небудь поле P . Це може бути поле дійсних чисел \mathbb{R} , поле комплексних чисел \mathbb{C} , або якесь інше поле. Елементи поля P будемо називати *скалярами*.

2.1.1. Вектори та лінійні операції над ними

Впорядковану послідовність (a_1, \dots, a_n) елементів поля P назовемо *n -вимірним вектором* над полем P , скаляри a_i — *координатами* (компонентами) вектора. Вектор (a_1, \dots, a_n) позначають \vec{a} і записують у вигляді вектор-стовпчика $\vec{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ або у вигляді вектор-рядка $\vec{a}^t = (a_1, \dots, a_n)$. Індекс t тут означає транспонування. Ми домовимося його пропускати у більшості випадків. Тому символ \vec{a} означатиме вектор-стовпчик або вектор-рядок в залежності від контексту. Вектори $\vec{a} = (a_1, \dots, a_n)$ і $\vec{b} = (b_1, \dots, b_n)$ називають *рівними* і пишуть $\vec{a} = \vec{b}$, якщо $a_i = b_i$ для всіх i , $1 \leq i \leq n$.

Множину всіх n -вимірних векторів над полем P позначають P^n : $P^n = \{(a_1, \dots, a_n) \mid a_i \in P\}$. Визначимо на множині P^n лінійні операції. Якщо $\vec{a} = (a_1, \dots, a_n) \in P^n$, $\vec{b} = (b_1, \dots, b_n) \in P^n$

і $\lambda \in P$, то

$$\begin{aligned}\vec{a} + \vec{b} &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n), \\ \lambda \vec{a} &= (\lambda a_1, \lambda a_2, \dots, \lambda a_n).\end{aligned}$$

Вектор, всі компоненти якого є нулі, називають *нуль-вектором* і позначають $\vec{0}$. Легко перевірити, що лінійні операції над векторами мають властивості, аналогічні властивостям лінійних операцій над матрицями (зауважимо, що поняття вектора, з цієї точки зору, є частковим випадком поняття матриці):

1. $\vec{a} + \vec{b} = \vec{b} + \vec{a}$,
2. $\vec{a} + (\vec{b} + \vec{c}) = (\vec{a} + \vec{b}) + \vec{c}$,
3. $\vec{a} + \vec{0} = \vec{a}$,
4. $\vec{a} + (-1)\vec{a} = \vec{0}$,
5. $\lambda(\mu\vec{a}) = (\lambda\mu)\vec{a}$,
6. $\vec{\lambda}(\vec{a} + \vec{b}) = \lambda\vec{a} + \lambda\vec{b}$,
7. $(\lambda + \mu)\vec{a} = \lambda\vec{a} + \mu\vec{a}$,
8. $1 \cdot \vec{a} = \vec{a}$.

Тут $\vec{a}, \vec{b}, \vec{c}$ — довільні вектори з P^n , а $\lambda, \mu \in P$ — довільні скаляри. Вектор \vec{b} називають *лінійною комбінацією* векторів $\vec{a}_1, \dots, \vec{a}_m$, якщо існують такі скаляри $\lambda_1, \dots, \lambda_m \in P$, що $\vec{b} = \lambda_1\vec{a}_1 + \dots + \lambda_m\vec{a}_m$.

2.1.2. Лінійна залежність

Означення 2.1.1. Систему векторів $\vec{a}_1, \dots, \vec{a}_m \in P^n$ називають *лінійно залежною*, якщо існують скаляри $\lambda_1, \dots, \lambda_m \in P$, що не всі дорівнюють нулю і такі, що

$$\lambda_1\vec{a}_1 + \dots + \lambda_m\vec{a}_m = \vec{0}. \quad (2.1.1)$$

Система векторів $\vec{a}_1, \dots, \vec{a}_m$ називається *лінійно незалежною*, якщо рівність (2.1.1) можлива лише тоді, коли $\lambda_1 = \dots = \lambda_m = 0$.

Приклад 2.1.1. 1. Нехай $\vec{a}_1 = (1, 1)$, $\vec{a}_2 = (0, 1)$, $\vec{a}_3 = (3, 4)$; $\vec{a}_1, \vec{a}_2, \vec{a}_3 \in \mathbb{R}^2$. Система векторів $\vec{a}_1, \vec{a}_2, \vec{a}_3$ є лінійно залежною, бо $3\vec{a}_1 + \vec{a}_2 - \vec{a}_3 = \vec{0}$. Система векторів $\vec{a}_1 = (1, 1)$, $\vec{a}_2 = (0, 1) \in \mathbb{R}^2$ лінійно незалежна, бо рівність $\lambda_1\vec{a}_1 + \lambda_2\vec{a}_2 = \vec{0}$ можлива лише тоді, коли $\lambda_1 = 0$, $\lambda_1 + \lambda_2 = 0$, тобто коли $\lambda_1 = \lambda_2 = 0$.

2. Одиничними векторами простору P^n називають вектори

$$\vec{e}_1 = (1, 0, \dots, 0), \quad \vec{e}_2 = (0, 1, 0, \dots, 0), \dots, \vec{e}_n = (0, \dots, 0, 1).$$

Система $\vec{e}_1, \dots, \vec{e}_n$ одиничних векторів є лінійно незалежною. Справді, нехай $\lambda_1\vec{e}_1 + \dots + \lambda_n\vec{e}_n = \vec{0}$. Остання рівність означає, що $(\lambda_1, \dots, \lambda_n) = (0, \dots, 0)$, тобто $\lambda_1 = \dots = \lambda_n = 0$.

У наступному твердженні наведено найпростіші властивості лінійної залежності.

Твердження 2.1.1. 1) Якщо система векторів простору P^n містить нуль-вектор, то вона лінійно залежна.

2) Якщо підсистема $\vec{a}_1, \dots, \vec{a}_m$ системи $\vec{a}_1, \dots, \vec{a}_k$ ($m < k$) є лінійно залежною, то і система $\vec{a}_1, \dots, \vec{a}_k$ — лінійно залежна.

3) Кожна підсистема лінійно незалежної системи векторів є лінійно незалежною.

Доведення. 1) Нехай $\vec{a}_1 = \vec{0}, \vec{a}_2, \dots, \vec{a}_m$ — система векторів, що містить нуль-вектор. Тоді $1 \cdot \vec{a}_1 + 0 \cdot \vec{a}_2 + \dots + 0 \cdot \vec{a}_n = \vec{0}$ і $\lambda_1 = 1 \neq 0$.

2) Якщо $\vec{a}_1, \dots, \vec{a}_m$ — лінійно залежна підсистема системи векторів $\vec{a}_1, \dots, \vec{a}_m, \vec{a}_{m+1}, \dots, \vec{a}_k$, то існує ненульовий набір скалярів $\lambda_1, \dots, \lambda_m \in P$ (не зменшуючи загальності, можна вважати, що $\lambda_1 \neq 0$), для яких $\lambda_1\vec{a}_1 + \dots + \lambda_m\vec{a}_m = \vec{0}$. Звідси $\lambda_1\vec{a}_1 + \dots + \lambda_m\vec{a}_m + 0 \cdot \vec{a}_{m+1} + \dots + \vec{a}_k = \vec{0}$, де $\lambda_1 \neq 0$. Отже, система $\vec{a}_1, \dots, \vec{a}_k$ лінійно залежна.

3) Якби підсистема лінійно незалежної системи виявилась лінійно залежною, то і вся система була б лінійно залежною. \square

2.1.3. Леми про лінійну залежність

Лема 2.1.1. *Система векторів $\vec{a}_1, \dots, \vec{a}_k \in P^n$, $k \geq 2$, є лінійно залежною тоді і тільки тоді, коли хоч один з цих векторів є лінійною комбінацією інших.*

Доведення. Якщо система $\vec{a}_1, \dots, \vec{a}_k$ є лінійно залежною, то існують скаляри $\lambda_1, \dots, \lambda_k \in P$, що не всі дорівнюють нулеві (не зменшуючи загальності, вважаємо, що $\lambda_1 \neq 0$) такі, що $\lambda_1\vec{a}_1 + \dots + \lambda_k\vec{a}_k = \vec{0}$. Звідси $\vec{a}_1 = -\frac{\lambda_2}{\lambda_1}\vec{a}_2 - \dots - \frac{\lambda_k}{\lambda_1}\vec{a}_k$, тобто вектор \vec{a}_1 є лінійною комбінацією векторів $\vec{a}_2, \dots, \vec{a}_k$. Нехай тепер один з векторів, наприклад \vec{a}_k , є лінійною комбінацією інших, тобто $\vec{a}_k = \mu_1\vec{a}_1 + \dots + \mu_{k-1}\vec{a}_{k-1} - 1 \cdot \vec{a}_k = \vec{0}$, тобто вектори $\vec{a}_1, \dots, \vec{a}_k$ лінійно залежні. \square

Лема 2.1.2. *Нехай $\vec{a}_1, \dots, \vec{a}_k \in P^n$ — лінійно незалежна система векторів, коєсний вектор якої є лінійною комбінацією векторів $\vec{b}_1, \dots, \vec{b}_m \in P^n$. Тоді $k \leq m$.*

Доведення. Міркуємо від супротивного. Припустимо, що $k > m$. Оскільки \vec{a}_1 є лінійною комбінацією векторів $\vec{b}_1, \dots, \vec{b}_m$, то система $\vec{a}_1, \vec{b}_1, \dots, \vec{b}_m$ лінійно залежна. Отже, існують скаляри $\lambda_1, \mu_1, \dots, \mu_m \in P$, що не всі дорівнюють нулеві і такі, що $\lambda_1\vec{a}_1 + \mu_1\vec{b}_1 + \dots + \mu_m\vec{b}_m = \vec{0}$. Зауважимо, що випадок $\mu_1 = \dots = \mu_m = 0$ неможливий, бо тоді ми мали б $\lambda_1\vec{a}_1 = \vec{0}$ і, оскільки $\lambda_1 \neq 0$, то $\vec{a}_1 = \vec{0}$. Це неможливо, бо система $\vec{a}_1, \dots, \vec{a}_k$ лінійно незалежна (див. твердження 2.1.1). Отже, існує відмінний від нуля скаляр μ_i ($1 \leq i \leq n$). Нехай, наприклад, $\mu_1 \neq 0$. Тоді, як і в лемі 2.1.1, вектор \vec{b}_1 є лінійною комбінацією векторів $\vec{a}_1, \vec{b}_2, \dots, \vec{b}_m$. Оскільки вектор \vec{a}_2 є лінійною комбінацією векторів $\vec{b}_1, \dots, \vec{b}_m$, то з доведеного випливає, що він є і лінійною комбінацією векторів $\vec{a}_1, \vec{b}_2, \dots, \vec{b}_m$. Звідси, за лемою 2.1.1, система $\vec{a}_1, \vec{a}_2, \vec{b}_1, \dots, \vec{b}_m$ лінійно залежна, тобто існує такий ненульовий набір скалярів $\lambda_1, \lambda_2, \mu_1, \dots, \mu_m \in P$, що

$$\lambda_1\vec{a}_1 + \lambda_2\vec{a}_2 + \mu_2\vec{b}_2 + \dots + \mu_m\vec{b}_m = \vec{0}.$$

Якщо $\mu_2 = \dots = \mu_m = 0$, то $\lambda_1 \neq 0$ або $\lambda_2 \neq 0$ і $\lambda_1 \vec{a}_1 + \lambda_2 \vec{a}_2 = \vec{0}$, що суперечить твердження 2.1.1. Отже, серед μ_2, \dots, μ_m існує ненульовий скаляр. Нехай $\mu_2 \neq 0$. Тоді $b_2 = \alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \beta_3 \vec{b}_3 + \dots + \beta_m \vec{b}_m$, де $\alpha_1, \alpha_2, \beta_3, \dots, \beta_m \in P$. Оскільки кожний вектор \vec{a}_i ($1 \leq i \leq k$) є лінійною комбінацією векторів $\vec{b}_1, \dots, \vec{b}_m$, то він є і лінійною комбінацією векторів $\vec{a}_1, \vec{a}_2, \vec{b}_3, \dots, \vec{b}_m$. Продовжуючи так міркувати, через m кроків одержимо, що кожний вектор \vec{a}_i ($1 \leq i \leq k$), зокрема, вектор \vec{a}_{m+1} є лінійною комбінацією векторів $\vec{a}_1, \dots, \vec{a}_m$. За лемою 2.1.1 система $\vec{a}_1, \dots, \vec{a}_m, \vec{a}_{m+1}$ є лінійно залежною. Тоді з твердження 2.1.1 випливає, що і вся система $\vec{a}_1, \dots, \vec{a}_k$ лінійно залежна. Одержані суперечності показують, що $k \leq m$, що і треба довести. \square

Лема 2.1.3. *Будь-які $k > n$ векторів з P^n лінійно залежні.*

Доведення. Розглянемо одиничні вектори

$$\vec{e}_1 = (1, 0, \dots, 0), \quad \vec{e}_2 = (0, 1, 0, \dots, 0), \dots, \vec{e}_n = (0, \dots, 0, 1).$$

Якщо $\vec{a} = (a_1, \dots, a_n) \in P^n$, то зрозуміло, що $\vec{a} = a_1 \vec{e}_1 + \dots + a_n \vec{e}_n$, тобто кожний вектор є лінійною комбінацією одиничних векторів. Якщо ми маємо k лінійно незалежних векторів $\vec{a}_1, \dots, \vec{a}_k$, то з леми 2.1.2 випливає, що $k \leq n$, тобто $k > n$ векторів з P^n не можуть бути лінійно незалежними, тому вони лінійно залежні. \square

2.1.4. Підпростори. База підпростору

Означення 2.1.2. Непорожня підмножина $L \subset P^n$ називається *підпростором*, якщо її елементи мають такі властивості:

1. $\forall \vec{a}, \vec{b} \in L \quad \vec{a} + \vec{b} \in L$,
2. $\forall \vec{a} \in L \quad \forall \lambda \in P \quad \lambda \vec{a} \in L$.

Очевидно, що P^n є підпростором; підмножина $\{0\}$, яка містить лише нуль-вектор, теж є підпростором. Ці два підпростори називають *тривіальними*, підпростір $\{0\}$ називають *нульовим*. Розглянемо довільну систему векторів

$\vec{a}_1, \dots, \vec{a}_m$
 $\in P^n$. Нехай

$$\mathcal{L}(\vec{a}_1, \dots, \vec{a}_m) = \left\{ x \in P \mid x = \sum_{i=1}^m \lambda_i a_i, \lambda_i \in P \right\}$$

- множина всіх лінійних комбінацій векторів $\vec{a}_1, \dots, \vec{a}_m$. Множину $\mathcal{L}(\vec{a}_1, \dots, \vec{a}_m)$ називають *лінійною оболонкою* векторів $\vec{a}_1, \dots, \vec{a}_m$. Переконаємося, що кожна лінійна оболонка є підпростором. Нехай $\vec{x} = \sum_{i=1}^m \lambda_i \vec{a}_i, \vec{y} = \sum_{i=1}^m \mu_i \vec{a}_i \in \mathcal{L}(\vec{a}_1, \dots, \vec{a}_m)$ і $\lambda \in P$. Тоді $\vec{x} + \vec{y} = \sum_{i=1}^m (\lambda_i + \mu_i) \vec{a}_i \in \mathcal{L}(\vec{a}_1, \dots, \vec{a}_m)$ і $\lambda \vec{x} = \sum_{i=1}^m (\lambda \lambda_i) \vec{a}_i \in \mathcal{L}(\vec{a}_1, \dots, \vec{a}_m)$.

Означення 2.1.3. Нехай V — підпростір простору P^n . Якщо V є лінійною оболонкою деякої системи векторів $\vec{a}_1, \dots, \vec{a}_k \in P^n$, то цю систему $\vec{a}_1, \dots, \vec{a}_k$ називають *системою твірних* підпростору V . Система твірних $\vec{a}_1, \dots, \vec{a}_k$ підпростору V називається *мінімальною*, якщо після вилучення хоч одного з векторів системи $\vec{a}_1, \dots, \vec{a}_k$ менша система перестає бути системою твірних.

Наприклад, система одиничних векторів $\vec{e}_1 = (1, 0, \dots, 0)$, $\vec{e}_2 = (0, 1, 0, \dots, 0), \dots, \vec{e}_n = (0, \dots, 0, 1)$ є мінімальною системою твірних простору P^n . Справді, очевидно, це — система твірних (див. початок доведення леми 2.1.3). З іншого боку, вилучивши i -ий вектор, ми не зможемо його одержати як лінійну комбінацію решти векторів, бо кожна така лінійна комбінація буде мати нульову i -ту компоненту. Якщо ми маємо яку-небудь систему твірних $\vec{a}_1, \dots, \vec{a}_k$ підпростору V , і один з векторів (нехай \vec{a}_1) цієї системи є лінійною комбінацією інших, то система $\vec{a}_2, \dots, \vec{a}_k$, яка залишається після вилучення вектора \vec{a}_1 , знову, очевидно, є системою твірних. Звідси легко випливає таке твердження.

Твердження 2.1.2. *Мінімальна система твірних підпростору є лінійно незалежною.*

Доведення. Якщо система твірних $\vec{a}_1, \dots, \vec{a}_k$ лінійно залежна, то за лемою 2.1.1 один з векторів цієї системи є лінійною комбінацією інших, а тому вона не може бути мінімальною. \square

Означення 2.1.4. *Базою підпростору* називається будь-яка лінійно незалежна система твірних цього підпростору.

Приклад 2.1.2. 1. Система $\vec{e}_1 = (1, 0, \dots, 0)$, $\vec{e}_2 = (0, 1, 0, \dots, 0), \dots, \vec{e}_n = (0, \dots, 0, 1)$ є лінійно незалежною системою твірних, отже, — базою простору P^n .

2. Підпростір може мати багато баз. Наприклад, $\vec{e}_1 = (1, 0)$, $\vec{e}_2 = (0, 1)$ та $\vec{a}_1 = (1, 1)$, $\vec{a}_2 = (2, 1)$ — дві різні бази простору \mathbb{R}^2 .

2.1.5. Теореми про базу

Теорема 2.1.3. *Кожен ненульовий підпростір має базу.*

Доведення. Нехай $L \neq \{\vec{0}\}$ — ненульовий підпростір в P^n , і \vec{e}_1 — ненульовий вектор, $\vec{e}_1 \in L$. Тоді система, що складається з одного вектора \vec{e}_1 , є лінійно незалежною. Якщо ця система є системою твірних простору L , то все доведено. В іншому випадку знайдеться вектор $\vec{e}_2 \in L$, який не є лінійною комбінацією вектора \vec{e}_1 . Тоді система \vec{e}_1, \vec{e}_2 лінійно незалежна, бо з рівності $\lambda_1 \vec{e}_1 + \lambda_2 \vec{e}_2 = \vec{0}$ випливає $\lambda_2 = 0$, а тоді і $\lambda_1 = 0$. Якщо система \vec{e}_1, \vec{e}_2 — база підпростору L , то доведення закінчене. В іншому випадку знайдеться вектор $\vec{e}_3 \in L$, який не виражається лінійно через \vec{e}_1 і \vec{e}_2 . Так само, як і раніше, звідси одержуємо, що вектори $\vec{e}_1, \vec{e}_2, \vec{e}_3$ лінійно незалежні. Продовжуючи так міркувати, на k -му кроці ми одержимо лінійно незалежну систему $\vec{e}_1, \dots, \vec{e}_k$ векторів з підпростору L . Оскільки при $k > n$ система векторів з P^n не може бути лінійно незалежною (за лемою 2.1.1), то через скінченне число кроків одержимо базу. \square

Наслідок 2.1.4. *Кожний ненульовий підпростір простору P^n над нескінченим полем P має нескінченну кількість баз.*

Доведення. З доведення теореми 2.1.3 видно, що побудову бази можна почати з будь-якого ненульового вектора підпростору L . \square

Метод доведення теореми 2.1.3 підказує, що може бути корисним таке означення.

Означення 2.1.5. Лінійно незалежна система векторів $\vec{e}_1, \dots, \vec{e}_k$ підпростору L називається *максимальною*, якщо вона стає лінійно залежною при додаванні до неї будь-якого вектора з підпростору L .

Теорема 2.1.5. *Кожні дві бази підпростору L складаються з однакової кількості векторів.*

Доведення. Нехай $\vec{e}_1, \dots, \vec{e}_m$ та $\vec{a}_1, \dots, \vec{a}_k$ — дві бази підпростору L . Система $\vec{e}_1, \dots, \vec{e}_m$ лінійно незалежна і кожний вектор \vec{e}_i ($1 \leq i \leq m$) є лінійною комбінацією векторів $\vec{a}_1, \dots, \vec{a}_k$. З леми 2.1.2 випливає, що $m \leq k$. Так само показуємо, що $k \leq m$. Отже, $m = k$. \square

З теореми 2.1.5 випливає, що наступне означення є коректним.

Означення 2.1.6. Розмірністю ненульового підпростору L називають кількість векторів будь-якої бази цього підпростору. Розмірність підпростору L позначають $\dim L$. За означенням $\dim \{0\} = 0$.

Теорема 2.1.6. Нехай $\vec{e}_1, \dots, \vec{e}_k$ — лінійно незалежна система векторів підпростору L . Тоді наступні твердження еквівалентні:

- 1) $\vec{e}_1, \dots, \vec{e}_k$ — база L ;
- 2) кожній вектор підпростору L однозначно записується у вигляді лінійної комбінації векторів $\vec{e}_1, \dots, \vec{e}_k$;
- 3) $\vec{e}_1, \dots, \vec{e}_k$ — мінімальна система твірних підпростору L ;

4) $\vec{e}_1, \dots, \vec{e}_k$ — максимальна лінійно незалежна система в L .

Доведення. Доведення проводимо за схемою 1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 1).

1) \Rightarrow 2). Нехай $x \in L$, причому

$$x = \lambda_1 \vec{e}_1 + \dots + \lambda_k \vec{e}_k \text{ і } x = \lambda'_1 \vec{e}_1 + \dots + \lambda'_k \vec{e}_k.$$

Звідси випливає, що

$$(\lambda_1 - \lambda'_1) \vec{e}_1 + \dots + (\lambda_k - \lambda'_k) \vec{e}_k = \vec{0}.$$

Тому маємо $\lambda_1 - \lambda'_1 = \dots = \lambda_k - \lambda'_k = 0$, тобто $\lambda_1 = \lambda'_1, \dots, \lambda_k = \lambda'_k$.

2) \Rightarrow 3). Якщо система твірних $\vec{e}_1, \dots, \vec{e}_k$ підпростору L не є мінімальною, то з неї можна вилучити один з векторів (наприклад, \vec{e}_1), так, що система $\vec{e}_2, \dots, \vec{e}_k$, яка залишиться, ще буде системою твірних. Тоді для вектора \vec{e}_1 одержимо

$$\begin{aligned} \vec{e}_1 &= 1 \cdot \vec{e}_1 + 0 \cdot \vec{e}_2 + \dots + 0 \cdot \vec{e}_k, \\ \vec{e}_1 &= 0 \cdot \vec{e}_1 + \lambda_2 \vec{e}_2 + \dots + \lambda_k \vec{e}_k, \end{aligned}$$

тобто вектор \vec{e}_1 можна двома способами подати у вигляді лінійної комбінації векторів $\vec{e}_1, \dots, \vec{e}_k$. Ця суперечність показує, що система $\vec{e}_1, \dots, \vec{e}_k$ мінімальна.

3) \Rightarrow 4). Мінімальна система твірних є лінійно незалежною за твердженням 2.1.2. Якщо вона не є максимальною, то існує вектор $\vec{a} \in L$ такий, що система $\vec{a}, \vec{e}_1, \dots, \vec{e}_k$ лінійно незалежна. Звідси випливає, що \vec{a} не виражається у вигляді лінійної комбінації векторів $\vec{e}_1, \dots, \vec{e}_k$. Суперечність.

4) \Rightarrow 1). Потрібно лише довести, що $\vec{e}_1, \dots, \vec{e}_k$ є системою твірних підпростору L . Для цього, нехай $\vec{x} \in L$. Система $\vec{x}, \vec{e}_1, \dots, \vec{e}_k$ лінійно залежна, тобто існує ненульовий набір скалярів $\lambda, \alpha_1, \dots, \alpha_k$ такий, що $\lambda \vec{x} + \alpha_1 \vec{e}_1 + \dots + \alpha_k \vec{e}_k = \vec{0}$. Тут обов'язково $\lambda \neq 0$, бо в іншому випадку ми мали б $\alpha_1 \vec{e}_1 + \dots + \alpha_k \vec{e}_k = \vec{0}$, причому не всі $\alpha_1, \dots, \alpha_k$ дорівнюють нулю, тобто система $\vec{e}_1, \dots, \vec{e}_k$ була б лінійно залежною. Отже, $\vec{x} = -\frac{\alpha_1}{\lambda} \vec{e}_1 - \dots - \frac{\alpha_k}{\lambda} \vec{e}_k$. Це завершує доведення останньої іmplікації і теореми в цілому. \square

2.2. Системи лінійних рівнянь

2.2.1. Елементарні перетворення матриць

Нехай A — матриця з елементами з поля P . Під перетворенням матриці A розуміють перехід від цієї матриці до іншої матриці A' , здійснений за певними правилами.

Означення 2.2.1. *Елементарними перетвореннями* рядків матриці A називають перетворення одного з трьох типів:

- 1) перестановка двох рядків матриці;
- 2) додавання до рядка матриці іншого рядка цієї матриці, помноженого на скаляр;
- 3) множення рядка на ненульовий скаляр.

Аналогічно визначають елементарні перетворення стовпчиків матриці. У цьому параграфі ми будемо розглядати лише елементарні перетворення рядків.

Означення 2.2.2. Якщо матриця A' отримується з матриці A за допомогою скінченної послідовності елементарних перетворень, то матриці A і A' називають *еквівалентними*.

Означення 2.2.3. Матриця A називається *східчастою*, якщо вона має такі дві властивості:

- 1) якщо i -ий рядок матриці A нульовий, то й $(i + 1)$ -ий рядок нульовий;
- 2) якщо перші ненульові елементи i -го та $(i + 1)$ -го рядків розташовані в стовпчиках з номерами k_i та $k_i + 1$ відповідно, то $k_i < k_i + 1$. Тут $i \leq m - 1$, де m — кількість рядків матриці A .

Інакше кажучи, матриця A є східчастою, якщо вона або ну-

льова або має вигляд

$$\begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & \dots & \dots \dots & \dots & \dots & a_{1n} \\ 0 & \dots & 0 & 0 & \dots & 0 & a_{2k_2} & \dots & \dots \dots & \dots & a_{2n} \\ \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & \dots & \dots & 0 & a_{sk_s} & \dots & a_{sn} \\ 0 & \dots & 0 & 0 & \dots & \dots & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & \dots & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$

де $a_{ik_i} \neq 0$ для $1 \leq i \leq s$, і $k_1 < k_2 < \dots < k_s$.

Теорема 2.2.1. *Коєсну матрицю можна звести до східчастого вигляду за допомогою скінченного числа елементарних перетворень.*

Доведення. Нехай матриця A не є східчастою (зокрема, вона ненульова і має не менше ніж два рядки). Якщо k_1 — номер першого ненульового стовпчика матриці A , то будемо вважати, що $a_{1k_1} \neq 0$ (цього можна домогтися, переставивши рядки матриці A). Отже, нехай матриця A має вигляд

$$A = \begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & \dots & a_{1n} \\ 0 & \dots & 0 & a_{2k_1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_{mk_1} & \dots & a_{mn} \end{pmatrix}.$$

Додамо до другого рядка перший, домножений на $-a_{2k_1}/a_{1k_1}$, до третього рядка — перший, домножений на $-a_{3k_1}/a_{1k_1}$, і т.д. В результаті цих елементарних перетворень одержимо матрицю

$$A' = \begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & a_{1k_1+1} & \dots & a_{1n} \\ 0 & \dots & 0 & 0 & a'_{2k_1+1} & \dots & a'_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & a'_{mk_1+1} & \dots & a'_{mn} \end{pmatrix}.$$

Тепер розглядаємо матрицю A'' , що одержується з матриці A' , якщо відкинути перший рядок матриці A' . Якщо вона

східчаста, то доведення завершено, а якщо ні, то повторимо з A'' попередню процедуру. І так далі. Через скінченне число кроків одержимо східчасту матрицю. \square

2.2.2. Еквівалентні системи лінійних рівнянь

Розглянемо систему m лінійних рівнянь з n невідомими x_1, \dots, x_n :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2, \\ \dots \dots \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m. \end{cases} \quad (2.2.1)$$

Елементи a_{ij} називаємо коефіцієнтами системи (2.2.1), а елементи b_i називаємо вільними членами. Вважаємо, що a_{ij} та b_i є елементами деякого фіксованого поля P . Матриця

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

називається *матрицею системи* (2.2.1), а матриця

$$A_b = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots \dots \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

називається *розв'язком системи* (2.2.1). Зрозуміло, що для задання системи (2.2.1) досить задати її розширену матрицю.

Розв'язком системи (2.1.1) називають впорядковану послідовність (c_1, c_2, \dots, c_n) елементів поля P таку, що після заміни невідомих x_i елементами c_i одержується система правильних рівностей.

Систему лінійних рівнянь називають *сумісною*, якщо вона має хоч один розв'язок, і *несумісною* в протилежному випадку.

Дві системи лінійних рівнянь називаються *еквівалентними*, якщо вони мають однакові множини розв'язків. Кожні дві несумісні системи еквівалентні.

Елементарними перетвореннями системи лінійних рівнянь (2.2.1) називають перетворення одного з трьох типів:

- 1) перестановка двох рівнянь системи;
- 2) додавання до одного рівняння системи іншого рівняння цієї системи, домноженого на скаляр λ ;
- 3) домноження будь-якого рівняння системи на ненульовий скаляр.

Теорема 2.2.2. *Елементарні перетворення системи лінійних рівнянь приводять до еквівалентної системи.*

Доведення. Очевидно, що після перестановки двох рівнянь системи одержимо еквівалентну систему. Переконаємося, що в результаті елементарного перетворення другого типу теж одержимо еквівалентну систему. Отже, нехай ми до i -го рівняння системи (2.2.1) додаємо l -те рівняння, домножене на $\lambda \in P$. Одержано нову систему, в якій всі рівняння, крім i -го, такі самі як в системі (2.2.1), а i -те рівняння має вигляд

$$\sum_{k=1}^n (a_{ik} + \lambda a_{lk})x_k = b_i + \lambda b_l. \quad (2.2.2)$$

Якщо (c_1, c_2, \dots, c_n) — розв'язок системи (2.2.1), то він задовольняє всі рівняння нової системи крім, можливо, рівняння (2.2.2). Покажемо, що він задоволяє і це останнє рівняння. Для цього додамо до рівності $\sum_{k=1}^n a_{ik}c_k = b_i$ рівність $\sum_{k=1}^n a_{lk}c_k = b_l$, домножену на λ . Одержано

$$\sum_{k=1}^n (a_{ik} + \lambda a_{lk})c_k = b_i + \lambda b_l.$$

Отже, кожний розв'язок системи (2.2.1) є розв'язком перетвореної системи. Але від перетвореної системи можна перейти до початкової теж за допомогою елементарних перетворень. Для елементарного перетворення первого типу (перестановок рівнянь) це очевидно, а для того, щоб одержати початкову систему (2.2.1) з нової системи, в якій всі рівняння крім i -го такі ж і в системі (2.2.1), а i -те має вигляд (2.2.2), потрібно l -те рівняння перетвореної системи домножити на $-\lambda$ і додати результат до i -го рівняння. Звідси випливає, що кожний розв'язок перетвореної системи є розв'язком системи (2.2.1). Випадок елементарних перетворень третього типу є очевидним. \square

Зрозуміло, що виконання елементарних перетворень над системою лінійних рівнянь зводиться до таких самих елементарних перетворень її розширеної матриці. Ми знаємо, що матрицю можна звести до східчастого вигляду елементарними перетвореннями. Тому з доведеної теореми випливає такий важливий наслідок.

Наслідок 2.2.3. *Система лінійних рівнянь (2.2.1) еквівалентна східчастій системі, тобто системі вигляду*

$$\left\{ \begin{array}{rcl} a_{1k_1}x_{k_1} + a_{1k_1+1}x_{k_1+1} + \cdots + a_{1n}x_n & = & b_1, \\ a_{2k_2}x_{k_2} + \cdots + a_{2n}x_n & = & b_2, \\ \dots & \dots & \dots \\ a_{sk_s}x_{k_s} + \cdots + a_{sn}x_n & = & b_s, \\ 0 & = & b_{s+1}, \end{array} \right. \quad (2.2.3)$$

де $a_{ik_i} \neq 0$, $1 \leq i \leq s$, $k_1 < k_2 < \cdots < k_s$. Тут $s+1 \leq m$, оскільки при зведенні розширеної матриці системи (2.2.1) до східчастого вигляду можуть з'являтися нульові рядки.

Для зручності дослідження системи (2.2.3) зробимо в ній деякі перепозначення. Позначимо $x_{k_j} = y_j$, $x_j = y_{k_j}$, $a_{ik_j} = a'_{ij}$, $a_{ij} = a_i k'_j$ для $1 \leq j \leq s$ та $x_j = y_j$, $a_{ij} = a'_{ij}$ для $j \notin \{1, \dots, s, k_1, \dots, k_s\}$.

В нових позначеннях система (2.2.3) прийме вигляд

$$\left\{ \begin{array}{lcl} a'_{11}y_1 + a'_{12}y_2 + \cdots + a'_{1n}y_n & = & b_1, \\ a'_{22}y_2 + \cdots + a'_{2n}y_n & = & b_2, \\ \cdots \cdots \cdots & \cdots & \cdots \\ a'_{ss}y_s + \cdots + a'_{sn}y_n & = & b_s, \\ 0 & = & b_{s+1}, \end{array} \right.$$

де $a'_{11} \neq 0, \dots, a'_{ss} \neq 0$.

Підсумовуючи, можемо стверджувати, що кожна система лінійних рівнянь (2.2.1) з точністю до нумерації невідомих еквівалентна системі лінійних рівнянь вигляду

$$\left\{ \begin{array}{lcl} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n & = & b_1, \\ a_{22}x_2 + a_{23}x_3 + \cdots + a_{2n}x_n & = & b_2, \\ \cdots \cdots \cdots & \cdots & \cdots \\ a_{ss}x_s + \cdots + a_{sn}x_n & = & b_s, \\ 0 & = & b_{s+1}, \end{array} \right. \quad (2.2.4)$$

де $a_{11} \neq 0, \dots, a_{ss} \neq 0$. Якщо система лінійних рівнянь має вигляд (2.2.4), то кажуть, що вона має *нормальний східчастий вигляд*. Зауважимо, що як в (2.2.3) так і в (2.2.4) ми не вимагаємо, щоб $b_{s+1} \neq 0$. Крім цього, в (2.2.3) і в (2.2.4) не виключається випадок $s = 0$. В цьому випадку (2.2.4) зводиться до $0 = 0$, якщо $b_1 = 0$ або до $0 = b_1$, якщо $b_1 \neq 0$.

2.2.3. Аналіз можливих випадків

Ми вже знаємо, що з точністю до нумерації невідомих кожна система лінійних рівнянь еквівалентна системі вигляду (2.2.4). Систему (2.2.4) легко дослідити.

- 1) Якщо $b_{s+1} \neq 0$ (тобто східчасти матриця системи містить ненульовий рядок $(0, \dots, 0|b)$), то система несумісна.
- 2) Нехай $b_{s+1} = 0$ і $s < n$. Тоді система (2.2.4) має більше, ніж один розв'язок, причому x_1, \dots, x_s можна знайти однозначно для будь-якого набору значень для невідомих x_{s+1}, \dots, x_n . У цьому

випадку невідомі x_1, \dots, x_s називають основними, а всі інші — вільними. Якщо поле P нескінченне, то в цьому випадку система має безліч розв'язків.

3) Якщо $b_{s+1} = 0$ і $s = n$, то очевидно, що система має єдиний розв'язок.

2.2.4. Лема Гауса

Систему лінійних рівнянь називають *однорідною*, якщо вона має вигляд

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + \dots + a_{2n}x_n = 0, \\ \dots\dots\dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = 0, \end{cases} \quad (2.2.5)$$

тобто всі вільні члени цієї системи дорівнюють нулю. Система (2.2.5) сумісна, вона має нульовий розв'язок.

Лема 2.2.1. Якщо в системі (2.2.5) $m < n$, то ця система має ненульовий розв'язок.

Доведення. Елементарними перетвореннями систему (2.2.5) можемо звести до нормального східчастого вигляду (2.2.4), де $b_1 = \dots = b_{s+1} = 0$. У нашому випадку $s \leq m < n$, тому система має ненульовий розв'язок. Вона має безліч розв'язків, якщо основне поле P нескінченне. \square

Зauważення 2.2.1. Викладений в цьому параграфі метод зведення систем лінійних рівнянь до східчастого вигляду належить К.Ф. Гаусу (1777–1855), тому його називають *методом Гауса*.

2.3. Визначники

2.3.1. Аксіоматичне означення визначника

Нехай нам дано квадратну матрицю A порядку n з елементами з деякого поля P

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

Позначимо через $\vec{a}_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$ i -ий стовпчик матриці A . Тоді матрицю A можна записати у вигляді $A = (\vec{a}_1, \dots, \vec{a}_n)$.

Означення 2.3.1. *Визначником* називається відображення F_n множини квадратних матриць порядку n з елементами поля P в поле P , яке задовольняє таким властивостям:

- 1) Лінійність за стовпчиками:

$$\begin{aligned} F_n((\vec{a}_1, \dots, \lambda \vec{a}'_i + \mu \vec{a}''_i, \dots, \vec{a}_n)) &= \\ &= \lambda F_n((\vec{a}_1, \dots, \vec{a}'_i, \dots, \vec{a}_n)) + \mu F_n((\vec{a}_1, \dots, \vec{a}''_i, \dots, \vec{a}_n)), \end{aligned}$$

де $\lambda, \mu \in P$.

- 2) Кососиметричність: $F_n((\vec{a}_1, \dots, \vec{a}, \dots, \vec{a}, \dots, \vec{a}_n)) = 0$, тобто визначник матриці, що має два однакові стовпчики, дорівнює нулю.
- 3) Нормування: $F_n(E) = 1$, тобто визначник одиничної матриці дорівнює одиниці.

Значення визначника на матриці A називається визначником цієї матриці і позначається $|A|$ або $\det A$.

2.3.2. Найпростіші властивості визначників

Лема 2.3.1. Якщо матриця A містить нульовий стовпчик, то $F_n(A) = 0$.

Доведення. Маємо

$$\begin{aligned} F_n((\vec{a}_1, \dots, \vec{0}, \dots, \vec{a}_n)) &= F_n((\vec{a}_1, \dots, 0 \cdot \vec{a}, \dots, \vec{a}_n)) = \\ &= 0 \cdot F_n((\vec{a}_1, \dots, \vec{a}, \dots, \vec{a}_n)) = 0 \end{aligned}$$

в силу лінійності визначника. \square

Лема 2.3.2. При домноженні будь-якого стовпчика матриці A на скаляр визначник домножується на цей же скаляр.

Доведення. Прийнявши в 1) $\mu = 0$, одержимо

$$\begin{aligned} F_n((\vec{a}_1, \dots, \lambda \vec{a}'_i + 0 \cdot \vec{a}''_i, \dots, \vec{a}_n)) &= \\ &= \lambda F_n((\vec{a}_1, \dots, \vec{a}'_i, \dots, \vec{a}_n)) + 0 \cdot F_n((\vec{a}_1, \dots, \vec{a}''_i, \dots, \vec{a}_n)) = \\ &= \lambda F_n((\vec{a}_1, \dots, \vec{a}'_i, \dots, \vec{a}_n)). \end{aligned}$$

\square

Лема 2.3.3. Якщо два стовпчики матриці переставити місцями, то визначник змінює знак на протилежний.

Доведення. Нехай $A = (\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_j, \dots, \vec{a}_n)$, $B = (\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_i, \dots, \vec{a}_n)$. Тоді

$$F_n((\vec{a}_1, \dots, \vec{a}_i + \vec{a}_j, \dots, \vec{a}_i + \vec{a}_j, \dots, \vec{a}_n)) = 0$$

за кососиметричністю визначника. Звідси, в силу лінійності визначника, маємо

$$\begin{aligned} F_n((\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_i, \dots, \vec{a}_n)) + F_n((\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_j, \dots, \vec{a}_n)) + \\ + F_n((\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_i, \dots, \vec{a}_n)) + F_n((\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_j, \dots, \vec{a}_n)) = 0. \end{aligned}$$

Оскільки відображення F_n кососиметричне, то звідси випливає, що

$$F_n((\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_i, \dots, \vec{a}_n)) + F_n((\vec{a}_1, \dots, \vec{a}_j, \dots, \vec{a}_j, \dots, \vec{a}_n)) = 0,$$

тобто $F_n(B) = -F_n(A)$. \square

Лема 2.3.4. Якщо матрицю $B = (\vec{a}_{i_1}, \dots, \vec{a}_{i_n})$ одержано з матриці $A = (\vec{a}_1, \dots, \vec{a}_n)$ за допомогою перестановки стовпчиків матриці A , то $F_n(B) = (-1)^{\text{sgn}\sigma} F_n(A)$, де $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ і $\text{sgn}\sigma$ – сигнатуря підстановки σ .

Доведення. Розкладемо підстановку σ в добуток транспозицій, тоді матрицю B можна одержати з матриці A послідовною перестановкою стовпчиків з номерами, вказаними у цих транспозиціях. При кожній такій перестановці, в силу леми 2.3.3, знак визначника зміниться на протилежний. Оскільки для парної підстановки σ число транспозицій парне, то $F_n(B) = F_n(A)$. Якщо ж σ непарна, то число транспозицій теж непарне і тому $F_n(B) = -F_n(A)$. Об'єднавши ці випадки, одержуємо $F_n(B) = (-1)^{\text{sgn}\sigma} F_n(A)$. \square

Лема 2.3.5. Якщо стовпчики матриці лінійно залежні, то визначник цієї матриці дорівнює нулю.

Доведення. Оскільки стовпчики лінійно залежні, то один з них є лінійною комбінацією інших. Нехай, наприклад, $\vec{a}_1 = \lambda_2 \vec{a}_2 + \dots + \lambda_n \vec{a}_n$, $\lambda_i \in P$. Тоді $F_n(\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n) = F_n((\lambda_2 \vec{a}_2 + \dots + \lambda_n \vec{a}_n, \vec{a}_2, \dots, \vec{a}_n)) = \lambda_2 F_n((\vec{a}_2, \vec{a}_2, \dots, \vec{a}_n)) + \dots + \lambda_n F_n((\vec{a}_n, \vec{a}_2, \dots, \vec{a}_n)) = \lambda_1 \cdot 0 + \dots + \lambda_n \cdot 0 = 0$. \square

Лема 2.3.6. Якщо до якого-небудь стовпчика матриці додати лінійну комбінацію інших стовпчиків, то визначник не зміниться.

Доведення. Нехай до i -го стовпчика матриці A додається лінійна комбінація інших стовпчиків. Враховуючи лінійність F_n за стовпчиками та попередню лему 2.3.5, одержимо

$$\begin{aligned} F_n((\vec{a}_1, \dots, \vec{a}_i + \sum_{j \neq i} \lambda_j \vec{a}_j, \dots, \vec{a}_n)) &= F_n((\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_n)) + \\ &+ F_n((\vec{a}_1, \dots, \vec{a}_{i-1}, \sum_{j \neq i} \lambda_j \vec{a}_j, \vec{a}_{i+1}, \dots, \vec{a}_n) \vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_n)) + 0 = \\ &= F_n((\vec{a}_1, \dots, \vec{a}_i, \dots, \vec{a}_n)). \end{aligned}$$

\square

2.3.3. Основна формула аксіоматичної теорії визначників

Розглянемо дві квадратні матриці A і C порядку n . Припустимо, що стовпчики матриці C є лінійними комбінаціями стовпчиків матриці A , тобто, припустимо, що якщо $A = (\vec{a}_1, \dots, \vec{a}_n)$, $C = (\vec{c}_1, \dots, \vec{c}_n)$, то

$$\vec{c}_j = \begin{pmatrix} c_{1j} \\ \vdots \\ c_{nj} \end{pmatrix} = \sum_{k=1}^n b_{kj} \vec{a}_k = \sum_{k=1}^n b_{kj} \begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix}.$$

Звідси бачимо, що $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$. Це означає, що $C = AB$, де $B = [b_{ij}]$ — матриця, складена з елементів b_{ij} . Розглянемо визначник матриці C :

$$F_n(C) = F_n\left(\sum_{k_1=1}^n b_{k_1 1} \vec{a}_{k_1}, \dots, \sum_{k_i=1}^n b_{k_i i} \vec{a}_{k_i}, \dots, \sum_{k_n=1}^n b_{k_n n} \vec{a}_{k_n}\right).$$

В силу лінійності визначника одержуємо

$$\begin{aligned} F_n(C) &= \sum_{k_1=1}^n b_{k_1 1} F_n\left(\vec{a}_{k_1}, \dots, \sum_{k_i=1}^n b_{k_i i} \vec{a}_{k_i}, \dots, \sum_{k_n=1}^n b_{k_n n} \vec{a}_{k_n}\right) = \\ &= \sum_{k_1=1}^n \dots \sum_{k_i=1}^n \dots \sum_{k_n=1}^n b_{k_1 1} \dots b_{k_i i} \dots b_{k_n n} F_n(\vec{a}_{k_1}, \dots, \vec{a}_{k_i}, \dots, \vec{a}_{k_n}). \end{aligned}$$

Ця n -кратна сума має багато нульових доданків. А саме, якщо серед індексів k_1, \dots, k_n є однакові, то $F_n(\vec{a}_{k_1}, \dots, \vec{a}_{k_n}) = 0$ як визначник матриці з двома одинаковими стовпчиками (власність кососиметричності визначника). Тому, пропускаючи ці нульові доданки, ми одержимо суму, доданки якої відповідають перестановкам (k_1, \dots, k_n) чисел $1, \dots, n$ або, що означає те саме, підстановкам $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$. Отже,

$$F_n(C) = \sum_{\sigma} = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} b_{k_1 1} \dots b_{k_n n} F_n(\vec{a}_{k_1}, \dots, \vec{a}_{k_n}).$$

Використовуючи лему 2.3.4 та рівність $C = AB$, звідси одержуємо

$$\begin{aligned} F_n(AB) &= F_n(C) = \\ &= \sum_{\sigma=\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{smallmatrix}\right)} (-1)^{\operatorname{sgn}\sigma} b_{k_1 1} \dots b_{k_n n} F_n(\vec{a}_1, \dots, \vec{a}_n). \quad (2.3.1) \end{aligned}$$

Формулу (2.3.1) називають основною формuloю аксіоматичної теорії визначників.

2.3.4. Єдиність визначника

Підставимо у формулу (2.3.1) замість матриці A одиничну матрицю E . Тоді $C = B$, $F_n(\vec{a}_1, \dots, \vec{a}_n) = 1$ і формула (2.3.1) дає формулу

$$F_n(C) = \sum_{\sigma} = \left(\begin{smallmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{smallmatrix}\right) (-1)^{\operatorname{sgn}\sigma} c_{k_1 1} \dots c_{k_n n}, \quad (2.3.2)$$

яку можна прочитати так: визначник матриці C дорівнює сумі $n!$ доданків, кожний з яких є добутком елементів матриці, взятих по одному з кожного стовпчика і з кожного рядка, причому такий добуток входить у суму зі знаком “+”, якщо підстановка σ парна і зі знаком “-”, якщо ця підстановка непарна.

З формули (2.3.2) випливає єдиність визначника. Справді, формула (2.3.2) означає, що коли існує відображення F_n , яке має властивості лінійності за стовпчиками, кососиметричності та нормування, то значення $F_n(C)$ може бути обчислене єдиним способом за формулою (2.3.2).

2.3.5. Визначник транспонованої матриці та визначник добутку матриць

Формулу (2.3.2) можна прочитати ще й так: визначник матриці C дорівнює сумі $n!$ доданків, кожний з яких є добутком елементів матриці, взятих по одному, з кожного рядка і з кожного

стовпчика, причому такий добуток входить у суму зі знаком “+”, якщо підстановка утворена номерами відповідних рядків і стовпчиків парна і зі знаком “−”, якщо ця підстановка непарна. Отже, формулу (2.3.2) можна записати у вигляді

$$F_n(C) = \sum_{\sigma=\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{smallmatrix}\right)} (-1)^{\operatorname{sgn}\sigma} c_{1k_1} c_{2k_2} \dots c_{nk_n}, \quad (2.3.3)$$

оскільки підстановки σ та σ^{-1} мають однакову парність. Звідси легко випливає наступна важлива властивість визначників.

Твердження 2.3.1. $F_n(C) = F_n(C^t)$, де C^t – транспонована матриця. Інакше кажучи, визначник матриці не змінюється при транспонуванні.

Доведення. Нехай $C = [c_{ij}]$, $C^t = [c_{ij}^t]$, $c_{ij}^t = c_{ji}$. Тому з формулі (2.3.2) одержуємо, використовуючи (2.3.3),

$$\begin{aligned} F_n(C^t) &= \sum_{\sigma=\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{smallmatrix}\right)} (-1)^{\operatorname{sgn}\sigma} c_{k_1 1}^t c_{k_2 2}^t \dots c_{k_n n}^t = \\ &= \sum_{\sigma=\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{smallmatrix}\right)} (-1)^{\operatorname{sgn}\sigma} c_{1k_1} c_{2k_2} \dots c_{nk_n} = F_n(C). \end{aligned}$$

□

Наслідок 2.3.2. Кожна властивість визначника, сформульована в термінах стовпчиків та рядків матриці A , залишається вірною, якщо в її формуллюванні кожне слово “рядок” замінити словом “стовпчик” і навпаки.

Зокрема, визначник має властивості лінійності за рядками, кососиметричності за рядками, а також такі властивості:

- 1') Якщо матриця A містить нульовий рядок, то $F_n(A) = 0$.
- 2') При домноженні будь-якого рядка матриці A на скаляр визначник домножується на цей же скаляр.

- 3') Якщо два рядки переставити місцями, то визначник змінює знак на протилежний.
- 4') Якщо до рядка матриці додати лінійну комбінацію інших рядків, то визначник матриці не зміниться.

Твердження 2.3.3.

$$F_n(AB) = F_n(A)F_n(B), \quad (2.3.4)$$

тобто визначник добутку матриць дорівнює добутку їх визначників.

Доведення. Запишемо формулу (2.3.1) у вигляді

$$F_n(AB) = F_n(A) \sum_{\sigma=\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{smallmatrix}\right)} (-1)^{\operatorname{sgn}\sigma} b_{k_1 1} \dots b_{k_n n},$$

де сума справа дорівнює $F_n(B)$ за формулою (2.3.2). Отже, $F_n(AB) = F_n(A)F_n(B)$. \square

2.3.6. Існування визначника n -го порядку

Формула (2.3.2) задає відображення з множини квадратних матриць порядку n з елементами з поля P в поле P . Переконасмося, що це відображення володіє властивостями 1)-3) з означення визначника. Це означатиме, що визначники існують. Зауважимо, що всі дотепер доведені властивості визначників (включно з формулою (2.3.2)) доведені за умови, що відображення F_n існує. Отже, перевіряємо властивості лінійності, кососиметричності та нормування для відображення F_n , заданого формулою (2.3.2).

1) Лінійність. Нехай $A = (\vec{a}_1, \dots, \lambda\vec{a}'_i + \mu\vec{a}''_i, \dots, \vec{a}_n)$. Тоді

$$\begin{aligned} F_n(A) &= \sum_{\sigma \in S_n} (-1)^{\text{sgn}\sigma} a_{k_1 1} \dots (\lambda a'_{k_i i} + \mu a''_{k_i i}) \dots a_{k_n n} = \\ &= \lambda \sum_{\sigma \in S_n} (-1)^{\text{sgn}\sigma} a_{k_1 1} \dots a'_{k_i i} \dots a_{k_n n} + \\ &\quad + \mu \sum_{\sigma \in S_n} (-1)^{\text{sgn}\sigma} a_{k_1 1} \dots a''_{k_i i} \dots a_{k_n n} = \\ &= \lambda F_n(\vec{a}_1, \dots, \vec{a}'_i, \dots, \vec{a}_n) + \mu F_n(\vec{a}_1, \dots, \vec{a}''_i, \dots, \vec{a}_n). \end{aligned}$$

2) Кососиметричність. Запишемо формулу (2.3.2) для матриці $A = (\vec{a}_1, \dots, \vec{a}_n)$:

$$F_n(A) = \sum_{\sigma \in S_n} (-1)^{\text{sgn}\sigma} a_{k_1 1} \dots a_{k_n n}. \quad (2.3.5)$$

Нехай матриця A має однакові i -ий та j -ий стовпчики: $\vec{a}_i = \vec{a}_j$.
Тоді

$$a_{k_i i} = a_{k_j i} \text{ та } a_{k_j i} = a_{k_i j}. \quad (2.3.6)$$

Разом з кожним доданком

$$(-1)^{\text{sgn}(\frac{1}{k_1} \dots \frac{i}{k_i} \dots \frac{j}{k_j} \dots \frac{n}{k_n})} a_{k_1 1} \dots a_{k_i i} \dots a_{k_j j} \dots a_{k_n n}, \quad (2.3.7)$$

що входить в суму (2.3.5), в неї входить і доданок

$$(-1)^{\text{sgn}(\frac{1}{k_1} \dots \frac{i}{k_j} \dots \frac{j}{k_i} \dots \frac{n}{k_n})} a_{k_1 1} \dots a_{k_j i} \dots a_{k_i j} \dots a_{k_n n}. \quad (2.3.8)$$

Доданки (2.3.7) і (2.3.8) відрізняються лише знаком. Це випливає з (2.3.6) і з того, що підстановки $(\frac{1}{k_1} \dots \frac{i}{k_i} \dots \frac{j}{k_j} \dots \frac{n}{k_n})$ та $(\frac{1}{k_1} \dots \frac{i}{k_j} \dots \frac{j}{k_i} \dots \frac{n}{k_n})$ мають протилежну парність. Тому, при наших припущеннях, всі доданки в (2.3.5) скорочуються, отже, $F_n(A) = 0$.

3) Нормування. Ця властивість очевидна, тому що для одиничної матриці A в формулі (2.3.5) справа є тільки один ненульовий доданок $a_{11}a_{22} \dots a_{nn} = 1 \cdot 1 \dots \cdot 1 = 1$.

2.3.7. Один практичний метод обчислення визначників

Припустимо, що матриця A є верхньою трикутною матрицею. Це означає, що всі елементи матриці A , розміщені нижче головної діагоналі (тобто елементи a_{ij} з $i > j$), дорівнюють нулю. Таку матрицю A звичайно записують у вигляді

$$A = \begin{pmatrix} a_{11} & * \\ & \ddots \\ 0 & a_{nn} \end{pmatrix}.$$

За формулою (2.3.5), визначник матриці A є сумою доданків

$$(-1)^{\operatorname{sgn}\sigma} a_{k_1 1} \dots a_{k_n n}. \quad (2.3.9)$$

Але в нашому випадку $a_{k_i i} = 0$ для $k_i > i$, тому в сумі (2.3.5) можна залишити лише ті доданки, для яких

$$k_1 \leq 1, \quad k_2 \leq 2, \dots, k_n \leq n. \quad (2.3.10)$$

Додавши почленно ці нерівності, одержуємо $k_1 + k_2 + \dots + k_n \leq n(n+1)/2$. Але k_1, k_2, \dots, k_n є деякою перестановкою чисел $1, \dots, n$. Тому ліва частина останньої нерівності теж дорівнює $n(n+1)/2$. Звідси випливає, що кожна з нерівностей (2.3.10) мусить бути рівністю. А це означає, що в сумі (2.3.5) можна залишити, не змінюючи її, єдиний доданок $a_{11}a_{22} \dots a_{nn}$. Отже, маємо

Твердження 2.3.4. *Визначник верхньої трикутної матриці дорівнює добуткові її діагональних елементів.*

Звідси випливає практичний метод обчислення визначників: зводимо довільну квадратну матрицю A до східчастого вигляду за допомогою елементарних перетворень рядків (стовпчиків), враховуючи при цьому, що при перестановці двох рядків (стовпчиків) визначник змінює знак, а при додаванні до одного рядка (стовпчика) іншого, домноженого на скаляр, визначник не змінюється за властивістю 2.3.6 та наслідком з 2.3.2. Визначник східчастої матриці дорівнює добутку елементів, розміщених на головній діагоналі.

2.4. Мінори, алгебраїчні доповнення та теорема Лапласа

Якщо

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

— квадратна матриця з елементами з поля P , то визначник матриці A прийнято позначати $\det A$ або $|A|$, або

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

2.4.1. Мінори та алгебраїчні доповнення

Нехай $A = [a_{ij}]_{1 \leq i \leq n, 1 \leq j \leq m}$ — прямокутна матриця з елементами з поля P і $1 \leq k \leq \min\{m, n\}$.

Означення 2.4.1. *Мінором k -го порядку матриці A називається визначник матриці, складеної з елементів, що розміщені на перетині довільним способом вибраних k рядків і k стовпчиків матриці A .*

Приклад 2.4.1. Нехай $A = \begin{pmatrix} 1 & 9 & 9 & 7 \\ 1 & 0 & 3 & -1 \\ 0 & 8 & 9 & 1 \end{pmatrix}$.

a) $-1, 9, 3, 8$ — деякі з мінорів 1-го порядку матриці A . Ця матриця має всього 12 мінорів 1-го порядку, і деякі з них рівні між собою.

b) $\begin{vmatrix} 1 & 9 \\ 1 & 0 \end{vmatrix}, \begin{vmatrix} 0 & -1 \\ 8 & 1 \end{vmatrix}, \begin{vmatrix} 1 & -1 \\ 0 & 1 \end{vmatrix}$ — деякі з мінорів другого порядку.

c) $\begin{vmatrix} 1 & 9 & 9 \\ 1 & 0 & 3 \\ 0 & 8 & 9 \end{vmatrix}, \begin{vmatrix} 1 & 9 & 7 \\ 1 & 0 & -1 \\ 0 & 8 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 9 & 7 \\ 1 & 3 & -1 \\ 0 & 9 & 1 \end{vmatrix}, \begin{vmatrix} 9 & 9 & 7 \\ 0 & 3 & -1 \\ 8 & 9 & 1 \end{vmatrix}$ — всі мінори третього порядку.

Означення 2.4.2. Нехай $A = [a_{ij}]_{1 \leq i, j \leq n}$ — квадратна матриця, M — який-небудь мінор k -го порядку матриці A . Припустимо, що M проходить через i_1 -ий, \dots, i_k -ий рядки та j_1 -ий, \dots, j_k -ий

стовпчики (тобто M є визначником матриці, що складається з елементів, розміщених на перетині вказаних рядків і стовпчиків).

Доповняльним мінором M' мінора M називають визначник матриці, що одержується з A викресленням i_1 -го, \dots , i_k -го рядків та j_1 -го, \dots , j_k -го стовпчиків. *Алгебраїчним доповненням* A_M мінора M називають його доповняльний мінор M' , домножений на $(-1)^{i_1+\dots+i_k+j_1+\dots+j_k}$. Алгебраїчне доповнення елемента a_{ij} матриці A позначають A_{ij} . A_{ij} — визначник матриці, одержаної викресленням в матриці A i -го рядка та j -го стовпчика, домножений на $(-1)^{i+j}$.

2.4.2. Лема про добуток мінора на алгебраїчне доповнення

Лема 2.4.1. *Нехай M — мінор r -го порядку матриці A n -го порядку, A_M — алгебраїчне доповнення мінора M . Добуток $M \cdot A_M$ є сумаю $r!(n-r)!$ доданків, кожен з яких входить у суму $\det A = \sum_{\sigma \in S_n} (-1)^{\operatorname{sgn} \sigma} a_{1k_1} \dots a_{nk_n}$.*

Доведення. Доведемо спочатку частковий випадок цієї леми, а потім покажемо, що загальний випадок випливає з часткового.

а) *Частковий випадок.* Припустимо, що мінор M розміщений у лівому верхньому куті матриці A , тобто M проходить через перші r рядків та перші r стовпчиків матриці A . У цьому випадку алгебраїчне доповнення мінора M збігається з його доповняльним мінором:

$$M = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{vmatrix}, \quad A_M = \begin{vmatrix} a_{r+1r+1} & \dots & a_{r+1n} \\ a_{r+2r+1} & \dots & a_{r+2n} \\ \dots & \dots & \dots \\ a_{nr+1} & \dots & a_{nn} \end{vmatrix},$$

$$M \cdot A_M = \sum_{\sigma_1} (-1)^{\operatorname{sgn} \sigma_1} a_{1k_1} \dots a_{rk_r} \sum_{\sigma_2} (-1)^{\operatorname{sgn} \sigma_2} a_{r+1k_{r+1}} \dots a_{nk_n}, \quad (2.4.1)$$

де $\sigma_1 = \begin{pmatrix} 1 & 2 & \dots & r \\ k_1 & k_2 & \dots & k_r \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} r+1 & \dots & n \\ k_{r+1} & \dots & k_n \end{pmatrix}$. Перемноживши дві суми в (2.4.1), одержуємо

$$\begin{aligned} M \cdot A_M &= \sum_{\sigma_1, \sigma_2} (-1)^{\operatorname{sgn}\sigma_1 + \operatorname{sgn}\sigma_2} a_{1k_1} \dots a_{rk_r} a_{r+1k_{r+1}} \dots a_{nk_n} = \\ &= \sum_{\sigma'} (-1)^{\operatorname{sgn}\sigma'} a_{1k_1} \dots a_{rk_r} a_{r+1k_{r+1}} \dots a_{nk_n}, \end{aligned} \quad (2.4.2)$$

де $\sigma' = \begin{pmatrix} 1 & \dots & r & r+1 & \dots & n \\ k_1 & \dots & k_r & k_{r+1} & \dots & k_n \end{pmatrix}$. Зауважимо, що σ' тут означає будь-яку таку підстановку, яка множини $\{1, \dots, r\}$ та $\{r+1, \dots, n\}$ переводить у ці ж множини. Всього існує $r!(n-r)!$ таких підстановок σ' , отже, сума (2.4.2) складається з $r!(n-r)!$ доданків.

Залишається перевірити, що кожний доданок у сумі (2.4.2) має той самий знак, з яким він входить у визначник матриці A , тобто потрібно перевірити, що $(-1)^{\operatorname{sgn}\sigma_1 + \operatorname{sgn}\sigma_2} = (-1)^{\operatorname{sgn}\sigma'}$. Але це випливає з того, що сума кількостей інверсій підстановки σ' збігається з сумаю сум кількостей інверсій підстановок σ_1 та σ_2 .

б) Нехай тепер мінор M проходить через i_1 -ий, \dots , i_r -ий рядки та j_1 -ий, \dots , j_r -ий стовпчики. Переставимо рядки та стовпчики так, щоб мінор M виявився у лівому верхньому кутку матриці A' , яка одержиться з матриці A після всіх цих перестановок. Для цього потрібно зробити $i_1 - 1 + i_2 - 2 + \dots + i_r - r + j_1 - 1 + j_2 - 2 + \dots + j_r - r$ перестановок сусідніх рядків чи стовпчиків. Позначимо $s_M = i_1 + \dots + i_r + j_1 + \dots + j_r$. Тоді $\det A = (-1)^{s_M} \det A'$, тому що $r(r+1)$ — парне число. За доведеним, добуток мінора M та доповніального мінора M' є сумаю $r!(n-r)!$ доданків, кожний з яких входить у $\det A'$. Тому добуток $M \cdot A_M = M \cdot (-1)^{s_M} \cdot M'$ входить у $\det A$. \square

2.4.3. Теорема Лапласа

Теорема 2.4.1. *Виберемо в матриці A n -го порядку довільним способом r рядків. Тоді сума добутків мінорів, що розміщені*

ні в цих r рядках, на їх алгебраїчні доповнення дорівнює визначнику матриці A .

Доведення. Щоб задати мінор r -го порядку, який проходить через вказані r рядків, потрібно зафіксувати r стовпчиків матриці серед n стовпчиків. Це можна зробити $\frac{n!(n-r)!}{r!}$ способами. За попередньою лемою добуток мінора на його алгебраїчне доповнення складається з $(n-r)!r!$ доданків. Зрозуміло, що доданки, які виникають з добутків різних мінорів на їх алгебраїчні доповнення є різними. Отже, вказана у формулюванні теореми сума складається з $n!$ доданків, причому, знову ж таки за попередньою лемою, всі ці доданки входять у визначник матриці A з потрібними знаками. Тому вказана сума мусить дорівнювати визначнику матриці A . \square

Зауваження 2.4.1. Оскільки визначник матриці не змінюється при її транспонуванні, то теорема залишається вірною, якщо в її формулюванні слова “рядки” замінити на слова “стовпчики”.

2.4.4. Розклад визначника за рядком

Застосуємо теорему Лапласа до випадку, коли $r = 1$. Тоді ми маємо один рядок матриці A , нехай це буде i -ий рядок. Мінори 1-го порядку, що проходять через цей рядок, це просто елементи a_{ij} i -го рядка матриці A . Якщо A_{ij} — алгебраїчне доповнення a_{ij} , то теорема Лапласа дає нам формулу

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}, \quad (2.4.3)$$

яку називають формулою розкладу визначника матриці A за i -им рядком. Беручи до уваги зауваження 2.4.1, одержуємо ще одну формулу

$$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj} \quad (2.4.4)$$

— формулу розкладу визначника за j -им стовпчиком. Наступна лема узагальнює формули (2.4.3) і (2.4.4).

Лема 2.4.2. Нехай $\delta_{ij} = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$ — символ Кронекера. Тоді

$$\sum_{k=1}^n a_{ik} A_{jk} = \delta_{ij} \det A, \quad (2.4.5)$$

$$\sum_{k=1}^n a_{ki} A_{kj} = \delta_{ij} \det A, \quad (2.4.6)$$

де a_{ij} — елементи квадратної матриці A , A_{ij} — алгебраїчне доповнення елемента a_{ij} .

Доведення. У випадку $i = j$ формули (2.4.5) і (2.4.6) зводяться до формул (2.4.3) і (2.4.4). Нехай $i \neq j$. Розглянемо матрицю

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{i1} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix},$$

у якої i -ий та j -ий рядки однакові. Визначник матриці A дорівнює нульові, тому розкладши його за j -им рядком, одержуємо ($a_{ik} = a_{jk}!$) $a_{i1}A_{j1} + a_{i2}A_{j2} + \dots + a_{in}A_{jn} = 0$. Так само, використовуючи матрицю з двома однаковими стовпчиками, одержуємо рівність $a_{1i}A_{1j} + a_{2i}A_{2j} + \dots + a_{ni}A_{nj} = 0$. \square

2.5. Застосування визначників

2.5.1. Обернена матриця

Означення 2.5.1. Кажуть, що квадратна матриця $A \in M_n(P)$ є зворотною (оборотною), якщо існує матриця $B \in M_n(P)$ така, що $AB = BA = E$, де E — одинична матриця. Матрицю B називають оберненою до A і позначають A^{-1} .

Зауваження 2.5.1. Згідно твердження 1.2.1 з асоціативності добутку матриць випливає, що коли матриця B , обернена до матриці A існує, то вона єдина.

Матрицю A називають *невиродженою* матриця, якщо $\det A \neq 0$.

Теорема 2.5.1. *Матриця A має обернену тоді і тільки тоді, коли A невироджена.*

Доведення. Якщо A має обернену A^{-1} , то $1 = \det E = \det(AA^{-1}) = \det A \cdot \det A^{-1}$. Звідси випливає, що $\det A \neq 0$ і, крім того, що $\det A^{-1} = (\det A)^{-1}$. Нехай тепер $\det A \neq 0$ і $A = [a_{ij}]_1 \leq i, j \leq n$. Розглянемо *приєднану матрицю* \tilde{A} :

$$\tilde{A} = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} = [A_{ij}]^t,$$

тобто матрицю, транспоновану до матриці $[A_{ij}]$, елементами якої є алгебраїчні доповнення A_{ij} елементів матриці A . Перевіримо, що матриця $B = (\det A)^{-1} \tilde{A}$ є оберненою до A . Для цього обчислюємо добутки AB і BA , використовуючи формули (2.4.5) і (2.4.6):

$$\begin{aligned} AB &= \left[\sum_{k=1}^n a_{ik} (\det A)^{-1} A_{jk} \right] = \left[\frac{1}{\det A} \sum_{k=1}^n a_{ik} A_{jk} \right] = \\ &= \left[\frac{1}{\det A} \det A \cdot \delta_{ij} \right] = [\delta_{ij}] = E \end{aligned}$$

і так само

$$BA = \left[\sum_{k=1}^n (\det A)^{-1} A_{ki} a_{kj} \right] = \left[(\det A)^{-1} \sum_{k=1}^n a_{kj} A_{ki} \right] = E.$$

□

2.5.2. Теорема про ранг матриці

Нехай дано матрицю

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

з елементами з деякого поля P . Якщо розглянути стовпчики даної матриці як m -вимірні вектори, то вони можуть бути лінійно залежними.

Означення 2.5.2. Нехай матриця A має r лінійно незалежних стовпчиків, а кожні $r + 1$ стовпчиків матриці A є лінійно залежними. Тоді число r називають *рангом* матриці A за стовпчиками.

Аналогічно можна розглядати рядки матриці A як n -вимірні вектори і ввести в розгляд поняття рангу матриці за рядками. Але виявляється, що ранг матриці як за рядками, так і за стовпчиками один і той самий. Доведення цього несподіваного результату отримаємо за допомогою ще одного визначення рангу матриці. Виберемо в матриці A довільні s рядків та s стовпчиків, $s \leq \min\{m, n\}$. Ми вже знаємо, що *мінором* s -го порядку називають визначник, утворений елементами, що стоять на перетині вибраних рядків і стовпчиків.

Теорема 2.5.2 (про ранг матриці). *Максимальний порядок відмінних від нуля мінорів матриці дорівнює рангу матриці за стовпчиками.*

Доведення. Нехай максимальний відмінний від нуля мінор Δ r -го порядку розташований у лівому верхньому куті матриці (цьо-

го можна добитися перестановкою рядків і стовпчиків).

$$A = \begin{pmatrix} a_{11} & \dots & a_{1r} & a_{1r+1} & \dots & a_{1n} \\ \dots & & \dots & \dots & & \dots \\ a_{r1} & \dots & a_{rr} & a_{rr+1} & \dots & a_{rn} \\ a_{r+11} & \dots & a_{r+1r} & a_{r+1r+1} & \dots & a_{r+1n} \\ \dots & & \dots & \dots & & \dots \\ a_{m1} & \dots & a_{mr} & a_{mr+1} & \dots & a_{mn} \end{pmatrix},$$

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \dots & & \dots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0.$$

Перші r стовпчиків матриці лінійно незалежні. Справді, якби вони були лінійно залежними, то такими були б і стовпчики мінора, а тоді він дорівнював би нулю, бо один з його стовпчиків був би лінійною комбінацією інших, а це суперечить нашому припущення.

Доведемо, що кожний стовпчик, починаючи з $r + 1$ -го і до n -го, є лінійною комбінацією перших r стовпчиків (з цього випливає, що максимальне число лінійно незалежних стовпчиків матриці дорівнює r , що і треба довести). Для цього облямуємо наш мінор j -им стовпчиком ($r < j \leq n$) та i -им рядком, $r + 1 \leq j \leq n$, $1 \leq i \leq m$; одержаний мінор $r + 1$ -го порядку за умовою теореми дорівнює нулю:

$$M = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1j} \\ \dots & & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{rj} \\ \dots & & \dots & \dots \\ a_{i1} & \dots & a_{ir} & a_{ij} \end{vmatrix} = 0.$$

Розкладемо цей мінор за останнім рядком: $a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{ir}A_{ir} + a_{ij}\Delta = 0$. Оскільки $\Delta \neq 0$, то $a_{ij} = -\frac{A_{i1}}{\Delta}a_{i1} - \frac{A_{i2}}{\Delta}a_{i2} - \dots - \frac{A_{ir}}{\Delta}a_{ir}$.

Тому можна записати, враховуючи, що A_{i1}, \dots, A_{ir} не зале-

жать від i :

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = -\frac{A_{i1}}{\Delta} \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} - \frac{A_{i2}}{\Delta} \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} - \cdots - \frac{A_{ir}}{\Delta} \begin{pmatrix} a_{1r} \\ \vdots \\ a_{mr} \end{pmatrix},$$

для всіх $j = r + 1, \dots, n$. Отже, кожний стовпчик матриці є лінійною комбінацією її перших r стовпчиків, що й треба було довести. \square

Як наслідок теореми про ранг матриці, одержуємо, що ранги за стовпчиками і за рядками однакові. Справді, досить розглянути транспоновану матрицю і застосувати теорему. Отже, ми довели таку теорему.

Теорема 2.5.3. *Ранги матриці A за рядками і за стовпчиками є однаковими і дорівнюють максимальному порядку відмінних від нуля мінорів матриці A .*

Часто максимальний порядок відмінних від нуля мінорів матриці називають рангом матриці за мінорами.

Як інший очевидний наслідок, одержимо теорему.

Теорема 2.5.4. *Визначник n -го порядку дорівнює нулю тоді і тільки тоді, коли його рядки (стовпчики) лінійно залежні.*

Доведення. Необхідність. Нехай A — квадратна матриця і $\det A = 0$, тоді $\text{rank } A < n$ (за теоремою про ранг). Отже, стовпчики (рядки) матриці A лінійно залежні.

Достатність — це одна з властивостей визначника. \square

2.5.3. Теорема Кронекера-Капеллі

Нехай дано систему лінійних рівнянь з коефіцієнтами з поля P :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \cdots \cdots \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m. \end{cases} \quad (2.5.1)$$

Питання про сумісність системи (2.5.1) цілком розв'язується наступною теоремою.

Теорема 2.5.5. *Система лінійних рівнянь (2.5.1) сумісна тоді і тільки тоді, коли ранг матриці системи дорівнює рангу розширеної матриці.*

Доведення. Нехай $\text{rank}A = \text{rank}A_b$, де A та A_b — відповідно матриця та розширена матриця системи 2.5.1. Тоді довільна максимальна лінійно незалежна система стовпчиків матриці A є максимальною лінійно незалежною системою стовпчиків матриці A_b ; через цю систему стовпчиків матриці A лінійно виражається і останній стовпчик матриці A_b . Інакше кажучи, існують такі скаляри c_1, \dots, c_n , що сума стовпчиків матриці A , взятих з коефіцієнтами

c_1, \dots, c_n , дорівнює стовпчику вільних членів, тобто t_1, \dots, t_n є розв'язком системи (2.5.1).

Якщо система (2.5.1) сумісна, а c_1, \dots, c_n — її довільний розв'язок, то бачимо, що останній стовпчик матриці A_b є сумаю стовпчиків матриці A , взятих з коефіцієнтами c_1, \dots, c_n . Отже, довільний стовпчик матриці A_b лінійно виражається через стовпчики матриці A . Це означає, що лінійні оболонки стовпчиків матриці A і стовпчиків матриці A_b збігаються. Тому максимальне число лінійно незалежних стовпчиків матриць A і A_b однакове (це розмірність лінійної оболонки стовпчиків матриці A), тобто $\text{rank}A = \text{rank}A_b$. \square

Теорема Кронекера-Капеллі дає нам лише умову існування розв'язку, але вона не дає практичного способу для пошуку всіх розв'язків. Зауважимо, що одним з практичних методів розв'язування систем лінійних рівнянь є метод Гауса. Він дуже зручний на практиці, зате його важко застосовувати в теоретичних питаннях. Тому розглянемо ще деякі методи дослідження та розв'язування систем лінійних рівнянь.

2.5.4. Формули Крамера

Означення 2.5.3. Система лінійних рівнянь

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \dots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases} \quad (2.5.2)$$

називається *системою Крамера*, якщо визначник Δ матриці цієї системи не дорівнює нулю.

Нехай $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ — матриця системи (2.5.2). Позначимо $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ — стовпчик невідомих і $\vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ — стовпчик вільних членів. Тоді систему (2.5.2) можна записати у матричному вигляді

$$A\vec{x} = \vec{b}. \quad (2.5.3)$$

Позначимо

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}, \quad \Delta_i = \begin{vmatrix} a_{11} & \dots & b_1 & \dots & a_{1n} \\ a_{21} & \dots & b_2 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & b_n & \dots & a_{nn} \end{vmatrix}$$

— визначник матриці, одержаної з A заміною її i -го стовпчика на стовпчик вільних членів. В цих позначеннях вірна така теорема

Теорема 2.5.6. Система Крамера (2.5.2) має єдиний розв'язок, що дається формулами $x_i = \frac{\Delta_i}{\Delta}$.

Доведення. За теоремою Кронекера-Капеллі система Крамера завжди сумісна. Справді, ранг її матриці дорівнює n , а ранг розширеної матриці теж мусить дорівнювати n , бо вона має n рядків. Далі, оскільки $\Delta = \det A \neq 0$, то існує A^{-1} . Домноживши матричну рівність (2.5.3) на A^{-1} , одержимо $A^{-1}(A\vec{x}) = A^{-1}\vec{b}$,

тобто $\vec{x} = A^{-1}\vec{b}$. Пригадавши, що $A^{-1} = \frac{1}{\Delta}[A_{ij}^t]$, одержуємо для i -ої компоненти вектора \vec{x} :

$$x_i = \frac{1}{\Delta} \sum_{k=1}^n A_{ki} b_k = \frac{\Delta_i}{\Delta}.$$

□

2.5.5. Рангові та вільні невідомі системи лінійних рівнянь

Нехай матриця A системи (2.5.1) має ранг $r > 0$. Оскільки A містить всього n стовпчиків, то $r \leq n$. Матриця A має ненульовий мінор M порядку r , який належить l_1, \dots, l_r -му рядку та i_1, \dots, i_r -му стовпчику матриці A . За теоремою про ранг, l_1, \dots, l_r -ий рядки матриці A_b системи (2.5.1) лінійно незалежні, а всі інші її рядки є лінійними комбінаціями вказаних рядків. Тому, залишивши в системі (2.5.1) лише l_1, \dots, l_r -е рівняння, ми отримаємо систему лінійних рівнянь, еквівалентну початковій системі (2.5.1). Тепер, залишивши в цих рівняннях зліва лише члени, які містять x_{i_1}, \dots, x_{i_r} , і переносячи вправо інші члени, ми зведемо дану систему до вигляду

$$\begin{cases} a_{l_1 i_1} x_{i_1} + \dots + a_{l_1 i_r} x_{i_r} = y_1, \\ \dots \\ a_{l_r i_1} x_{i_1} + \dots + a_{l_r i_r} x_{i_r} = y_r, \end{cases} \quad (2.5.4)$$

де $y_s = -a_{l_s j_1} x_{j_1} - \dots - a_{l_s j_{n-r}} x_{j_{n-r}} + b_{l_s}$, $s = 1, \dots, r$. Надавши невідомим $x_{j_1}, \dots, x_{j_{n-r}}$ довільних значень $d_{j_1}, \dots, d_{j_{n-r}} \in P$, з системи (2.5.4) одержимо систему Крамера, яка має єдиний розв'язок d_{i_1}, \dots, d_{i_r} . Очевидно, $d_{i_1}, \dots, d_{i_r}, d_{j_1}, \dots, d_{j_{n-r}}$ є розв'язком системи (2.5.1). Назвемо невідомі $x_{j_1}, \dots, x_{j_{n-r}}$ вільними невідомими, а x_{i_1}, \dots, x_{i_r} — ранговими невідомими.

Звідси ми одержуємо правило для розв'язання довільної системи лінійних рівнянь.

Якщо задано сумісну систему лінійних рівнянь (2.5.1) і матриця A системи має ранг r , то виберемо в A r лінійно незалежних рядків і залишимо в системі (2.5.1) лише рівняння, коефіцієнти яких ввійшли у вибрані рядки. В цих рівняннях залишимо у лівих частинах такі r невідомих, що визначник матриці з коефіцієнтів при них відмінний від нуля, а інші невідомі (їх назовемо *вільними*) переносимо в праву частину рівнянь. Надаючи вільним невідомим довільні значення з поля P і обчислюючи значення інших невідомих, ми одержимо всі розв'язки системи.

2.5.6. Фундаментальна система розв'язків

Розглянемо однорідну систему лінійних рівнянь

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0, \\ \dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0. \end{cases} \quad (2.5.5)$$

Будемо трактувати розв'язки системи (2.5.5) як вектори $\vec{c} = (c_1, c_2, \dots, c_n)^t \in P^n$. Індекс t означає транспонування, отже, \vec{c} означає вектор-стовпчик.

Лема 2.5.1. *Множина розв'язків системи (2.5.5) утворює підпростір простору P^n .*

Доведення. Нехай \vec{a} і \vec{b} — розв'язки, $\vec{0}$ — нульовий вектор-стовпчик. Тоді маємо матричні рівності $A\vec{a} = \vec{0}$ і $A\vec{b} = \vec{0}$. Додавши ці рівності, одержимо $A\vec{a} + A\vec{b} = A(\vec{a} + \vec{b}) = \vec{0}$, тобто $\vec{a} + \vec{b}$ є розв'язком системи (2.5.5). Якщо $\lambda \in P$, то домноживши рівність $A\vec{a} = \vec{0}$ на λ , маємо $\lambda(A\vec{a}) = A(\lambda\vec{a}) = \lambda \cdot \vec{0} = \vec{0}$, а це означає, що і $\lambda\vec{a}$ є розв'язком системи (2.5.5). Лему доведено. \square

Означення 2.5.4. *Фундаментальною системою розв'язків однорідної системи лінійних рівнянь називають базу підпростору її розв'язків.*

Теорема 2.5.7. *Нехай матриця системи (2.5.5) має ранг r . Тоді кожна фундаментальна система розв'язків цієї системи складається з $n - r$ розв'язків.*

Доведення. Перенумеровуючи, якщо потрібно, рівняння та невідомі, можемо вважати, що

$$\begin{vmatrix} a_{11} & \dots & a_{1r} \\ \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0.$$

Міркування попереднього п.2.5.5 показують, що система (2.5.5) еквівалентна такій системі лінійних рівнянь:

$$\begin{cases} a_{11}x_1 + \dots + a_{1r}x_r = -a_{1r+1}x_{r+1} - \dots - a_{1n}x_n, \\ \dots \\ a_{r1}x_1 + \dots + a_{rr}x_r = -a_{rr+1}x_{r+1} - \dots - a_{rn}x_n, \end{cases} \quad (2.5.6)$$

де x_1, \dots, x_r — рангові, а x_{r+1}, \dots, x_n — вільні невідомі. Нехай E — одинична матриця порядку $n - r$. Будемо підставляти в систему (2.5.6) по черзі кожний рядок матриці E як значення вільних невідомих (x_{r+1}, \dots, x_n) . Одержано $n - r$ систем Крамера, кожна з яких має єдиний розв'язок. Позначимо ці розв'язки (c_{i1}, \dots, c_{ir}) , $1 \leq i \leq n - r$, і розглянемо таку систему векторів простору P^n :

$$\begin{cases} \vec{c}_1 = (c_{11}, \dots, c_{1r}, 1, 0, \dots, 0), \\ \vec{c}_2 = (c_{21}, \dots, c_{2r}, 0, 1, \dots, 0), \\ \dots \\ \vec{c}_{n-r} = (c_{(n-r)1}, \dots, c_{(n-r)r}, 0, 0, \dots, 1). \end{cases} \quad (2.5.7)$$

Вектори (2.5.7) є розв'язками системи рівнянь (2.5.6) за побудовою. Ці вектори лінійно незалежні, бо матриця, рядками якої є ці вектори, має, очевидно, ранг $n - r$.

Залишається показати, що кожний розв'язок системи (2.5.6) є лінійною комбінацією векторів $\vec{c}_1, \dots, \vec{c}_{n-r}$. Нехай $\vec{b} =$

$(b_1, \dots, b_r, b_{r+1}, \dots, b_n)$ — розв'язок. Розглянемо вектор

$$\vec{d} = \vec{b} - b_{r+1}\vec{c}_1 - \dots - b_n\vec{c}_{n-r}.$$

Вектор \vec{d} — розв'язок системи (2.5.6), тому що він є лінійною комбінацією розв'язків, а множина розв'язків є підпростором. Останні $n-r$ компонент вектора \vec{d} , очевидно, дорівнюють нулю, а його перші r компонент задовільняють систему

$$\begin{cases} a_{11}x_1 + \dots + a_{1r}x_r = 0, \\ \dots \\ a_{r1}x_1 + \dots + a_{rr}x_r = 0, \end{cases} \quad (2.5.8)$$

яка одержується з (2.5.6) при $x_{r+1} = \dots = x_n = 0$. Система (2.5.8) є однорідною системою Крамера, тому вона має лише нульовий розв'язок. Отже, $\vec{d} = 0$ і $\vec{b} = b_{r+1}\vec{c}_1 + \dots + b_n\vec{c}_{n-r}$, що і треба було довести. \square

2.6. Вправи

- 1) Довести, що ненульові рядки східчастої матриці є лінійно незалежними.
- 2) Нехай розмірність підпростору $L \subset P^n$ дорівнює r . Довести, що будь-які r лінійно незалежних векторів з L складають базу L .
- 3) Нехай $m \geq 1$ і $n \geq 1$. Матриці $A, B \in M_{m,n}(P)$ назовемо еквівалентними, якщо $A = B$ або B може бути одержана з A за допомогою елементарних перетворень. Довести, що це відношення еквівалентності.
- 4) *Визначник Вандермонда.* Нехай $\alpha_1, \alpha_2, \dots, \alpha_n$ — елементи поля P . Довести, що

$$\begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i>j} (\alpha_i - \alpha_j).$$

(Вказівка. Використайте індукцію. Для кроку індукції відніміть від кожного стовпчика попередній, домножений на α_1 .)

- 5) *Формула Біне-Коши.* Нехай $A = [a_{ij}]$, $B = [b_{ij}]$ — матриці розмірів $n \times m$ та $m \times n$ відповідно, і нехай $C = AB$. Тоді $\det C =$

$$= \sum_{1 \leq j_1 < \dots < j_n \leq m} \begin{vmatrix} a_{1j_1} & a_{2j_1} & \dots & a_{nj_1} \\ a_{1j_2} & a_{2j_2} & \dots & a_{nj_2} \\ \dots & \dots & \dots & \dots \\ a_{1j_n} & a_{2j_n} & \dots & a_{nj_n} \end{vmatrix} \cdot \begin{vmatrix} b_{j_11} & b_{j_12} & \dots & b_{j_1n} \\ b_{j_21} & b_{j_22} & \dots & b_{j_2n} \\ \dots & \dots & \dots & \dots \\ b_{j_n1} & b_{j_n2} & \dots & b_{j_nn} \end{vmatrix}.$$

Сума справа береться по всіх підмножинах з n елементів $\{j_1, j_2, \dots, j_n\}$ з $\{1, 2, \dots, m\}$. Зокрема, $\det C = \det A \cdot \det B$ при $m = n$ і $\det C = 0$ при $n > m$.

(Вказівка. Оскільки $C = [c_{ij}]$, $c_{ij} = \sum a_{ik}b_{kj}$, то багаторазове застосування розкладу визначника за рядком дає $\det C =$

$$\begin{aligned} & \sum_{k_1, \dots, k_n=1}^n \begin{vmatrix} a_{1k_1} & a_{2k_1} & \dots & a_{nk_1} \\ a_{1k_2} & a_{2k_2} & \dots & a_{nk_2} \\ \dots & \dots & \dots & \dots \\ a_{1k_n} & a_{2k_n} & \dots & a_{nk_n} \end{vmatrix} b_{k_11} b_{k_22} \dots b_{k_nn} = \\ & = \sum_{1 \leq j_1 < \dots < j_n \leq m} \begin{vmatrix} a_{1j_1} & a_{2j_1} & \dots & a_{nj_1} \\ a_{1j_2} & a_{2j_2} & \dots & a_{nj_2} \\ \dots & \dots & \dots & \dots \\ a_{1j_n} & a_{2j_n} & \dots & a_{nj_n} \end{vmatrix} \\ & \quad \sum_{\pi} (-1)^{\operatorname{sgn} \pi} b_{j_11} \dots b_{j_nn}, \end{aligned}$$

(сума береться по всіх попарно різних k_1, \dots, k_n).

Остання рівність одержується групуванням доданків, відповідних фікований підмножині $\{j_1, \dots, j_n\}$).

- 6) Нехай $A = [a_{ij}]$ — матриця порядку n , $a_{ij} \in \{0, 1, \dots, 9\}$. Кожний рядок матриці A є записом n -цифрового натурального числа. Припустимо, всі ці числа діляться на просте число p . Довести, що і $\det A$ ділиться на p .

7) Довести, що кожне елементарне перетворення матриці A , тобто перетворення одного з таких типів:

- а) перестановка двох рядків (стовпчиків);
- б) додавання до одного рядка (стовпчика) іншого рядка (стовпчика), домноженого на довільний скаляр;
- в) домноження рядка (стовпчика) на ненульовий скаляр,

може бути одержане домноженням матриці A зліва (справа) на невироджену матрицю P . Знайти вигляд матриць P .

(*Вказівка.* Матриці P одержуються з одиничної матриці E за допомогою таких самих елементарних перетворень.)

- 8) Використовуючи попередню вправу, довести, що кожну невироджену матрицю A елементарними перетвореннями лише рядків (або лише стовпців) можна звести до одиничної матриці A . Якщо виконані над A елементарні перетворення в тому ж порядку застосувати до одиничної матриці E , то в результаті одержиться матриця A^{-1} , обернена до A .
- 9) *Визначники матриць над комутативним кільцем з одиницею.* Нехай R — комутативне кільце з одиницею і $A = [a_{ij}] \in M_n(R)$. Замінити в означенні визначника з п.2.3.1 поле P на кільце R і перевірити, що всі результати п.2.3.1–2.3.6 та 2.4.1–2.4.4 залишаються правильними і в цьому більш загальному випадку. Довести, що $A \in M_n(R)$ має обернену в кільці $M_n(R)$ матрицю тоді і тільки тоді, коли елемент $\det A$ має обернений відносно множення в кільці R .

10) Довести, що:

- а) ранг матриці за рядками не змінюється при елементарних перетвореннях рядків;
- б) максимальний порядок відмінних від нуля мінорів теж не змінюється при елементарних перетвореннях;

- в) ранг за рядками східчастої матриці дорівнює кількості її ненульових рядків і дорівнює максимальному порядку відмінних від нуля мінорів цієї матриці. Вивести звідси теорему про ранг матриці.
- 11) Довести, що ранг добутку матриць не перевищує рангу кожної матриці-множника.
- 12) Послідовність $a_1 = 1, a_2 = 1, a_3 = a_1 + a_2, \dots, a_n = a_{n-1} + a_{n-2}, \dots$ називають *послідовністю Фіbonacci*. Довести, що

$$a_{n+1} = \begin{vmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & -1 & 1 \end{vmatrix},$$

де матриця має порядок n .

- 13) Загальним розв'язком системи лінійних рівнянь називають множину всіх її розв'язків. Довести, що загальний розв'язок є сумою якого-небудь часткового розв'язку цієї системи і загального розв'язку відповідної однорідної системи лінійних рівнянь (тобто системи, що має ті самі коефіцієнти при невідомих і нульові вільні члени).

Розділ 3

Поліноми та евклідові кільця

3.1. Кільця поліномів

3.1.1. Означення. Операції над поліномами

Нехай R — кільце з 1. Побудуємо нове кільце A , елементами якого є нескінчені впорядковані послідовності $f = (f_0, f_1, \dots)$, де $f_i \in R$, причому всі f_i крім, можливо, скінченного їх числа, дорівнюють нулю. Визначимо на A операції додавання і множення:

$$f + g = (f_0 + g_0, f_1 + g_1, \dots, f_n + g_n, \dots),$$

$$f \cdot g = (h_0, h_1, \dots, h_n, \dots), \text{ де } h_k = \sum_{i+j=k} f_i g_j, \quad k = 0, 1, \dots$$

Тут $f = (f_0, f_1, \dots, f_n, \dots)$, $g = (g_0, g_1, \dots, g_n, \dots)$.

Перевіримо, що A — кільце. Асоціативність та комутативність додавання додавання в A зводиться до асоціативності та комутативності додавання в R . Елемент $(0, \dots, 0, \dots) \in A$ є нейтральним елементом, а елемент

$$-f = (-f_0, \dots, -f_n, \dots) \in A$$

є оберненим до f для операції додавання. Операція множення асоціативна. Справді, нехай $f = (f_0, f_1, \dots, f_n, \dots)$, $g = (g_0, g_1, \dots, g_n, \dots)$, $h = (h_0, h_1, \dots, h_n, \dots)$; тоді на i -му місці у добутку $(fg)h$ маємо

елемент

$$\sum_{s+t=i} \left(\sum_{k+l=s} f_k g_l \right) h_t = \sum_{k+l+t=i} f_k g_l h_t,$$

а в добутку $f(gh)$ — елемент

$$\sum_{k+j=i} f_k \left(\sum_{l+t=j} g_l h_t \right) = \sum_{k+l+t=i} f_k g_l h_t,$$

тобто $(fg)h = f(gh)$. Операція множення комутативна, якщо кільце R комутативне. Це випливає з комутативності операцій додавання і множення в кільці R . Нехай f, g і h такі як раніше. Тоді на i -му місці у послідовності $(f+g)h$ буде елемент $\sum_{k+l=i} (f_k + g_k) h_l$, а у послідовності $fh+gh$ — елемент $\sum_{k+l=i} f_k h_l + \sum_{k+l=i} g_k h_l$. Але, оскільки

$$\sum_{k+l=i} (f_k + g_k) h_l = \sum_{k+l=i} f_k h_l + \sum_{k+l=i} g_k h_l,$$

то $(f+g)h = fh+gh$. Таким чином, ми переконалися, що в A виконується закон дистрибутивності. Отже, A — кільце (з одиницею $(1, 0, \dots, 0, \dots)$), якщо кільце R з одиницею 1). Це кільце називається *кільцем поліномів* над кільцем R , а його елементи називаються *поліномами*. Послідовності $(a, 0, \dots, 0, \dots)$ додаються і множаться так само як елементи кільця R . Це дозволяє ототожнити такі послідовності з відповідними елементами із R , тобто вважати, що $a = (a, 0, \dots, 0, \dots)$ для кожного елемента $a \in R$, інакше кажучи, ототожнити R з підкільцем кільця A . Позначимо $X = (0, 1, 0, \dots, 0, \dots)$ і назовемо X змінною над R . Легко переконатися, що $X^2 = (0, 0, 1, 0, \dots, 0, \dots)$, $X^3 = (0, 0, 0, 1, 0, \dots, 0, \dots)$ і т.д. Крім того, завдяки включення $R \subset A$, маємо

$$\underbrace{(0, \dots, 0, a, 0, \dots)}_n = aX^n = X^n a.$$

Звідси випливає, що коли f_n — останній ненульовий член послідовності $f = (f_0, \dots, f_n, \dots)$, то $f = f_0 + f_1 X + \dots + f_n X^n =$

$f(X)$, і ми одержуємо стандартний запис полінома f . Елементи f_0, f_1, \dots, f_n називають *коефіцієнтами* полінома f , а f_n — *старшим коефіцієнтом*.

Побудоване кільце називають ще кільцем поліномів від змінної X , а його елементи f позначають $f(X)$. Натуральне число n таке, що f_n — останній відмінний від нуля коефіцієнт полінома f , називають *степенем* полінома $f(X)$ і записують $\deg f(X) = n$. Нульовому поліному приписують степінь $-\infty$. Кільце поліномів від змінної X над кільцем R позначають $R[X]$. Легко переконатися, що

$$\begin{aligned}\deg(f + g) &\leq \max(\deg f, \deg g), \\ \deg(fg) &\leq \deg f + \deg g.\end{aligned}$$

Нагадаємо, що кільце R називають кільцем без дільників нуля, якщо для довільних двох елементів a і b кільця R $ab = 0$ лише тоді, коли $a = 0$ або $b = 0$. У випадку кільця R без дільників нуля остання формула стає більш точною.

Твердження 3.1.1. а) Якщо R — комутативне кільце без дільників нуля, то $\deg(f \cdot g) = \deg f + \deg g$ для довільних $f, g \in R[X]$.

б) $R[X]$ — кільце без дільників нуля.

Доведення. Нехай $\deg f(X) = n$, $\deg g(X) = m$, а старшими коефіцієнтами поліномів $f(X)$ і $g(X)$ є, відповідно, f_n і g_m . Тоді, очевидно, старшим коефіцієнтом полінома $f(X)g(X)$ є f_ng_m і $\deg(f(X)g(X)) = n+m$. Як очевидний наслідок звідси випливає, що $R[X]$ — кільце без дільників нуля. \square

3.1.2. Поліноми як функції

Нехай $f(X) = f_0 + f_1X + \dots + f_nX^n \in R[X]$. Надамо змінній X певного значення з кільця R , наприклад $X = a$, а тоді розглянемо елемент $f_0 + f_1a + \dots + f_na^n$ з кільця R , який позначимо $f(a)$ і назовемо значенням полінома $f(X)$ при $X = a$. Отже, кожному

елементу a з кільця R відповідає єдиний елемент $f(a) \in R$; тому поліном $f(X)$ визначає функцію $f : R \rightarrow R$, для якої $f(a)$ є образом елемента $a \in R$.

Зауваження 3.1.1. У загальному випадку поліноми не слід ототожнювати з функціями. Наприклад, різні поліноми X^2 і X з кільця $\mathbb{Z}/2\mathbb{Z}[X]$ визначають одну функцію із $\mathbb{Z}/2\mathbb{Z}$ в $\mathbb{Z}/2\mathbb{Z}$.

З'єднувальною ланкою між функціональною і алгебраїчною точками зору на поліноми є така теорема.

Теорема 3.1.2. *Нехай R — підкільце комутативного кільця K . Для кожного елемента $t \in K$ існує єдиний гомоморфізм $\pi_t : R[X] \rightarrow K$ такий, що $\pi_t(a) = a$ для довільного $a \in R$ і $\pi_t(X) = t$.*

Доведення. Припустимо, що такий гомоморфізм π_t існує. Оскільки $\pi_t(f_i) = f_i$ для кожного коефіцієнта f_i полінома $f(X)$ і $\pi_t(X^k) = (\pi_t(X))^k = t^k$, то $\pi_t(f) = f_0 + f_1t + \dots + f_nt^n$, тобто $\pi_t(f)$ визначений однозначно. Навпаки, задавши відображення π_t формулою $\pi_t(f) = f(t)$, одержимо гомоморфізм, що задовільняє умовам теореми. \square

Елемент $\pi_t(f) = f(t)$ називається підстановкою t у $f(X)$ замість X . Якщо x — змінний елемент кільця R і $f(X) = a_0 + a_1X + \dots + a_nX^n \in R[X]$ — поліном, то $\pi_x(f) = a_0 + a_1x + \dots + a_nx^n$ є функцією з областю визначення R . На множині $R[x]$ всіх таких функцій введемо операції додавання та множення:

$$\begin{aligned}\pi_x(f) + \pi_x(g) &= \pi_x(f + g), \\ \pi_x(f) \cdot \pi_x(g) &= \pi_x(fg).\end{aligned}$$

Відносно цих операцій $R[x]$ є кільцем, і відображення $\pi_x : R[X] \rightarrow R[x]$ є сюр'єктивним гомоморфізмом кілець. З наступного твердження випливає, що якщо R — нескінченне поле, то π_x — ізоморфізм кілець $R[X]$ та $R[x]$.

Твердження 3.1.3. Нехай P — нескінченне поле, і нехай $f(X), g(X) \in P[X]$ — два різні поліноми. Тоді функції $\pi_x(f)$ і $\pi_x(g)$ теж різні.

Доведення. Нехай $\pi_x(f) = \pi_x(g)$ і нехай $h(X) = f(X) - g(X) = c_0 + c_1X + \dots + c_dX^d$. Тоді $\pi_x(h) =$ нульова функція. Виберемо $d+1$ різних елементів $\alpha_1, \dots, \alpha_{d+1}$ з поля P . Тоді $\pi_{\alpha_1}(h) = \dots = \pi_{\alpha_{d+1}}(h) = 0$, тобто маємо систему

$$\begin{cases} c_0 + c_1\alpha_1 + \dots + c_d\alpha_1^d = 0, \\ c_0 + c_1\alpha_2 + \dots + c_d\alpha_2^d = 0, \\ \dots \dots \dots \\ c_0 + c_1\alpha_{d+1} + \dots + c_d\alpha_{d+1}^d = 0. \end{cases} \quad (3.1.1)$$

Визначник цієї системи

$$\begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^d \\ 1 & \alpha_2 & \dots & \alpha_2^d \\ \dots \dots \dots \\ 1 & \alpha_{d+1} & \dots & \alpha_{d+1}^d \end{vmatrix}$$

є визначником Вандермонда, тому він не дорівнює нулю (див. вправу 4 в кінці Розділу 2). Тому система (3.1.1) має лише нульовий розв'язок $c_0 = c_1 = \dots = c_d = 0$, отже, $h(X) = f(X) - g(X) = 0$ і $f(X) = g(X)$. \square

З доведеного твердження випливає, що кільце поліномів над нескінченим полем P ізоморфне кільцю поліноміальних функцій $P[x]$, елементи якого теж називатимемо поліномами. Якщо P — скінченне поле, то різним поліномам з $P[X]$ можуть відповідати однакові функції (див. зауваження 3.1.1); у цьому випадку можна лише стверджувати, що кільце $P[x]$ є гомоморфним образом кільця $P[X]$. Враховуючи ці факти, ми будемо використовувати позначення $f(X)$ або $f(x)$ для поліномів та $R[X]$ або $R[x]$ для кілець поліномів. У більшості випадків це не приводить

до непорозумінь. За індукцією означають *кільце поліномів від n змінних*:

$$R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n].$$

Так само, як і у випадку $n = 1$, поліноми від n змінних можна розглядати як функції від n змінних і позначати або $f(X_1, \dots, X_n)$ або $f(x_1, \dots, x_n)$.

3.1.3. Ділення з остачею

Зазначимо, що поліном $c_0 + c_1 X + \dots + c_n X^n$ деколи записують і за спадними степенями X у вигляді $c_n X^n + \dots + c_1 X + c_0$ або $a_0 X^n + \dots + a_{n-1} X + a_n$, де $a_i = c_{n-i}$, $0 \leq i \leq n$. Зокрема, саме такий запис поліномів використовується у цьому пункті.

Нехай $P[X]$ — кільце поліномів з коефіцієнтами з поля P . При вивченні питань, пов'язаних з діленням поліномів, важливе значення має теорема про ділення з остачею.

Теорема 3.1.4 (про ділення з остачею). *Для будь-яких двох поліномів $f(X) = a_0 X^n + \dots + a_{n-1} X + a_n$ та $g(X) = b_0 X^m + \dots + a_{m-1} X + a_m$, де $f(X), g(X) \in P[X]$, $g(X) \neq 0$, існує єдина пара поліномів $q(X), r(X) \in P[X]$ таких, що*

$$f(X) = g(X)q(X) + r(X),$$

причому $\deg r(X) < \deg g(X)$, або $r(X) = 0$.

Доведення. Якщо $n < m$, то візьмемо $q(X) = 0$, $r(X) = f(X)$. Тоді $f(X) = g(X) \cdot 0 + r(X)$, де $\deg r(X) < \deg g(X)$.

Нехай $n \geq m$. Доведення проведемо індукцією за степенем полінома $f(X)$. Якщо $n = 0$, то $f(X) = a_0$, $g(X) = b_0$ і $f(X) = g(X) \cdot a_0/b_0$, де $b_0 \neq 0$, бо $g(X) \neq 0$. Отже, нехай $\deg f(X) > 0$. Розглянемо $f(X) - \frac{a_0}{b_0} X^{n-m} g(X) = f_1(X)$, тоді або $f_1(X) = 0$, або $\deg f_1(X) < n$. Якщо $\deg f_1(X) < n$, то за припущенням індукції існують поліноми $q_1(X), r(X) \in P[X]$ такі, що

$\in P[X]$ такі, що $f_1(X) = g(X)q_1(X) + r(X)$, де $r(X) = 0$ або $\deg r(X) < \deg g(X)$. Звідси

$$f(X) = g(X) \left(\frac{a_0}{b_0} X^{n-m} + q_1(X) \right) + r(X),$$

де $r(X) = 0$ або $\deg r(X) < \deg g(X)$, що й потрібно довести.

Доведемо єдиність поліномів $q(X)$ і $r(X)$. Припустимо, що в $P[X]$ існує ще одна пара поліномів $q_1(X)$ і $r_1(X)$, які задовольняють рівність

$$f(X) = g(X)q_1(X) + r_1(X),$$

причому $r_1(X) \neq 0$ або нуль-поліномом, або поліномом меншого степеня, ніж степінь $g(X)$. Тоді

$$g(X)q(X) + r(X) = g(X)q_1(X) + r_1(X).$$

Звідси маємо $g(X)(q(X) - q_1(X)) = r_1(X) - r(X)$. Припустимо, що $r_1(X) - r(X) \neq 0$. Тоді $q(X) - q_1(X) \neq 0$. В такому випадку $\deg(r_1(X) - r(X)) \geq \deg g(X)$, що неможливо. Отже, $r_1(X) = r(X)$, і оскільки $P[X]$ — кільце без дільників нуля, то $q_1(X) - q(X) = 0$, тобто $q_1(X) = q(X)$, що й потрібно було довести. \square

Зауважимо, що поліном $q(X)$ називається *часткою* від ділення $f(X)$ на $g(X)$, а $r(X)$ — *остачею* від цього ділення. Якщо при діленні полінома $f(X)$ на поліном $g(X)$ остача $r(X)$ дорівнює нулю, то кажуть, що поліном $f(X)$ ділиться на поліном $g(X)$, а поліном $g(X)$ називають *дільником* полінома $f(X)$.

Твердження 3.1.5. Якщо $f(X)$ ділиться на $g(X)$, то $f(X)$ ділиться також на $cg(X)$, де c — довільний ненульовий елемент поля P .

Доведення. Справді, якщо $f(X) = g(X)q(X)$, то $f(X) = cg(X)(c^{-1}q(X))$. \square

3.1.4. Узагальнення на випадок поліномів над областями цілісності

Нагадаємо, що областю цілісності називають комутативне кільце з 1 і без дільників нуля. Якщо R — область цілісності, то кільце поліномів $R[X]$ над R теж є областю цілісності. Це випливає з твердження 3.1.1. Теорема 3.1.4 узагальнюється на випадок кільця поліномів над областю цілісності. А саме, маємо таку теорему.

Теорема 3.1.6. *Нехай R — область цілісності,*

$$\begin{aligned} f(X) &= a_n X^n + \cdots + a_1 X + a_0 \quad i \\ g(X) &= b_m X^m + \cdots + b_1 X + b_0 \end{aligned}$$

— два поліноми з коефіцієнтами з кільця R . Якщо b_m має обернений відносно множення в R , то існує едина пара поліномів $d(X), r(X) \in P[X]$ таких, що

$$f(X) = g(X)d(X) + r(X),$$

де $\deg r(X) < \deg g(X)$ або $r(X) = 0$.

Доведення. Всі міркування з доведення теореми 3.1.4 цілком придатні і в цьому випадку. \square

3.1.5. Теорема Безу та схема Горнера

Нехай A — комутативне кільце з одиницею, яке міститься в області цілісності K .

Означення 3.1.1. Елемент $c \in K$ називається *коренем* (або нулем) полінома $f \in A[X]$, якщо $f(c) = 0$. Кажуть також, що c — корінь рівняння $f(X) = 0$.

Теорема 3.1.7 (Безу). *Елемент $c \in A$ є коренем полінома $f \in A[X]$ тоді і тільки тоді, коли $X - c$ ділить f в кільці $A[X]$.*

Доведення. За алгоритмом ділення з остачею $f(X) = (X - c)g(X) + r(X)$, де $\deg r(X) < \deg(X - c) = 1$ або $r(X) = 0$. Отже, $r(X) = r_0 \in A$. Підстановка c замість X (тобто застосування відображення π_c) дає $f(c) = r_0$, так що завжди $f(X) = (X - c)g(X) + f(c)$. Зокрема, $f(c) = 0$ тоді і тільки тоді, коли $f(X) = (X - c)g(X)$. \square

Ділення полінома $f(X)$ з коефіцієнтами в області цілісності A на лінійний поліном $X - c$ зручно здійснювати за схемою Горнера, яка простіша від алгоритму ділення з остачею. А саме, нехай

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n, \quad a_i \in A.$$

Скористаємося рівністю

$$f(X) = (X - c)q(X) + f(c), \quad (3.1.2)$$

де $q(X) = b_0X^{n-1} + b_1X^{n-2} + \cdots + b_{n-1}$, $b_j \in A$. Порівнюючи в (3.1.2) коефіцієнти при одинакових степенях X (починаючи зі старших), одержимо: $a_0 = b_0, a_1 = b_1 - b_0c, \dots, a_{n-1} = b_{n-1} - b_{n-2}c, a_n = f(c) - b_{n-1}c$, тобто

$$\begin{aligned} b_0 &= a_0, \\ &\dots \\ b_k &= b_{k-1}c + a_k, \\ &\dots \\ b_{n-1} &= b_{n-2}c + a_{n-1}, \\ f(c) &= b_{n-1}c + a_n. \end{aligned} \quad (3.1.3)$$

Зauważимо, що заодно обчислюється значення полінома f для $X = c$.

Приклад 3.1.1. Розділити $f(X) = 2X^5 - X^4 - 3X^3 + X - 3$ на $X - 3$ над \mathbb{Z} . Обчислення зручно розташувати у вигляді таблиці:

	2	-1	-3	0	1	-3
3	2	5	12	36	109	324

у верхньому рядку якої розміщені коефіцієнти полінома $f(X)$, а в нижньому — коефіцієнти частки $q(X)$ та остача $f(c)$, які обчислюються за допомогою рекурентних формул (3.1.3). Ця таблиця показує, що

$$q(X) = 2X^4 + 5X^3 + 12X^2 + 36X + 109, \quad r = f(3) = 324.$$

3.2. Евклідові кільця

Кільце поліномів $P[X]$ з коефіцієнтами з поля P має багато властивостей, які дуже схожі на властивості кільця цілих чисел \mathbb{Z} , особливо в питаннях, що стосуються подільності. Тому зручно вивчати ці кільця одночасно, а разом з ними і інші важливі в алгебрі та теорії чисел кільця. З цією метою вивчають так звані евклідові кільця, найпростішими прикладами яких є кільце \mathbb{Z} і кільце $P[X]$. Але, перш ніж давати означення евклідового кільця, систематизуємо деякі загальні поняття, що стосуються подільності в комутативних кільцих.

3.2.1. Ділення в кільциях. Дільники одиниці та прості елементи

Нехай R — область цілісності, тобто комутативне кільце з 1 і без дільників нуля.

Означення 3.2.1. Нехай $a, b \in R$. Кажуть, що b ділить a (a ділиться на b) і пишуть $b|a$, якщо існує елемент $c \in R$ такий, що $a = bc$. Запис $b \nmid a$ означає, що b не ділить a .

Приклад 3.2.1. З теореми Безу випливає, що $(X - 2)|(X^2 - 5X + 6)$, а $(X - 1) \nmid (X^2 - X + 1)$ в кільці $\mathbb{Z}[X]$.

З означення 3.2.1 безпосередньо випливають такі найпростіші властивості подільності (доведіть їх самостійно):

- 1) якщо $b|a_1$ і $b|a_2$, то $b|a_1 \pm a_2$;
- 2) якщо $b|a$ і $c \in R$, то $b|ac$.

Означення 3.2.2. Якщо $a \in R$ і $a|1$, то a називають *дільником одиниці* (або *одиницею*) кільця R .

Приклад 3.2.2. 1. В кільці \mathbb{Z} є два дільники 1, а саме ± 1 . В кільці $P[X]$ поліномів з коефіцієнтами з поля P дільниками одиниці є всі ненульові поліноми нульового степеня, тобто всі ненульові константи.

2. Розглянемо кільце $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi \mid a, b \in \mathbb{Z}\}$ цілих гаусових чисел із звичайними операціями додавання і множення. Якщо $a + bi \in \mathbb{Z}[i]$ — дільник одиниці, то існує таке $c + di \in \mathbb{Z}[i]$, що $(a + bi)(c + di) = 1$. Перейдемо до спряжених чисел в останній рівності: $(a - bi)(c - di) = 1$. Перемноживши ці дві рівності, одержимо

$$(a^2 + b^2)(c^2 + d^2) = 1.$$

Звідси випливає $a^2 + b^2 = 1$, тобто $a = \pm 1$, $b = 0$ або $a = 0$, $b = \pm 1$. Тому в кільці цілих гаусових чисел є чотири дільники одиниці: $\pm 1, \pm i$.

3. В кільці $\mathbb{Z}[\sqrt{2}] \stackrel{\text{def}}{=} \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ із звичайними операціями додавання і множення елемент $\sqrt{2} + 1$ є дільником 1, бо $(\sqrt{2} + 1)(\sqrt{2} - 1) = 1$. Якщо n — натуральне число, то маємо також $(\sqrt{2} + 1)^n(\sqrt{2} - 1)^n = 1$. Тому в кільці $\mathbb{Z}[\sqrt{2}]$ існує нескінчена кількість дільників одиниці.

Означення 3.2.3. Ненульові елементи $a, b \in R$ називають *асоційованими*, якщо $a|b$ і $b|a$.

Твердження 3.2.1. Елементи a і b асоційовані тоді і тільки тоді, коли $a = bu$, де $u|1$.

Доведення. Якщо $a = bu$ і $b = av$, то $a = avu$, тобто $a(1-vu) = 0$. Звідси, $1-vu = 0$, тобто $uv = 1$. Навпаки, якщо $a = bu$ і $uv = 1$, то $av = buv = b$, отже, $a|b$ і $b|a$. \square

Означення 3.2.4. Елемент $p \in K$ називають *простим*, якщо $p \neq 1$ і з того, що $a|p$ випливає, що $a|1$ або a асоційований з p .

Інакше кажучи, простий елемент — це елемент p , що не є дільником 1, і єдиними дільниками якого є дільники 1 та асоційовані з p елементи.

Приклад 3.2.3. 1. В кільці \mathbb{Z} числа $\pm 2, \pm 3, \pm 5, \pm 7, \dots$ є простими елементами. Додатні прості елементи в кільці \mathbb{Z} , тобто числа $2, 3, 5, 7, \dots$ називають простими числами.

2. Прості елементи кільця $R[X]$ називають незвідними поліномами. Якщо R — поле, то всі поліноми першого степеня незвідні.

3. В кільці $\mathbb{Z}[i]$ елемент 3 є простим. Справді, якщо $(a + bi)(c + di) = 3$, $a + bi \not\mid 1$, $c + di \not\mid 1$, то звідси випливає, переходячи до спряження, що $(a - bi)(c - di) = 3$, і тому $(a^2 + b^2)(c^2 + d^2) = 9$. Оскільки $a + bi \not\mid 1$, $c + di \not\mid 1$, то $a^2 + b^2 = 3$. Але, очевидно, не існує цілих чисел a і b з властивістю $a^2 + b^2 = 3$.

З іншого боку, $5 = (2-i)(2+i)$ і $2 \pm i \not\mid 1$, тому 5 не є простим елементом кільця $\mathbb{Z}[i]$.

Означення 3.2.5. Нехай a, b — ненульові елементи кільця R .

Елемент $d \in R$ називають найбільшим спільним дільником (Н.С.Д.) a і b і пишуть $d = (a, b)$ або $d = \text{НСД}(a, b)$, якщо d — спільний дільник a і b (тобто $d|a$ і $d|b$) і d ділиться на кожний інший спільний дільник цих елементів (тобто якщо $d'|a$ і $d'|b$, то $d'|d$). Аналогічно, найбільшим спільним дільником ненульових елементів $a_1, \dots, a_k \in R$ називають такий спільний дільник цих елементів, який ділиться на кожний інший спільний дільник цих елементів.

Приклад 3.2.4. 1. $-5 = (75, 20)$; $5 = (75, 20)$ в кільці \mathbb{Z} .

2. Легко пересвідчитися, що $(3, 2+i) = 1$ в кільці $\mathbb{Z}[i]$. Справді, ми вже знаємо, що 3 є простим елементом в $\mathbb{Z}[i]$. Тому досить показати, що $3 \nmid 2+i$. Якби це було не так, то для деякого $a+bi \in \mathbb{Z}[i]$ ми мали б $3(a+bi) = 2+i$. Взявши спряжені $3(a-bi) = 2-i$ і перемноживши, одержуємо $9(a^2 + b^2) = 5$ з цілими a і b , а це неможливо.

Зауважимо, що найбільший спільний дільник елементів визначається цими елементами з точністю до асоційованості. Коли кажуть, що найбільший спільний дільник елементів a і b дорівнює d , то мають на увазі, що всі асоційовані з d елементи теж є найбільшими спільними дільниками цих елементів a і b .

Означення 3.2.6. Елементи a і b кільця R називаються *взаємно простими*, якщо $(a, b) = 1$, тобто 1 є їх найбільшим спільним дільником.

3.2.2. Означення та приклади евклідових кілець

Означення 3.2.7. Область цілісності R називають *евклідовим кільцем*, якщо існує відображення $\delta: R \setminus \{0\} \rightarrow \mathbb{N}$, що має такі дві властивості:

- 1) $\delta(ab) \geq \delta(a)$;
- 2) для будь-яких $a, b \in R$, $b \neq 0$ існують $d, r \in R$ такі, що $a = bd + r$, де $\delta(r) < \delta(b)$ або $r = 0$.

Приклад 3.2.5. 1. Кільце \mathbb{Z} — евклідове. Для того, щоб це перевірити, розглянемо відображення $\delta: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$, для якого $\delta(a) = |a|$ — модуль числа a . Очевидно, що $|ab| \geq |a|$. Для перевірки другої умови з означення, нехай d найбільше ціле число, для якого $d \leq \frac{a}{b}$ (тобто d — ціла частина раціонального числа $\frac{a}{b}$). Тоді $0 \leq \frac{a}{b} - d = \frac{r}{b} < 1$ для деякого цілого r . Звідси $a - bd = r$, тобто $a = bd + r$, причому $|r| < |b|$ або $r = 0$.

2. Нехай P — поле. Тоді кільце поліномів $P[X]$ евклідове. Справді, розглянемо відображення $\delta: P[X] \setminus \{0\} \rightarrow \mathbb{N}$, де $\delta(f(X)) = \deg f(X)$ — степінь полінома $f(X)$. Властивість 1) з означення очевидна, а властивість 2) — це теорема 3.1.4 попереднього параграфа. 3. Щоб зрозуміти, що існують і інші евклідові кільця, покажемо, що кільце цілих гаусових чисел $\mathbb{Z}[i]$ евклідове. Взагалі, нормою будь-якого комплексного числа α називають добуток α і спряженого числа $\bar{\alpha}$ і пишуть $N(\alpha) = \alpha\bar{\alpha}$. Якщо $\alpha = a + bi$, то $N(\alpha) = a^2 + b^2$. Розглянемо відображення

$$\delta: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N},$$

$$\delta(m+ni) = N(m+ni) = m^2 + n^2.$$

Маємо $\delta((m+ni)(r+si)) = (m^2+n^2)(r^2+s^2) \geq m^2+n^2 = \delta(m+ni)$, тобто δ задовільняє умову 1) з означення евклідового кільця.

Нехай $a = m+ni$, $b = l+ki$, де $m, n, k, l \in \mathbb{Z}$, $b \neq 0$. Розглянемо комплексне число $\alpha = a/b = u+vi$. u і v є раціональними числами. Виберемо $d = s+ti \in \mathbb{Z}[i]$ так, щоб $|s-u| \leq \frac{1}{2}$, $|t-v| \leq \frac{1}{2}$. Тоді $a/b = d + \alpha + \beta i$, де $|\alpha| \leq \frac{1}{2}$ і $|\beta| \leq \frac{1}{2}$. Звідси маємо

$$a = bd + b(\alpha + \beta i).$$

Ця рівність показує, що $r = b(\alpha + \beta i) \in \mathbb{Z}[i]$. Крім цього, $\delta(r) = N(b(\alpha + \beta i)) = N(b)N(\alpha + \beta i) = \delta(b)(\alpha^2 + \beta^2) \leq \delta(b)(\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}\delta(b) < \delta(b)$, якщо $r \neq 0$. Отже, $\mathbb{Z}[i]$ — евклідово кільце.

3.2.3. Алгоритм Евкліда знаходження Н.С.Д. в евклідових кільцях

Нехай K — евклідове кільце. Якщо a і b — ненульові елементи кільця K , то

$$a = bd + r \quad (3.2.1)$$

для деяких $d, r \in K$, $\delta(r) < \delta(b)$ або $r = 0$. Рівність (3.2.1) називають діленням a на b з остачею: d називають *неповною часткою*, а r — *остачею*. Позначимо в (3.2.1) $d = d_1$, $r = r_1$ і, якщо $r_1 \neq 0$, то розділимо b з остачею на r_1

$$b = r_1 d_2 + r_2, \quad (3.2.2)$$

де $\delta(r_2) < \delta(r_1)$ або $r_2 = 0$. Якщо $r_2 \neq 0$, то розділимо r_1 з остачею на r_2

$$r_1 = r_2 d_3 + r_3. \quad (3.2.3)$$

І так далі, якщо на i -ому кроці $r_i \neq 0$, то ділимо r_{i-1} з остачею на r_i

$$r_{i-1} = r_i d_{i+1} + r_{i+1}. \quad (3.2.4)$$

Остачі $r_1, r_2, r_3, \dots, r_i$ визначають спадну послідовність натуральних чисел $\delta(r_1) > \delta(r_2) > \dots > \delta(r_i)$, тому через скінченне число кроків (nehай на $m+1$ -ому кроці, отже, r_m — остання ненульова остача) ми повинні прийти до ділення без остачі

$$r_{m-1} = r_m d_{m+1}. \quad (3.2.5)$$

Зупинимося на цьому і випишемо всі одержані рівності (3.2.1)–(3.2.5):

$$\left\{ \begin{array}{l} a = bd_1 + r_1, \\ b = r_1 d_2 + r_2, \\ \dots \dots \dots \\ r_{i-1} = r_i d_{i+1} + r_{i+1}, \\ \dots \dots \dots \\ r_{m-2} = r_{m-1} d_m + r_m, \\ r_{m-1} = r_m d_{m+1}. \end{array} \right. \quad (3.2.6)$$

Процедуру побудови системи рівностей (3.2.6) називають *алгоритмом Евкліда* знаходження найбільшого спільного дільника в евклідових кільцях. Обґрунтуванням цього є така теорема.

Теорема 3.2.2. *Остання ненульова остача r_m в процесі послідовного ділення з остачею (3.2.6) є найбільшим спільним дільником елементів a і b .*

Доведення. Доведемо спочатку, що $r_m|a$ і $r_m|b$. З останньої рівності в (3.2.6) маємо $r_m|r_{m-1}$, тоді з передостанньої випливає $r_m|r_{m-2}$. І так далі, якщо ми вже знаємо, що $r_m|r_{i+1}$ і $r_m|r_i$, то $i+1$ -ша рівність в (3.2.6) показує, що $r_m|r_{i-1}$. Так рухаючись доверху від рівності до рівності в (3.2.6) одержуємо $r_m|r_2$ і $r_m|r_1$, отже, $r_m|b$, тому $r_m|a$.

Залишається довести, що r_m ділиться на кожний інший спільний дільник елементів a і b . Якщо $c|a$ і $c|b$, то перша рівність в (3.2.6) показує, що $c|r_1$, тоді друга показує, що $c|r_2$. І так далі, переходячи тепер в (3.2.6) від рівності до рівності зверху вниз, одержуємо, що $c|r_{m-2}$ і $c|r_{m-1}$, тому (за передостанньою рівністю в (3.2.6)) $c|r_m$. \square

Сформулюємо важливий наслідок цієї теореми.

Наслідок 3.2.3 (з алгоритму Евкліда). *Нехай $d = (a, b)$ – найбільший спільний дільник елементів a і b евклідового кільця R . Тоді існують елементи $u, v \in R$ такі, що $ua + vb = d$.*

Доведення. Передостання рівність в (3.2.6) дозволяє записати $d = r_{m-2} - r_{m-1}d_m$. Підставимо сюди $r_{m-1} = r_{m-3} - r_{m-2}d_{m-1}$. Одержано $d = u'r_{m-3} + v'r_{m-2}$ для деяких $u', v' \in R$, які можна виписати явно, але їх явний вигляд нас не цікавить. Тепер виражаємо r_{m-2} через r_{m-3} і r_{m-4} , і т.д., рухаючись по системі (3.2.6) знизу доверху, ми знайдемо такі елементи $u, v \in R$, що $ua + vb = d$. \square

Цей наслідок пізніше буде не один раз використовуватись в такій формі:

Наслідок 3.2.4. *Нехай a і b – взаємно-прості елементи евклідового кільця. Тоді існують $u, v \in R$ такі, що $ua + vb = 1$.*

Доведення випливає з попереднього наслідку та з означення взаємно простих елементів.

3.2.4. Поняття про факторіальне кільце

Означення 3.2.8. Область цілісності R називають *факторіальним кільцем*, якщо R має такі дві властивості:

- 1) кожний ненульовий елемент $a \in R$ є добутком $a = up_1p_2 \dots p_k$, де $u|1$, p_i – прості елементи, $1 \leq i \leq k$, $k \geq 0$ (якщо $k = 0$, то $a = u$);

- 2) якщо $up_1p_2 \dots p_k = u'q_1q_2 \dots q_l$, де $u|1$, $u'|1$, p_1, \dots, p_k , q_1, \dots, q_l — прості елементи, то $k = l$ і кожний елемент p_i асоційований з деяким елементом q_j , $1 \leq i, j \leq k$.

Не будемо зараз наводити приклади факторіальних кілець, оскільки в наступному пункті ми доведемо, що кожне евклідове кільце факторіальне (зокрема, кільця \mathbb{Z} , $\mathbb{Z}[i]$ та $P[X]$, де P — поле, є факторіальними кільцями). Замість цього, розглянемо два приклади не факторіальних кілець.

Приклад 3.2.6. 1. Розглянемо кільце $K = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ із звичайними операціями. Знайдемо дільники 1 в цьому кільці. Якщо, $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$, то $i(a - b\sqrt{-5})(c - d\sqrt{-5}) = 1$, тому $(a^2 + 5b^2)(c^2 + 5d^2) = 1$. Отже, $a^2 + 5b^2 = 1$, а це можливо лише тоді, коли $a = \pm 1$, $b = 0$. Розглянемо рівність

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Покажемо, що $3, 7, 1 \pm 2\sqrt{-5}$ — прості елементи (вони, очевидно, попарно не асоційовані, бо ± 1 — єдині дільники 1). Розглянемо, наприклад, число $1 - 2\sqrt{-5}$, а інші три розглядаються так само. Якщо

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1 - 2\sqrt{-5},$$

то $(a - b\sqrt{-5})(c - d\sqrt{-5}) = 1 + 2\sqrt{-5}$. Звідси $(a^2 + 5b^2)(c^2 + 5d^2) = 21$, тому $a^2 + 5b^2 = 3$ або $a^2 + 5b^2 = 7$, а це неможливо (ми вважаємо, звичайно, що $a + b\sqrt{-5} \neq 1$ і $c + d\sqrt{-5} \neq 1$).

2. Нехай $K = \{a_0 + a_1X + \dots + a_nX^n \mid a_i \in P, n \neq 1\}$ — множина поліномів з коефіцієнтами з поля P , в які не входить мономи a_1X . Легко пересвідчитися в тому, що K — область цілісності, X^2 та X^3 — прості елементи кільця K . Маємо $X^6 = X^3 \cdot X^3 = X^2 \cdot X^2 \cdot X^2$, тобто розклад на прості множники, як і в попередньому прикладі, неоднозначний.

Зауваження 3.2.1. В означення факторіального кільця входять дві умови. Якщо виконується перша з них, то кажуть, що розклад на прості множники в кільці R існує, а якщо виконується друга, то кажуть, що він однозначний.

3.2.5. Факторіальність евклідових кілець

Почнемо з двох лем.

Лема 3.2.1. *Нехай a і b — ненульові елементи евклідового кільця R і $b \neq 1$. Тоді $\delta(ab) > \delta(a)$.*

Доведення. Розділимо a з остачею на ab : $a = (ab)d + r$, де $\delta(r) < \delta(ab)$ або $r = 0$. Якщо $r = 0$, то $a = a(bd)$, тобто $a(1 - bd) = 0$, тому $1 - bd = 0$, отже $b|1$, що суперечить умовам леми. Таким чином, $a = abd = r \neq 0$. Маємо $\delta(ab) > \delta(r) = \delta(a(1 - bd)) \geq \delta(a)$, що і треба було довести. \square

Лема 3.2.2. *Нехай p — простий елемент, a і b — ненульові елементи евклідового кільця R . Припустимо, що $p|ab$ і $(p, a) = 1$. Тоді $p|b$.*

Доведення. За наслідком 3.2.4 з алгоритму Евкліда існують $u, v \in R$ такі, що $up + va = 1$. Домножуючи на b , отримуємо $upb + vab = b$. Очевидно, p ділить ліву частину цієї рівності, тому $p|b$. \square

Тепер доведемо наступний важливий результат.

Теорема 3.2.5. *Кожне евклідово кільце є факторіальним.*

Доведення. 1) *Існування розкладу на прості множники.* Образ $\text{Im}\delta$ відображення δ з означення евклідового кільця є підмножиною множини натуральних чисел \mathbb{N} . Нехай m_0 — найменший елемент підмножини $\text{Im}\delta$. Якщо $a \in R$, $\delta(a) = m_0$ і $a = bc$, то $b|1$, інакше згідно леми 3.2.1 ми мали б $m_0 = \delta(a) > \delta(c)$, а це неможливо за вибором a . Так само $c|1$. Отже, $a|1$ і за означенням розклад для a існує. Далі міркуємо

за індукцією. Припустимо, що $\delta(a) = m$ і що розклад на прості множники існує для всіх $a' \in R$ з $\delta(a') < m$. Якщо $a|1$ або a — простий елемент, то доводити нічого. Нехай $a \nmid 1$ і a не простий. Тоді існують $b, c \in R$ такі, що $a = bc$ і $b \nmid 1, c \nmid 1$. Звідси за лемою 3.2.1 випливає, що $\delta(b) < \delta(a)$ і $\delta(c) < \delta(a)$, отже, для b і c розклад в добуток простих елементів існує, а тому він існує і для елемента a .

2) *Єдиність.* Нехай маємо рівність

$$up_1 \dots p_k = u'q_1 \dots q_l, \quad (3.2.7)$$

де p_i, q_j — прості елементи, а u, u' — дільники одиниці. Припустимо, що $k > l$.

З (3.2.7) випливає, що $p_1|u'q_1 \dots q_l$. Якщо $p_1|q_1$, то p_1 і q_1 асоційовані, тобто існує $v, v|1$ і $q_1 = vp_1$. Підставимо vp_1 в (3.2.7) замість q_1 і скоротимо на p_1 ; це можливо, бо R не має дільників нуля. Одержано

$$up_2 \dots p_k = u''q_2 \dots q_l, \quad (3.2.8)$$

де $u'' = u'v$. Якщо ж $p_1 \nmid q_1$, то тоді $(p_1, q_1) = 1$, і тому з леми 3.2.2 випливає, що $p_1|u''q_2 \dots q_l$. Повторюючи вже проведені міркування, одержимо, що або p_1 асоційоване з q_2 і знову рівність 3.2.7 можна розділити на p_1 і (з точністю до нумерації простих елементів q_1, \dots, q_l) одержати 3.2.8 або $p_1|u''q_3 \dots q_l$. В кінці кінців ми мусимо знайти q_j , який асоційований з p_1 (в найгіршому випадку ним може виявитися останній простий елемент q_l), і, перенумерувавши (якщо потрібно) прості елементи, отримати рівність (3.2.8).

Застосувавши аналогічні міркування до p_2, \dots, p_l , одержимо $up_{l+1} \dots p_k = w$, де $w|1$. Переписавши цю рівність у вигляді $w^{-1}up_{l+1} \dots p_k = 1$, бачимо, що $p_{l+1}|1$, але це неможливо, бо p_{l+1} — простий елемент. Виявлена суперечність показує, що $k \geq l$. Так само доводимо, що і $k \leq l$. Отже, $k = l$. Крім цього, бачимо, що вже доведено і твердження про асоційованість кожного простого елемента p_i з деяким простим елементом q_j , $1 \leq i, j \leq k$, тому доведення теореми завершено. \square

3.2.6. Кільце цілих чисел \mathbb{Z}

Кільце \mathbb{Z} евклідове, тому воно факторіальне. Твердження “ \mathbb{Z} — факторіальне кільце” називають *основною теоремою арифметики* (тобто теорії чисел).

Кільце цілих чисел є одним з основних об'єктів вивчення великого і багатого на результати розділу математики — теорії чисел. Багато результатів теорії чисел просто формулюються і мають досить складні доведення (як наприклад, теорема Діріхле про прості числа в арифметичній прогресії, яка стверджує, що кожна арифметична прогресія цілих чисел зі взаємно простими першим членом та різницею містить нескінченну кількість простих чисел). Існує багато тверджень про цілі числа, які досить давно були сформульовані і для яких дотепер не знайдено, ні доведення ні спростування (одним з них є твердження про те, що існує нескінчenna кількість пар простих чисел-близнят, тобто пар простих чисел, різниця яких дорівнює 2, наприклад, 5 і 7, 29 і 31, 1997 і 1999). Одним з перших результатів про цілі (точніше, натуральні) числа була теорема Евкліда про те, що існує нескінчenna кількість простих чисел. Доведення цієї теореми дуже просте. Припустимо, що існує лише скінчenna кількість простих чисел p_1, p_2, \dots, p_n . Розглянемо натуральне число $m = p_1 p_2 \dots p_n + 1$. Оскільки $p_i < m$ для всіх i , $i \leq 1 \leq n$, то існує простий множник числа m , менший від m . Цим множником може бути лише одне з чисел p_1, p_2, \dots, p_n . З точністю до нумерації, можна вважати, що $p_1 | m$. Тоді $p_1 k = p_1 p_2 \dots p_n + 1$ для деякого k . Звідси $p_1(k - p_2 \dots p_n) = 1$, тобто $p_1 | 1$, що суперечить означенню простого числа.

3.3. Поліноми над факторіальними кільцями

3.3.1. Поле дробів

Щоб задати раціональне число $\frac{a}{b}$, потрібно вказати впорядковану пару цілих чисел — чисельник a і знаменник b , $b \neq 0$. Одне і те ж раціональне число може бути записане у вигляді різних дробів (тобто задане багатьма впорядкованими парами цілих чисел, наприклад, $-\frac{1}{2} = \frac{-5}{10} = \frac{3}{-6}$ і т.п.). Два дроби $\frac{a}{b}$ і $\frac{a'}{b'}$ рівні тоді і тільки тоді, коли $ab' = a'b$. Всі рівні дроби визначають те саме раціональне число. Крім того, цілі числа, очевидно, ототожнюються з раціональними числами, що задаються дробами вигляду $\frac{a}{1}$, де $a \in \mathbb{Z}$, при цьому ототожненні операції додавання і множення цілих чисел збігаються з операціями додавання і множення відповідних їм дробів. Коротко таку ситуацію характеризують так: кільце \mathbb{Z} є підкільцем поля \mathbb{Q} .

Ми хочемо для кожної області цілісності R побудувати поле P (поле дробів кільця R), яке так само зв'язане з R , як \mathbb{Q} з \mathbb{Z} (точніше кажучи, поле P є підполем кожного поля, що містить R).

Розглянемо для цього множину $M = \{(a, b) \mid a \in R, b \in R \setminus \{0\}\}$ впорядкованих пар елементів кільця R , причому в кожній парі друга компонента не дорівнює нулю, і означимо на множині M наступне відношення \sim :

$$(a, b) \sim (c, d) \Leftrightarrow ad - bc = 0.$$

Твердження 3.3.1. \sim є відношенням еквівалентності.

Доведення. Очевидно, що відношення \sim рефлексивне і симетричне. Покажемо, що воно транзитивне. Нехай $(a, b) \sim (c, d)$ і $(c, d) \sim (e, f)$. Тоді $ad - bc = 0$ і $cf - de = 0$. Звідси $adf - bcf = 0$ і $bcf - bde = 0$, тому $adf - bde = 0$. Оскільки $d \neq 0$ і R — область цілісності, то звідси випливає, що $af = be$, тобто $(a, b) \sim (e, f)$. \square

Ми переконалися, що \sim — відношення еквівалентності. Тому можна розглянути фактор-множину M/\sim , яку позначимо P . Елементами множини P є класи еквівалентних між собою пар (суміжні класи). Суміжний клас з представником (a, b) позначимо $\frac{a}{b}$. Означимо на множині P операції додавання та множення.

Означення 3.3.1.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \quad (3.3.1)$$

Твердження 3.3.2. *Операції (3.3.1) є коректно означеними, тобто не залежать від вибору представників суміжних класів.*

Доведення. Нехай $\frac{a}{b} = \frac{a'}{b'}$. Це означає, що $ab' - a'b = 0$. Нам потрібно вияснити чи

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c}{d} \stackrel{\text{def}}{=} \frac{a'd + b'c}{b'd}?$$

Для цього розглянемо різницю $(ad + bc)b'd - bd(a'd + b'c) = ab'd^2 + bb'cd - a'bd^2 - bb'cd = d^2(ab' - a'b) = 0$. Отже, відповідь на останнє запитання є ствердною, а це означає, що сума не залежить від вибору представника другого доданка.

Аналогічно перевіряємо, що вона не залежить від вибору представника другого доданка. Тому додавання означене коректно. Зробимо схоже обчислення і для множення, змінивши тепер представник першого співмножника. Маємо $\frac{a'}{b'} \cdot \frac{c}{d} = \frac{a'c}{b'd}$, і $acb'd - a'cbd = dc(ab' - ba') = 0$, отже, і множення означене коректно. \square

Твердження 3.3.3. *Множина P є полем відносно операцій додавання і множення, заданих формулами (3.3.1), і кільце R ізоморфне підкільцу поля P .*

Доведення. Проста перевірка переконує, що операції (3.3.1) комутативні, асоціативні, а множення дистрибутивне відносно додавання. Далі, легко перевірити, що $\frac{0}{1}$ — нейтральний елемент для додавання, $\frac{1}{1}$ — нейтральний елемент для множення, $\frac{-a}{b}$ — обернений до $\frac{a}{b}$ для додавання і, нарешті, для $\frac{a}{b} \neq \frac{0}{1}$

елемент $\frac{b}{a}$ обернений до $\frac{a}{b}$ відносно множення. Залишається показати, що R' ізоморфне підкільцю поля P . Нехай $R' = \{\frac{a}{1} \mid a \in R\}$. Тоді легко переконатися, що R' — підкільце поля P і що R можна ототожнити з R' за допомогою відображення $\phi: R \rightarrow R'$, $\phi(a) = \frac{a}{1}$. Доведення закінчено. \square

3.3.2. Лема Гауса про примітивні поліноми

Нехай R — факторіальне кільце і $f(X) \in R[X]$ — поліном з коефіцієнтами з кільця R

$$f(X) = a_0 + a_1X + \cdots + a_nX^n.$$

Означення 3.3.2. Змістом полінома $f(X)$ називають найбільший спільний дільник його коефіцієнтів. Якщо зміст полінома дорівнює 1, то поліном називається *примітивним*.

Лема 3.3.1. Добуток двох примітивних поліномів є примітивним поліномом.

Доведення. Нехай $f(X) = a_0 + a_1X + \cdots + a_mX^m$ і $g(X) = b_0 + b_1X + \cdots + b_nX^n$ — примітивні поліноми з коефіцієнтами з R і нехай

$$h(X) = c_0 + c_1X + \cdots + c_{m+n}X^{m+n}$$

— добуток поліномів $f(X)$ і $g(X)$. Для доведення леми досить переконатися, що не існує жодного простого елемента $p \in R$, який ділив би всі коефіцієнти полінома $h(X)$.

Нехай p — будь-який простий елемент кільця R . Оскільки $f(X)$ і $g(X)$ — примітивні поліноми, то p не ділить всіх коефіцієнтів як $f(X)$, так і $g(X)$. Нехай a_i — коефіцієнт з найбільшим індексом полінома $f(X)$ з властивістю $p \nmid a_i$, а b_j — коефіцієнт з найбільшим індексом полінома $g(X)$ з властивістю $p \nmid b_j$. (Отже, a_i та b_j вибрані так, що $p \nmid a_{i+1}$,

$p|a_{i+2}, \dots, p|b_{j+1}, p|b_{j+2}, \dots)$ Розглянемо коефіцієнт c_{i+j} полінома $h(X)$:

$$c_{i+j} = a_i b_j + a_{i+1} b_{j-1} + a_{i-1} b_{j+1} + \dots \quad (3.3.2)$$

З простоти p випливає, що $p \nmid a_i b_j$, а за вибором коефіцієнтів a_i та b_i простий елемент p ділить всі інші доданки у правій частині рівності (3.3.2). Звідси випливає, що $p \nmid c_{i+j}$, бо в іншому випадку ми одержали б $p|a_i b_j$, тобто суперечність. \square

Наслідок 3.3.4. *Зміст добутку двох поліномів дорівнює добутку їх змістів.*

Доведення. Якщо a і b — змісти поліномів $f(X)$ і $g(X)$, то $f(X) = af_1(X)$, $g(X) = bg_1(X)$, де $f_1(X)$ і $g_1(X)$ — примітивні поліноми. Отже, $f(X)g(X) = abf_1(X)g_1(X)$. За лемою 3.3.2 $f_1(X)g_1(X)$ — примітивний поліном, тому ab — зміст полінома $f(X)g(X)$. \square

3.3.3. Незвідні поліноми

Нехай R — факторіальне кільце, P — його поле дробів. Прості елементи кільця $R[X]$ називають *незвідними* поліномами над R . Наша мета — показати, що незвідний поліном над R залишається незвідним і над P . Для цього доведемо одну просту лему.

Лема 3.3.2. *Нехай $f(X) \in R[X]$ — примітивний поліном і нехай $a \in P$, причому $af(X) \in R[X]$. Тоді $a \in R$.*

Доведення. Нехай $f(X) = a_0 + a_1 X + \dots + a_n X^n$, де $a_i \in R$. Для $a = \frac{s}{t} \in P$ елементи s і t можна вважати взаємно простими. Якщо $a \notin R$, то існує простий елемент $p \in R$ такий, що $p|t$. Але, оскільки $\frac{a_i s}{t} \in R$, то $p|a_i s$, отже, $p|a_i$ для всіх i , $0 \leq i \leq n$, бо $(p, s) = 1$. Це означає, що зміст полінома $f(X)$ ділиться на p , тому цей поліном не може бути примітивним. Одержані суперечність показує, що $a \in R$. \square

Теорема 3.3.5. Якщо $f(X) \in R[X]$ незвідний над R , то він незвідний і над P .

Доведення. Міркуємо від супротивного. Нехай $f(X)$ розкладається над P :

$$f(X) = f_1(X)f_2(X),$$

де $f_1(X), f_2(X) \in P[X]$. Позначимо через b_1 і b_2 спільні знаменники коефіцієнтів поліномів $f_1(X)$ і $f_2(X)$. Тоді

$$f(X) = \frac{1}{b_1 b_2} f'_1(X) f'_2(X),$$

де $f'_1(X), f'_2(X) \in R[X]$. Далі, якщо a_1 і a_2 — змісти поліномів $f_1(X)$ і $f_2(X)$, то

$$f(X) = \frac{a_1 a_2}{b_1 b_2} f''_1(X) f''_2(X), \quad (3.3.3)$$

де $f''_1(X), f''_2(X)$ — примітивні поліноми над R . З попередньої леми випливає, що $\frac{a_1 a_2}{b_1 b_2} = c \in R$, а тому (3.3.3) є розкладом $f(X)$ над R . Суперечність. \square

Існують різні критерії незвідності поліномів над R . Одним з найвідоміших є *критерій Айзенштайнa*.

Теорема 3.3.6 (критерій Айзенштайнa). *Нехай $f(X) = a_0 + a_1 X + \dots + a_n X^n$ — поліном над R . Припустимо, що існує простий елемент $p \in R$, що має такі властивості:*

- 1) $p|a_0, p|a_1, \dots, p|a_{n-1}, p \nmid a_n;$
- 2) $p^2 \nmid a_0$.

Тоді поліном $f(X)$ незвідний над R .

Доведення. Припустимо, від супротивного, що це не так. Тоді існують поліноми степенів, наприклад, k і l , такі, що

$$a_0 + a_1 X + \dots + a_n X^n = (b_0 + b_1 X + \dots + b_k X^k)(c_0 + c_1 X + \dots + c_l X^l).$$

Прирівнюючи коефіцієнти при відповідних степенях X , одержуємо

$$\begin{aligned} a_0 &= b_0 c_0, \\ a_1 &= b_0 c_1 + b_1 c_0, \\ &\dots \\ a_i &= b_0 c_i + b_1 c_{i-1} + \dots + b_i c_0, \\ a_n &= b_k c_l, \end{aligned} \tag{3.3.4}$$

p не ділить одночасно b_0 і c_0 , бо в іншому випадку ми мали б $p^2 | a_0$, що суперечить умовам теореми. Припустимо, що $p \nmid c_0$, тоді $p | b_0$ і друга рівність в (3.3.4) показує, що $p | b_1$. Якщо ми вже довели, що $p | b_0, p | b_1, \dots, p | b_{i-1}$, то з $i+1$ -ої рівності в (3.3.4) випливає, що $p | b_i$. Тому, переходячи в (3.3.4) від рівності до рівності зверху вниз, ми одержимо через k кроків, що $p | b_k$, а тоді остання рівність в (3.3.4) дає $p | a_n$, що суперечить умовам теореми. \square

Приклад 3.3.1. 1. Нехай a_0, a_1, \dots, a_n — довільні цілі числа, p — просте число. Поліном

$$X^n + a_{n-1}pX^{n-1} + \dots + a_1pX + a_0p^2 + p$$

незвідний в кільцях $\mathbb{Z}[X]$ та $\mathbb{Q}[X]$. Зокрема, поліноми $X^5 - 3, X^{10} + 2000X^7 + 8X^4 - 6X - 2$ незвідні в $\mathbb{Q}[X]$.

2. Нехай p — просте число,

$$f(X) = X^{p-1} + X^{p-2} + \dots + X + 1$$

— поліном з цілими коефіцієнтами. Запишемо $f(X) = \frac{X^p - 1}{X - 1}$. Зробивши заміну $X - 1 = Y$, одержуємо

$$\begin{aligned} f(X) &= f(Y + 1) = \frac{(Y + 1)^p - 1}{Y} = \sum_{k=0}^{p-1} C_p^k Y^{p-k-1} = \\ &= Y^{p-1} + C_p^1 Y^{p-2} + \dots + C_p^{p-2} Y + C_p^{p-1}. \end{aligned}$$

Оскільки p — просте число, то p ділить всі біномальні коефіцієнти $C_p^1, \dots, C_p^{p-2}, C_p^{p-1} = p$. Але вільний член C_p^{p-1} не ділиться на p^2 , тому $f(Y + 1)$, а отже, і $f(X)$ незвідний над \mathbb{Q} .

Подивимося тепер, які елементи кільця $R[X]$ є дільниками одиниці і які є простими. Якщо $a|1$ в $R[X]$, то $a|1$ в $P[X]$, а в $P[X]$ дільниками одиниці є ненульові елементи поля P . Тому $a \in P \cap R[X] = R$ і a — дільник одиниці кільця R .

Прості елементи кільця R залишаються простими в $R[X]$. Якщо $f(X)$ — незвідний поліном, то $f(X)$ залишається незвідним і в $P[X]$. Його зміст повинен дорівнювати 1, інакше ми розкладали б $f(X)$ у добуток змісту і примітивного полінома. Простими елементами кільця $R[X]$ є прості елементи кільця R та незвідні над R поліноми змісту 1 і тільки вони.

3.3.4. Факторіальність кілець поліномів

Теорема 3.3.7. Якщо R — факторіальне кільце, то кільце поліномів $R[X]$ факторіальне.

Доведення. 1. *Існування розкладу.* Нехай $f(X) \in R[X]$. Розглядаючи $f(X)$ як поліном над полем дробів P кільця R і використовуючи факторіальність кільця $P[X]$ (теорема 3.2.5), ми можемо розкласти $f(X)$ в добуток незвідних поліномів

$$f(X) = f_1(X) \dots f_r(X). \quad (3.3.5)$$

Нехай b — добуток спільних знаменників поліномів $f_1(X), \dots, f_r(X)$. Тоді (3.3.5) можна записати так:

$$f(X) = \frac{1}{b} f'_1(X) \dots f'_r(X), \quad (3.3.6)$$

де $f'_i(X) \in R[X]$. Нехай a — добуток змістів поліномів $f'_1(X), \dots, f'_r(X)$, тоді (3.3.6) записується у вигляді

$$f(X) = \frac{a}{b} f''_1(X) \dots f''_r(X),$$

де $f''_i(X)$ — примітивні і незвідні над R поліноми. Елемент $c = \frac{a}{b}$ належить R за лемою 3.3.2. Розклавши c на прості множники в R , одержуємо, що

$$f(X) = p_1 \dots p_m f''_1(X) \dots f''_r(X)$$

– розклад на прості множники полінома $f(X)$ в кільці $R[X]$.

2. *Єдиність.* Якщо

$$f(X) = p_1 \dots p_m f_1(X) \dots f_r(X) = q_1 \dots q_l g_1(X) \dots g_s(X) \quad (3.3.7)$$

($p_1, \dots, p_m, q_1, \dots, q_l$ — прості елементи кільця R , $f_1, \dots, f_r, g_1, \dots, g_s$ — примітивні незвідні поліноми в $R[X]$), то, перш за все $p_1 \dots p_m = uq_1 \dots q_l$, де $u|1$, бо кожен з цих добутків є змістом полінома $f(X)$. З факторіальності кільця R випливає, що $m = l$ і кожний простий елемент p_i асоційований з деяким простим елементом q_j . Розділимо (3.3.7) на $q_1 \dots q_m$:

$$uf_1(X) \dots f_r(X) = g_1(X) \dots g_s(X).$$

Оскільки $P[X]$ факторіальне, то тут $r = s$ (зауважимо, що $f_i(X), g_j(X)$ — прості елементи факторіального кільця $P[X]$ (за теоремою 3.3.5)), тому з точністю до нумерації $f_i(X) = a_i g_i(X)$, де $a_i \in P$. Але $a_i \in R$ за лемою 3.3.2 і a_i є дільником 1 в R , оскільки рівність $f_i(X) = a_i g_i(X)$ показує, що a_i — зміст примітивного полінома. Теорему доведено. \square

Наслідок 3.3.8. *Нехай P — поле або будь-яке факторіальне кільце. Тоді кільце поліномів $P[X_1, \dots, X_n]$ є факторіальним. Зокрема, кільце $\mathbb{Z}[X]$ та $\mathbb{Z}[X_1, \dots, X_n]$ факторіальні.*

Доведення. Для кільця $\mathbb{Z}[X]$ наслідок безпосередньо випливає з теореми. Для кілець $\mathbb{Z}[X_1, \dots, X_n]$ та $P[X_1, \dots, X_n]$ наслідок так само випливає з теореми за допомогою індукції. \square

3.4. Корені поліномів

3.4.1. Похідна полінома та кратні корені

Означення 3.4.1. Нехай R — комутативне кільце. Відображення $\frac{d}{dX} : R[X] \rightarrow R[X]$, для якого

$$\frac{d}{dX}(a_0 + a_1 X + \dots + a_n X^n) = a_1 + 2a_2 X + \dots + n a_n X^{n-1},$$

називають *диференціюванням*.

Якщо $f = f(X) \in R[X]$, то $\frac{d}{dX}(f(X))$ записують $\frac{df}{dX}$ або, коротше, $f'(X)$ чи f' і називають *похідною* полінома f . Якщо до полінома $f(X)$ застосувати відображення $\frac{d}{dX} k$ разів, то одержимо k -у похідну полінома $f(X)$, яку позначають $f^{(k)}(X)$.

Твердження 3.4.1. *Похідна має такі властивості:*

- (1) $(f + g)' = f' + g'$;
- (2) $(af)' = af'$, де $a \in R$, $f \in R[X]$, $\deg f \geq 1$;
- (3) $(fg)' = f'g + fg'$;
- (4) $(f^m)' = mf^{m-1}f'$.

Доведення. Властивості (1) і (2) безпосередньо випливають з означення похідної та додавання поліномів. Оскільки добуток поліномів є сумою добутків мономів $a_i X^i$ і $b_j X^j$, то, беручи до уваги властивість (1), досить довести (3) у випадку $f(X) = a_i X^i$, $g(X) = b_j X^j$. Маємо

$$\begin{aligned} (a_i X^i \cdot b_j X^j)' &= (a_i b_j X^{i+j})' = (i+j)a_i b_j X^{i+j-1}, \\ (a_i X^i)' b_j X^j + a_i X^i (b_j X^j)' &= ia_i b_j X^{i+j-1} + ja_i b_j X^{i+j-1} = \\ &= (i+j)a_i b_j X^{i+j-1}, \end{aligned}$$

тому властивість (3) теж справедлива. Властивість (4) доводимо індукцією. Випадок $m = 1$ очевидний. Припустимо, що рівність (4) доведена для показника m . Використовуючи (3) для $g = f^m$, маємо $(f^{m+1})' = (f \cdot f^m)' = f' f^m + f m f^{m-1} f' = (m+1) f^m f'$. \square

Далі вважатимемо, що кільце R є підкільцем області цілісності A .

Означення 3.4.2. Елемент c кільця A називають *k -кратним коренем* полінома $f(X) \in R[X]$, якщо $f(X)$ ділиться на кільці $A[X]$ на $(X - c)^k$ і не ділиться на $(X - c)^{k+1}$. Корені

кратності > 1 називають *кратними*, 1-кратні корені називають *простими*. Якщо $k = 2$ або $k = 3$, то c називають подвійним або потрійним коренем.

З теореми Безу випливає, що $c \in A$ є k -кратним коренем полінома $f(X)$ тоді і тільки тоді, коли $f(X) = (X - c)^k g(X)$, де $g(X) \in A[X]$, $g(c) \neq 0$. Очевидно, що $\deg f = k + \deg g$, отже, $k \leq \deg f$.

Твердження 3.4.2. *Нехай A — область цілісності, R — підкільце в A і $f(X) \in R[X]$ — ненульовий поліном над R . Припустимо, що $c_1, \dots, c_r \in A$ — всі корені полінома $f(X)$, і що ці корені мають кратності, відповідно, k_1, \dots, k_r . Тоді*

$$f(X) = (X - c_1)^{k_1} \dots (X - c_r)^{k_r} g(X),$$

де $g(X) \in A[X]$, $g(c_i) \neq 0$ для $i = 1, \dots, r$. Зокрема, кількість коренів полінома $f(X)$ з врахуванням їх кратностей не перевищує степеня полінома: $k_1 + \dots + k_r \leq \deg f$.

Доведення. Нехай P — поле дробів кільця A . Оскільки $P[X]$ — факторіальне кільце, то з рівностей

$$f(X) = (X - c)_i^k f_i(X),$$

випливає, що в розклад полінома $f(X)$ на прості множники в кільці $P[X]$ входить добуток $(X - c_1)_1^k \dots (X - c_r)_r^k$. Отже,

$$f(X) = (X - c_1)^{k_1} \dots (X - c_r)^{k_r} g(X).$$

Зауважимо, що з теореми 3.1.7 випливає, що коефіцієнти полінома $g(X)$ містяться не тільки в полі P , але і в кільці A . Якби, наприклад, $g(c_1) = 0$, то $g(X) = (X - c_1)g_1(X)$ і $f(X) = (X - c_1)^{k_1+1} \dots (X - c_r)^{k_r} g_1(X)$, тобто c_1 був би коренем кратності $\geq k_1 + 1$. Тому $g(c_i) \neq 0$ для $i = 1, \dots, r$. \square

Твердження 3.4.3. *Нехай A — область цілісності (зокрема, поле), $f(X) \in A[X]$. Елемент $c \in A$ є кратним коренем полінома $f(X)$ тоді і тільки тоді, коли $f'(c) = 0$.*

Доведення. Нехай $f(X) = (X - c)^k g(X)$, де $g(c) \neq 0$. Маємо

$$f'(X) = k(X - c)^{k-1} g(X) + (X - c)^k g'(X). \quad (3.4.1)$$

Якщо $k > 1$, то звідси випливає, що $f'(c) = 0$. Навпаки, якщо $k = 1$, то $f'(c) = g(c) \neq 0$. \square

Доведене твердження допускає уточнення у випадку, коли кільце A має характеристику 0.

Означення 3.4.3. Кажуть, що кільце з 1 (зокрема, поле) має характеристику 0, якщо не існує ненульових натуральних чисел n з властивістю $n \cdot 1 = \underbrace{1 + \cdots + 1}_n = 0$.

Наприклад, кільце \mathbb{Z} має характеристику 0, а кільце $\mathbb{Z}/2\mathbb{Z}$ не має цієї властивості, бо $2 \cdot 1 = \bar{0}$ в $\mathbb{Z}/2\mathbb{Z}$.

Твердження 3.4.4. *Нехай A – цілісне кільце характеристики 0. Якщо елемент $c \in A$ є k -кратним коренем полінома $f(X) \in A[X]$, то c є $(k-1)$ -кратним коренем полінома $f'(X)$.*

Доведення. Запишемо (3.4.1) у вигляді

$$f'(X) = (X - c)^{k-1} (kg(X) + (X - c)g'(X)).$$

Оскільки A має характеристику 0, то поліном $kg(X)$ ненульовий. Звідси випливає, що $X - c$ не ділить $kg(X) + (X - c)g'(X)$, тобто c є $(k-1)$ -кратним коренем полінома $f'(X)$. \square

Зауваження 3.4.1. Якщо A не є областю цілісності, то твердження 3.4.2 невірне. Наприклад, поліном $f(X) = X^3 \in \mathbb{Z}/8\mathbb{Z}[X]$ має чотири різних корені: $f(\bar{0}) = f(\bar{2}) = f(\bar{4}) = f(\bar{6}) = 0$. Зауважимо ще, що кільце $\mathbb{Z}/8\mathbb{Z}[X]$ не є факторіальним, бо поліном X^3 допускає різні розклади в добуток незвідних поліномів:

$$X^3 = X(X - \bar{4})^2 = (X - \bar{2})(X^2 + \bar{2}X + \bar{4}) = (X - \bar{6})(X^2 - \bar{2}X + \bar{4}).$$

З твердження 3.4.4 випливає наслідок, що може бути корисним при знаходженні коренів поліномів.

Наслідок 3.4.5. Нехай $f(X) \in P[X]$ – поліном над полем P характеристики 0. Кратні корені полінома $f(X)$ є коренями найбільшого спільного дільника $d(X)$ поліномів $f(X)$ та $f'(X)$. Якщо $f(X) = d(X)h(X)$, то $h(X)$ має ті ж корені, що і $f(X)$ і всі корені полінома $h(X)$ є простими.

3.4.2. Спільний множник двох поліномів. Результант

Якщо два поліноми $f(X)$ і $g(X)$ над полем P мають спільний корінь $a \in P$, то вони мають спільний множник, в який входить $X - a$ і навпаки. Тому варто розглянути таку задачу: коли два поліноми $f(X), g(X) \in P[X]$ мають спільний множник?

Нехай $f(X), g(X) \in R[X]$, де R – факторіальне кільце (зокрема, поле). Константами або сталими поліномами будемо називати поліноми нульового степеня 0.

Теорема 3.4.6. Поліноми f і g мають спільний множник, відмінний від сталої, тоді і тільки тоді, коли існують поліноми $f_1, g_1 \in R[X]$, $\deg f_1 < \deg f$, $\deg g_1 < \deg g$ і такі, що $fg_1 = f_1g$.

Доведення. (\Rightarrow) Якщо поліноми f і g мають спільний множник h , то $f = f_1h$, $g = g_1h$, $\deg f_1 < \deg f$, $\deg g_1 < \deg g$ і $fg_1 = f_1g_1h = f_1g$.

(\Leftarrow) Навпаки, нехай $fg_1 = f_1g$, $\deg f_1 < \deg f$, $\deg g_1 < \deg g$. Розкладемо f і g в добуток незвідних поліномів. Не всі незвідні множники полінома f входять в f_1 , бо $\deg f_1 < \deg f$, тому з рівності $fg_1 = f_1g$ випливає, що деякі незвідні множники f входять в g , а це і означає, що f і g мають спільний множник. \square

Означення 3.4.4. Нехай $f(X) = a_0 + a_1X + \dots + a_nX^n$, $g(X) =$

$b_0 + b_1X + \dots + b_mX^m$ поліноми з кільця $R[X]$. Визначник

$$R(f, g) = \left| \begin{array}{cccc} a_0 & a_1 & \dots & a_n \\ a_0 & a_1 & \dots & a_n \\ \dots & \dots & \dots & \dots \\ & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m \\ b_0 & b_1 & \dots & b_m \\ \dots & \dots & \dots & \dots \\ b_0 & b_1 & \dots & b_m \end{array} \right| \begin{cases} m \\ n \end{cases}$$

називають *результатом* поліномів f і g .

Теорема 3.4.7. Поліноми $f(X), g(X) \in R[X]$ мають несталий спільний множник тоді й лише тоді, коли $R(f, g) = 0$.

Доведення. (\Rightarrow) Нехай поліноми f і g мають несталий спільний множник. Тоді за теоремою 3.4.6 існують ненульові поліноми

$$\begin{aligned} f_1 &= \alpha_0 + \alpha_1X + \dots + \alpha_{n-1}X^{n-1}, \\ g_1 &= \beta_0 + \beta_1X + \dots + \beta_{m-1}X^{m-1}, \end{aligned}$$

для яких $fg_1 = gf_1$. Порівнюючи відповідні коефіцієнти добутків fg_1 і gf_1 , одержимо

$$\begin{cases} a_0\beta_0 = b_0\alpha_0, \\ a_1\beta_0 + a_0\beta_1 = b_1\alpha_0 + b_0\alpha_1, \\ \dots \\ a_n\beta_m = b_m\alpha_n. \end{cases} \quad (3.4.2)$$

Цю систему рівностей можна трактувати як систему лінійних однорідних рівнянь відносно невідомих β_0, \dots, α_n . Ця система має $m+n$ рівнянь, $m+n$ невідомих і має ненульовий розв'язок. Отже визначник цієї системи, який з точністю до знаку і є $R(f, g)$, дорівнює нулю.

(\Leftarrow) Навпаки, якщо $R(f, g) = 0$, то система (3.4.2) має ненульовий розв'язок в полі дробів P кільця R . Домноживши всі α_i, β_i на їх спільний знаменник, одержимо ненульовий розв'язок в кільці R . Якщо не всі α_i дорівнюють нулю, то $f_1 \neq 0$, отже і $g_1 \neq 0$, а оскільки $fg_1 = f_1g$, то за теоремою 3.4.6 поліноми f і g мають не сталій множник. \square

3.4.3. Результант однорідних поліномів

Означення 3.4.5. Поліном $f(X_1, \dots, X_n)$ з кільця поліномів $R[X_1, \dots, X_n]$ називають *однорідним* степеня m , якщо в кільці $R[X_1, \dots, X_n, T]$ правильна рівність

$$f(TX_1, \dots, TX_n) = T^m f(X_1, \dots, X_n).$$

Теорема 3.4.8. *Hexay*

$$\begin{aligned} f_r &= a_r + a_{r-1}X_n + \dots + a_0X_n^r, \\ g_s &= b_s + b_{s-1}X_n + \dots + b_0X_n^s, \end{aligned}$$

де a_i, b_i — однорідні поліноми степеня i відносно X_1, \dots, X_{n-1} . Тоді результант $R(f_r, g_s)$ поліномів f_r і g_s відносно X_n або дорівнює нулю або є однорідним поліномом степеня rs від X_1, \dots, X_{n-1} .

Доведення. Зрозуміло, що результант $R(f_r, g_s)$ є поліномом $R(X_1, \dots, X_{n-1})$ від $n-1$ змінних X_1, \dots, X_{n-1} . Припустимо, що $R(X_1, \dots, X_{n-1}) \neq 0$. Тоді $R(TX_1, \dots, TX_{n-1}) =$

$$= \begin{vmatrix} T^r a_r & T^{r-1} a_{r-1} & \dots & a_0 & & \\ & T^r a_r & \dots & & a_0 & \\ \dots & \dots & \dots & \dots & \dots & \\ T^s b_s & T^{s-1} b_{s-1} & \dots & b_0 & \dots & a_0 \\ & T^s b_s & \dots & & b_0 & \\ \dots & \dots & \dots & \dots & \dots & \\ & T^s b_s & T^{s-1} b_{s-1} & \dots & b_0 & \end{vmatrix}. \quad (3.4.3)$$

Домножимо у визначнику (3.4.3) i -ий рядок для $1 \leq i \leq s$ на T^{s-i+1} , а j -ий рядок $s+1 \leq j \leq s+r$ на $T^{r+s-j+1}$. Одержано

$$T^p R(TX_1, \dots, TX_{n-1}) =$$

$$= \begin{vmatrix} T^{r+s}a_r & T^{r+s-1}a_{r-1} & \dots & T^s a_0 & \dots & \dots \\ \dots & T^{r+s-1}a_r & \dots & T^{s-1}a_0 & \dots & \dots \\ \dots & \dots & T^{r+1}a_r & \dots & Ta_0 & \dots \\ T^{r+s}b_s & T^{r+s-1}b_{s-1} & \dots & T^r b_0 & \dots & \dots \\ \dots & T^{r+s-1}b_s & \dots & T^{r-1}b_0 & \dots & \dots \\ \dots & \dots & T^{1+s}b_s & \dots & Tb_0 & \dots \end{vmatrix} =$$

$$= T^q R(X_1, \dots, X_n), \quad (3.4.4)$$

де $p = \frac{r(r+1)}{2} + \frac{s(s+1)}{2}$ і $q = \frac{(r+s)(r+s+1)}{2}$. Оскільки

$$q - p = \frac{(r+s)(r+s+1)}{2} - \frac{r(r+1)}{2} - \frac{s(s+1)}{2} = rs,$$

то з (3.4.4) одержуємо

$$R(TX_1, \dots, TX_n) = T^{rs} R(X_1, \dots, X_n),$$

що й потрібно було довести. \square

3.4.4. Основна теорема алгебри

Теорема 3.4.9. Якщо $f(X) \in \mathbb{C}[X]$ – поліном з комплексними коефіцієнтами, $i \deg f(X) \geq 1$ то $f(X)$ має хоч один комплексний корінь.

Зауважимо, що назва “основна теорема алгебри” – це данина традиції; вона нагадує про часи, коли основною задачею алгебри була задача знаходження коренів поліномів.

Основна теорема алгебри вперше була сформульована (у вигляді, що відрізняється від сучасного) А. Жірапом і Р. Декартом.

К. Маклорен і Л. Ейлер сформулювати її у вигляді, що еквівалентний сучасному: кожний поліном з дійсними коефіцієнтами можна розкласти в добуток лінійних та квадратних поліномів з дійсними коефіцієнтами. Першим, хто опублікував доведення, був Ж. Д'Аламбер (1746), після цього у другій половині XVIIIст. з'являються доведення Л. Ейлера, П. Лапласа, Ж. Лагранжа та інших математиків; всі ці доведення мали певні недоліки.

Перше строгое доведення основної теореми алгебри запропонував К. Гаус. У 1808–1817 роках він опублікував декілька різних доведень цієї теореми. Зараз існує багато доведень основної теореми алгебри. Пропонуємо читачеві ознайомитися хоч з одним з них за іншими підручниками. Зауважимо, що у всіх доведеннях основної теореми алгебри використовуються специфічні топологічні властивості дійсних та комплексних чисел. В курсі теорії функцій комплексної змінної основна теорема алгебри доводиться в один рядок як наслідок з теореми Ліувілля про обмеженість цілих аналітичних функцій. Сформулюємо деякі наслідки з основної теореми алгебри.

Наслідок 3.4.10. *Будь-який поліном степеня ≥ 1 над полем \mathbb{C} розкладається в $\mathbb{C}[X]$ на лінійні множники.*

Доведення. Нехай $f(X) \in \mathbb{C}[X]$, $\deg f \geq 1$. Міркуємо індукцією за $m = \deg f$. Якщо $m = 1$, то доводити нічого. Нехай $m > 1$ і наслідок доведено для всіх поліномів степеня $< m$. За основною теоремою алгебри існує $c_1 \in \mathbb{C}$, $f(c_1) = 0$. Тоді за теоремою Безу $f(X) = (X - c_1)f_1(X)$. Розкладши $f_1(X)$ на лінійні множники, що можливо за припущенням індукції, одержимо шуканий розклад полінома $f(X)$. \square

Наслідок 3.4.11. *Незвідними поліномами в кільці $\mathbb{C}[X]$ є поліноми першого степеня і тільки вони.*

Наслідок 3.4.12. *Незвідними поліномами в кільці $\mathbb{R}[X]$ поліномів над полем дійсних чисел \mathbb{R} є поліноми першого степеня та квадратні тричлени з від'ємними дискримінантами і тільки вони.*

Доведення. Очевидно, що поліноми першого степеня та квадратні тричлени без дійсних коренів є незвідними над \mathbb{R} . Навпаки, нехай $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{R}[X]$. За основною теоремою алгебри $f(X)$ має комплексний корінь c . Якщо $c \in \mathbb{R}$, то $X - c$ ділить $f(X)$.

Якщо $c \in \mathbb{C} \setminus \mathbb{R}$, то коренем полінома $f(X)$ буде і спряжене число \bar{c} . Справді, переходячи до спряжених чисел в рівності $a_0 + a_1c + \dots + a_nc^n = 0$, і використовуючи, що число, спряжене до суми (добутку), дорівнює сумі (добутку) спряжених, а також $\bar{a}_i = a_i$ для $0 \leq i \leq n$, одержимо $a_0 + a_1\bar{c} + \dots + a_n\bar{c}^n = 0$, тобто $f(\bar{c}) = 0$. Звідси випливає, що $f(X)$ ділиться на $X - \bar{c}$ і на $X - c$, але $X - \bar{c}$ і $X - c$ взаємно прості. Отже, $f(X)$ ділиться на поліном $(X - c)(X - \bar{c}) = X^2 - (c + \bar{c})X + c\bar{c}$, коефіцієнти якого, очевидно, дійсні. \square

3.4.5. Формули Вієта

Нехай унітарний (тобто зі старшим коефіцієнтом 1) поліном $f(X) \in P[X]$ має в полі P (або в деякому його розширенні) n коренів c_1, c_2, \dots, c_n , враховуючи їх кратності. Тоді

$$f(X) = (X - c_1)(X - c_2) \dots (X - c_n). \quad (3.4.5)$$

Запишемо $f(X)$ у звичайному вигляді по степенях X :

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0. \quad (3.4.6)$$

Прирівнюючи коефіцієнти при одинакових степенях X у (3.4.5) і (3.4.6), маємо

$$\begin{aligned} a_{n-1} &= -(c_1 + c_2 + \dots + c_n), \\ a_{n-2} &= c_1c_2 + c_1c_3 + \dots + c_{n-1}c_n, \\ &\dots\dots\dots \\ a_{n-k} &= (-1)^k \sum_{i_1 < i_2 < \dots < i_k} c_{i_1}c_{i_2} \dots c_{i_k}, \\ &\dots\dots\dots \\ a_0 &= (-1)^n c_1c_2 \dots c_n. \end{aligned}$$

Ці рівності називають *формулами Вієта*.

3.5. Вправи

1) *Многочлени як функції.* Нехай A – комутативне кільце, $f(X) \in A[X]$. Поставимо у відповідність поліному $f(X)$ відображення $\hat{f}: A \rightarrow A$, де $\hat{f}(a) = f(a)$ для всіх $a \in A$. Позначимо через $\widehat{A[X]}$ множину всіх таких відображень \hat{f} .

2) Показати, що множина всіх відображень A^A кільця A в себе є кільцем відносно операцій:

$$(\phi + \psi)(a) = \phi(a) + \psi(a), \quad (\phi \cdot \psi)(a) = \phi(a)\psi(a),$$

де $\phi, \psi \in A^A$, а множина $\widehat{A[X]}$ є його підкільцем.

3) Довести, що коли A – область цілісності з нескінченим числом елементів, то відображення $A[X] \rightarrow \widehat{A[X]}$, яке поліному f ставить у відповідність функцію \hat{f} , є ізоморфізмом.

4) На прикладі кільця поліномів з коефіцієтами з поля $\mathbb{Z}/p\mathbb{Z}$ (p просте) переконатися, що твердження вправи 2 невірне, якщо A – скінчenna область цілісності. (*Вказівка.* Різним поліномам 0, $X^p - X$ відповідає нульова функція.)

5) *Інтерполяція функцій поліномами.* Постановка задачі інтерполяції функцій поліномами є така: нехай P – поле і нехай задана таблиця

a_0	a_1	\dots	a_n
b_0	b_1	\dots	b_n

,

де $a_i, b_i \in P$ і всі a_0, a_1, \dots, a_n різні. Потрібно знайти поліном $f(X) \in P[X]$ такий, що $f(a_i) = b_i$ для всіх i , $1 \leq i \leq n$, причому $\deg f(X) \leq n$.

Показати, що сформульована вище задача інтерполяції має не більше ніж один розв'язок. (*Вказівка.* Кількість коренів полінома над полем не більша ніж степінь цього полінома.)

- 6) *Інтерполяційна формула Лагранжа.* Перевірити, що поліном

$$f(X) = \sum_{i=1}^n b_i \frac{(X - a_0) \dots (X - a_{i-1})(X - a_{i+1}) \dots (X - a_n)}{(a_i - a_0) \dots (a_i - a_{i-1})(a_i - a_{i+1}) \dots (a_i - a_n)}$$

є розв'язком задачі інтерполяції.

- 7) *Інтерполяційна формула Ньютона.* Перевірити, що поліном

$$f(X) = u_0 + u_1(X - a_0) + \dots + u_n(X - a_0)(X - a_1) \dots (X - a_n),$$

де коефіцієнти u_0, u_1, \dots, u_n визначаються за допомогою послідовної підстановки замість X значень a_0, a_1, \dots, a_n , теж є розв'язком задачі інтерполяції.

- 8) *Формула Тейлора.* Нехай P — поле характеристики 0, $a \in P$. Для кожного полінома $f(X) \in P[X]$ $f(X) =$

$$= f(a) + \frac{f'(a)}{1!}(X - a) + \frac{f''(a)}{2!}(X - a)^2 + \dots + \frac{f^{(n)}(a)}{n!}(X - a)^n.$$

(Вказівка. Продиференціювати k разів рівність $f(X) = \sum_{i=0}^n b_i(X - a)^i$ і підставити $X = a$.)

- 9) Для кільця поліномів $P[X_1, \dots, X_n]$ від n змінних вводять оператор часткового диференціювання по k -ій змінній:

$$\frac{\partial}{\partial X_k}: aX_1^{i_1} \dots X_k^{i_k} \dots X_n^{i_n} \mapsto i_k a X_1^{i_1} \dots X_k^{i_k-1} \dots X_n^{i_n},$$

де $a \in P$. Довести, що коли $f(X_1, \dots, X_n)$ — однорідний поліном степеня m , то

$$\sum_{k=1}^n X_k \frac{\partial f}{\partial X_k} = m f(X_1, \dots, X_n).$$

- 10) Довести, що коли нескоротний раціональний дріб $\frac{p}{q}$ є коренем полінома $f(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + a_nX^n$ з цілими коефіцієнтами, то а) $p|a_0$; б) $q|a_n$; в) $p - mq|f(m)$ для всіх $m \in \mathbb{Z}$.

- 11) Нехай P — поле дробів області цілісності R , і нехай R є підкільцем деякого поля P' . Довести, що поле P ізоморфне підполю поля P' .

Розклад раціональних функцій на прості дроби. Нехай $P[X]$ — кільце поліномів над полем P . Поле дробів кільця $P[X]$ позначають $P(X)$ і називають полем раціональних функцій від однієї змінної над полем P . Якщо $\frac{f}{g} \in P(X)$, то $\frac{f}{g}$ називають нескоротним дробом, якщо поліноми f і g взаємно прості. Якщо $\deg f < \deg g$, то $\frac{f}{g}$ називають правильним дробом (нульовий поліном теж вважаємо правильним дробом). $\deg f - \deg g$ називають степенем дробу $\frac{f}{g}$. Степінь дробу не залежить від конкретного вибору поліномів f і g .

- 12) Довести, що кожний раціональний дріб $\frac{f}{g}$ з поля $P(X)$ одно-значно подається у вигляді суми полінома та правильного дробу. (*Вказівка.* а) Розділити f з остачею на g . б) Якщо $a_1 + \frac{r_1}{g_1} = a_2 + \frac{r_2}{g_2}$, то $a_1 - a_2 = \frac{r_2g_1 - r_1g_2}{g_1g_2}$ і для доведення єдиності потрібно порівняти степені обох частин цієї рівності.)
- 13) Правильний раціональний дріб $\frac{f}{g}$ називають простим, якщо $g = p^n$, $n \geq 1$, де p — незвідний поліном і $\deg f < \deg p$. Довести, що кожний правильний раціональний дріб $\frac{f}{g}$ розкладається в суму простих дробів. (*Вказівка.* а) Якщо $g = g_1g_2$, де g_1 і g_2 взаємно прості, то існують $u_1, u_2 \in P[X]$, $u_2g_1 + u_1g_2 = 1$. Звідси $f = fu_2g_1 + fu_1g_2$. Розділимо fu_2 з остачею на g_2 : $fu_2 = dg_2 + v_2$. Тоді $f = v_2g_1 + v_1g_2$ з $v_1 = fu_1 + dg_1$ і $\frac{f}{g} = \frac{v_1}{g_1} + \frac{v_2}{g_2}$ — сума правильних дробів. б) Якщо $g = p_1^{n_1}p_2^{n_2} \dots p_m^{n_m}$, де p_1, \dots, p_n — незвідні поліноми, то використовуючи а), можна одержати $\frac{f}{g} = \frac{a_1}{p_1^{n_1}} + \dots + \frac{a_m}{p_m^{n_m}}$.

в) Чисельник правильного дробу $\frac{a}{p^n}$ подати у вигляді

$$a = d_1 p^{n-1} + d_2 p^{n-2} + \cdots + d_{n-1} p + d_n,$$

де $\deg d_i < \deg p.$)

- 14) Показати, що кожна раціональна функція над полем дійсних чисел є сумою полінома та дробів вигляду $\frac{a}{(X-c)^m}$ та $\frac{bX+d}{((X+l)^2+r^2)^n}$, де $a, b, c, d, l, r \in \mathbb{R}$, $r \neq 0$, $m, n \in \mathbb{N}$.

- 15) *Метод Штурма виділення дійсних коренів поліномів з дійсними коефіцієнтами* (див. [?]) Нехай $f(X) \in \mathbb{R}[X]$. Припустимо, що нас цікавить кількість дійсних коренів полінома $f(X)$, що належать проміжку (a, b) . Цю кількість можна підрахувати за допомогою послідовності поліномів Штурма. Послідовність f_0, f_1, \dots, f_n поліномів називають послідовністю Штурма для полінома $f = f_0$ і інтервалу (a, b) , якщо ця послідовність має такі властивості:

- 1) f_n не має коренів в інтервалі (a, b) ;
- 2) Сусідні поліноми не мають спільних коренів в інтервалі (a, b) ;
- 3) Якщо $f_i(X_0) = 0$, де $X_0 \in (a, b)$, $1 \leq i \leq n - 1$, то $f_{i-1}(X_0)f_{i+1}(X_0) < 0$;
- 4) Добуток f_0f_1 змінює знак з мінуса на плюс, якщо X , зростаючи, переходить через корінь полінома f_0 .

Теорема Штурма. Показати, що кількість коренів полінома $f(X) \in \mathbb{R}[X]$ в проміжку $[a, b]$ дорівнює кількості змін знаків в значеннях поліномів послідовності Штурма при $X = a$ мінус кількість змін знаків при $X = b$. Вважається, що кінці проміжка не є коренями $f(X)$. (*Вказівки.*
а) Якщо X_0 — корінь деякого полінома f_i з послідовності Штурма, $X_0 \in (a, b)$ і X_0 не є коренем полінома f_0 , то можна розглянути окіл $(X_0 - \varepsilon, X_0 + \varepsilon)$ точки X_0 , в якому поліноми ряду Штурма не мають інших коренів, крім X_0 .

Використовуючи властивості послідовності Штурма і перебір можливих випадків, показати, що при переході X від $X_0 - \varepsilon$ через X_0 до $X_0 + \varepsilon$ кількість змін знаків в послідовності Штурма не змінюється. б) Якщо X_0 — корінь f_0 і, можливо, деякого іншого полінома f_i , то, використовуючи, як і раніше, проміжок $(X_0 - \varepsilon, X_0 + \varepsilon)$, властивості послідовності Штурма та перебір можливих випадків, показати, що при переході через X_0 в підпослідовності f_0, f_1 кількість змін знаків зменшується на 1, а в підпослідовності f_{i-1}, f_i, f_{i+1} вона не змінюється.)

- 16) *Побудова послідовності Штурма.* Нехай $f(X) \in \mathbb{R}[X]$ — поліном без кратних коренів. Візьмемо $f_0 = f$, $f_1 = f'$ — похідна полінома f і для $i \geq 2$ $f_i =$ остатча, взята з потилежним знаком при діленні f_{i-2} на f_{i-1} . Останній поліном f_k буде ненульовою константою, оскільки f і f' , як випливає з нашого припущення, є взаємно простими. Показати, що послідовність f_0, f_1, \dots, f_k є послідовністю Штурма для будь-якого проміжка. (*Вказівки.* а) Властивість 1) з означення послідовності Штурма очевидна. Властивість 2) одержується із взаємної простоти f_i та f_{i-1} , оскільки, як показує алгоритм Евкліда знаходження НСД, їх спільний корінь мусить бути спільним коренем $f_0 = f$ і $f_1 = f'$. Для доведення властивості 3) потрібно записати $f_i + 1 = -f_{i-1} + f_i d_i$ і підставити сюди X_0 . б) Залишається перевірити властивість 4). Маємо $f(X) = (X - X_0)g(X)$, де $g(X_0) \neq 0$, $f' = g + (X - X_0)g'$, $ff' = (X - X_0)[g^2 + (X - X_0)g'] = (X - X_0)u(X)$. Оскільки $u(X_0) > 0$, то $u(X) > 0$ в деякому околі точки X_0 . Звідси випливає, що ff' змінює знак з мінуса на плюс при переході через X_0 .)

Зауважимо, що метод Штурма, звичайно, використовує неперервність поліномів над \mathbb{R} як функцій дійсної змінної.

- 17) *Симетричні поліноми.* Нехай $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \in S_n$, $f = f(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$, де R — комутативне

кільце. Позначимо поліном $f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ символом f^σ : він одержується з f заміною X_1 на $X_{\sigma(1)}, \dots, X_n$ на $X_{\sigma(n)}$. Поліном f називають *симетричним*, якщо $f^\sigma = f$ для всіх $\sigma \in S_n$. Поліноми

$$\begin{aligned}s_1 &= X_1 + X_2 + \dots + X_n, \\ s_2 &= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n, \\ &\dots \\ s_n &= X_1X_2 \dots X_n.\end{aligned}$$

називають *елементарними симетричними поліномами*.

Для дослідження поліномів від декількох змінних є корисним поняття *лексикографічного впорядкування* мономів: моном $aX_1^{k_1}X_2^{k_2} \dots X_n^{k_n}$ старший від монома $bX_1^{l_1}X_2^{l_2} \dots X_n^{l_n}$, якщо перша ненульова різниця серед $k_1 - l_1, k_2 - l_2, \dots, k_n - l_n$ є додатною. Очевидно, що в кожний ненульовий поліном від декількох змінних входить єдиний найстарший член. Його називають старшим членом полінома.

Довести, що старший член добутку двох поліномів дорівнює добутку старших членів поліномів — співмножників. (*Вказівка*. Порівняти добуток старших членів з іншими добутками мономів або використати індукцію за кількістю змінних.)

- 18) Показати, що коли $aX_1^{k_1}X_2^{k_2} \dots X_n^{k_n}$ — старший член симетричного полінома, то $k_1 \geq k_2 \geq \dots \geq k_n$. (*Вказівка*. Якщо, наприклад, $k_1 < k_2$, то моном $aX_1^{k_2}X_2^{k_1} \dots X_n^{k_n}$, який теж входить в наш симетричний поліном, старший від $aX_1^{k_1}X_2^{k_2} \dots X_n^{k_n}$. Суперечність.)
- 19) Показати, що кожний симетричний поліном є поліномом від елементарних симетричних поліномів. (*Вказівки*. Досить обмежитися випадком однорідних симетричних поліномів. Нехай $f(X_1, \dots, X_n)$ — однорідний симетричний поліном і $aX_1^{k_1}X_2^{k_2} \dots X_n^{k_n}$ — його старший член. Використо-

вуючи вправи 16 і 17, одержати, що поліном

$$f_1 = f - as_1^{k_2-k_1}s_2^{k_2-k_3} \dots s_{n-1}^{k_{n-1}-k_n}s_n^{k_n}$$

є симетричним і має менший (згідно лексикографічного впорядкування) старший член. Застосуйте цей же прийом до f_1 , і так далі, доки через скінченну кількість кроків різниця дорівнюватиме нулю.)

- 20) Показати, що $f(s_1, s_2, \dots, s_n)$ — ненульовий поліном, якщо $f(X_1, X_2, \dots, X_n)$ — ненульовий поліном.

- 21) Вивести з вправи 19, що кожний симетричний поліном єдиним способом записується у вигляді полінома від елементарних симетричних поліномів.

- 22) Нехай $p_k = p_k(X_1, \dots, X_n) = X_1^k + X_2^k + \dots + X_n^k$. Довести наступні формули (*формули Ньютона*):

$$p_k - p_{k-1}s_1 + p_{k-2}s_2 + \dots + (-1)^{k-1}p_1s_{k-1} + (-1)^kks_k = 0$$

для $1 \leq k \leq n$ і

$$\begin{aligned} p_k - p_{k-1}s_1 + p_{k-2}s_2 + \dots + \\ + (-1)^{n-1}p_{k-n+1}s_{n-1} + (-1)^n p_{k-n}s_n = 0 \end{aligned}$$

для $k > n$. (*Вказівка*. Використати рівність

$$(Y - X_1) \dots (Y - X_n) = Y^n - s_1Y^{n-1} + s_2Y^{n-2} + \dots + (-1)^n s_n$$

для доведення формул Ньютона для $k \geq n$. У випадку $k < n$ використайте індукцію за $r = n - k$.

- 23) *Дискримінантом* полінома називають результант полінома та його похідної. Довести, що поліном над областю цілісності характеристики 0 має кратний множник тоді і тільки тоді, коли його дискримінант дорівнює нулю.

- 24) Обчислити дискримінант поліномів $X^2 + pX + q$ та $X^3 + aX + b$.

Розділ 4

Класи лишків та їх застосування

4.1. Кільце $\mathbb{Z}/n\mathbb{Z}$

4.1.1. Означення кільця класів лишків. Скінченні поля

Розглянемо в кільці цілих чисел \mathbb{Z} підмножину $n\mathbb{Z}$ всіх цілих чисел, що діляться на задане натуральне число n . Множина $n\mathbb{Z}$ є ідеалом кільця \mathbb{Z} , тому можна утворити фактор-кільце $\mathbb{Z}/n\mathbb{Z}$. Фактор-кільце $\mathbb{Z}/n\mathbb{Z}$ для різних n мають велике значення в елементарній теорії чисел та її різноманітних застосуваннях: від проблеми розв'язування рівнянь в цілих числах до питань, пов'язаних з шифруванням та передачею інформації.

Елементами кільця $\mathbb{Z}/n\mathbb{Z}$ є суміжні класи $\bar{a} = a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$. Якщо $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, то кажуть, що \bar{a} — клас лишків з представником a . Ми вже неодноразово використовували критерій рівності суміжних класів. Запишемо цей критерій для випадку класів лишків:

$$\bar{a}_1 = \bar{a}_2 \iff n \mid a_1 - a_2. \quad (4.1.1)$$

Розділимо a_1 і a_2 з остачею на n : $a_1 = nd_1 + r_1$, $a_2 = nd_2 + r_2$, $0 \leq r_1, r_2 < n$. Звідси маємо $a_1 - a_2 = n(d_1 - d_2) + r_1 - r_2$. Тому $n \mid a_1 - a_2$ тоді і тільки тоді, коли $n \mid r_1 - r_2$, а це можливо тоді і тільки тоді, коли $r_1 = r_2$. Отже, критерій (4.1.1) можна

сформулювати так: $\bar{a_1} = \bar{a_2}$ тоді і тільки тоді, коли a_1 і a_2 мають однакові остачі (лишки) при діленні на n .

Якщо $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, то $\bar{a} = \bar{r}$, де r — остатча від ділення a на n . Звідси одержуємо, що кільце $\mathbb{Z}/n\mathbb{Z}$ має n елементів

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}.$$

$\bar{0}$ — нульовий елемент цього кільця, а $\bar{1}$ — одиничний елемент. $\mathbb{Z}/n\mathbb{Z}$ — комутативне кільце, що має дільники нуля у випадку, коли n не є простим числом.

Нагадаємо, що додавання та множення у кільці $\mathbb{Z}/n\mathbb{Z}$ визначаються так само, як і в будь-якому фактор-кільці, тобто:

$$\bar{a} + \bar{b} = \overline{fa+b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Приклад 4.1.1. 1) Складемо таблички додавання та множення у кільці $\mathbb{Z}/7\mathbb{Z}$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$							
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

2) Розглянемо число 1991^{1994} . Як знайти остатчу від ділення цього числа, наприклад, на 17? Безнадійно пробувати підносити 1991 до степеня 1994 . Замість цього розглянемо елемент 1991^{1994} кільця $\mathbb{Z}/17\mathbb{Z}$. Оскільки $\bar{1991} = \bar{2}$, то $\bar{1991}^{1994} = \bar{2}^{1994} = \bar{2}^{4 \cdot 498 + 2} = (\bar{2}^4)^{498} \cdot \bar{2}^2 = \bar{16}^{498} \cdot \bar{2}^2 = \bar{-1}^{498} \cdot \bar{2}^2 = \bar{1} \cdot \bar{2}^2 = \bar{4}$. Тому число 1991^{1994} дає в остатчі 4 при діленні на 17.

4.1.2. Поле \mathbb{F}_p

З таблички множення в кільці $\mathbb{Z}/7\mathbb{Z}$ видно, що в її кожному рядку, крім першого, який складається лише з нулів, зустрічається елемент $\bar{1}$. Це означає, що для кожного ненульового елемента в $\mathbb{Z}/7\mathbb{Z}$ існує обернений відносно множення, тобто $\mathbb{Z}/7\mathbb{Z}$ є полем. Нагадаємо, що у Розділі 1 була доведена теорема, яка стверджує, що кільце $\mathbb{Z}/n\mathbb{Z}$ є полем тоді й лише тоді, коли n — просте число.

Виявляється, що існують і інші скінчені поля, кількість елементів яких не обов'язково є простим числом. Щоб переконатися у цьому, розглянемо один приклад поля з чотирьох елементів.

Приклад 4.1.2. Розглянемо кільце поліномів $R = \mathbb{Z}/2\mathbb{Z}[X]$ з коефіцієнтами з поля $\mathbb{Z}/2\mathbb{Z}$. $X^2 + X + \bar{1}$ — незвідний поліном у цьому кільці. $\mathcal{I} = (X^2 + X + \bar{1})\mathbb{Z}/2\mathbb{Z}[X]$ — головний ідеал, породжений поліномом $X^2 + X + \bar{1}$. Зайдемо всі елементи фактор-кільця R/\mathcal{I} . Якщо $\overline{f(X)} \in R/\mathcal{I}$, то, розділивши $f(X)$ на $X^2 + X + \bar{1}$ з остачею, одержимо

$$\begin{aligned} f(X) &= d(X)(X^2 + X + \bar{1}) + r(X), \text{ де } \deg r(X) < 2, \\ \text{тобто } r(X) &= a_0 + a_1 X, \quad a_0, a_1 \in \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Отже, $\overline{f(X)} = \overline{a_0 + a_1 X}$ за критерієм рівності суміжних класів, а тому кожен елемент фактор-кільця R/\mathcal{I} є одним з 4-х елементів $\bar{0}, \bar{1}, \bar{X}$ і $\bar{1+X}$. Тепер $\bar{X}(1+\bar{X}) = \overline{X^2 + X} = \bar{1}$. Це означає, що всі ненульові елементи кільця R/\mathcal{I} мають обернені відносно множення: $\bar{1}^{-1} = \bar{1}$, $\bar{X}^{-1} = \bar{1+X}$ і $\bar{1+X}^{-1} = \bar{X}$. Тому R/\mathcal{I} є полем з чотирьох елементів.

Зауваження 4.1.1. Скінченне поле з q елементів прийнято позначати символом \mathbb{F}_q .

4.1.3. Мультиплікативна група скінченного поля

Нехай \mathbb{F}_q — скінченне поле з q елементів. Зокрема, \mathbb{F}_q може означати поле з p елементів $\mathbb{Z}/p\mathbb{Z}$, коли $q = p$ — просте число. Ми

тільки що бачили, що можуть існувати і інші скінченні поля, відмінні від $\mathbb{Z}/p\mathbb{Z}$. Позначимо символом \mathbb{F}_q^* мультиплікативну групу ненульових елементів поля \mathbb{F}_q .

Теорема 4.1.1. Група \mathbb{F}_q^* — циклічна.

Доведення. Доведення. Можна вважати, що $q \geq 3$, бо при $q = 2$ твердження теореми тривіальне. Нехай $n = q - 1$ — порядок групи \mathbb{F}_q^* . Розкладемо число n на прості множники:

$$n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}.$$

Для кожного p_i , $1 \leq i \leq s$, поліном $X^{\frac{n}{p_i}} - 1$ має не більше, ніж $\frac{n}{p_i}$ коренів в полі \mathbb{F}_q . Оскільки $\frac{n}{p_i} < n$, а кожний з n елементів групи \mathbb{F}_q^* є коренем полінома $X^n - 1$ за наслідком з теореми Лагранжа, то існує елемент $b_i \in \mathbb{F}_q^*$, який не є коренем полінома $X^{\frac{n}{p_i}} - 1$. Нехай $c_i = b_i^{\frac{n}{k_i}}$. Тоді порядок елемента c_i дорівнює точно $p_i^{k_i}$. Справді, $c_i^{p_i^{k_i}} = b_i^n = 1$, і якби існував менший показник h , для якого $c_i^h = 1$, то $h = p_i^{l_i}$, де $l_i < k_i$, і ми мали б $c_i^h = c_i^{p_i^{l_i}} = b_i^{\frac{n}{k_i-l_i}} = 1$. Звідси

$$\left(b_i^{\frac{n}{k_i-l_i}}\right)^{p_i^{k_i-l_i-1}} = b_i^{\frac{n}{p_i}} = 1,$$

а це суперечить вибору b_i .

Розглянемо тепер елемент $a = c_1 \cdots c_s$ і покажемо, що його порядок дорівнює n . Якщо це не так, то порядок елемента a є власним дільником числа n , отже, є дільником хоч одного з чисел $\frac{n}{p_i}$, $1 \leq i \leq s$. Не зменшуючи загальності, можна вважати, що він є дільником числа $\frac{n}{p_1}$. Тоді $a^{\frac{n}{p_1}} = 1$ і ми маємо

$$a^{\frac{n}{p_1}} = c_1^{\frac{n}{p_1}} \cdot c_2^{\frac{n}{p_1}} \cdots c_s^{\frac{n}{p_1}} = 1.$$

$c_i^{\frac{n}{p_1}} = 1$ для $2 \leq i \leq s$, бо число $\frac{n}{p_1}$ ділиться на $p_i^{k_i}$ і тому ми одержуємо

$$c_1^{\frac{n}{p_1}} = 1.$$

Остання рівність означає, що $\frac{n}{p_1}$ ділиться на $p_1^{k_1}$, а це неможливо. Одержані суперечність, а тому припущення, що порядок елемента a менший, ніж n , невірне. Отже, порядок елемента a дорівнює порядку n групи \mathbb{F}_q^* . Тому циклічна група, породжена елементом a , збігається з усією групою \mathbb{F}_q^* . \square

Зауваження 4.1.2. Ці міркування показують також, що кожна скінченна підгрупа мультиплікативної групи будь-якого поля є циклічною.

4.1.4. функція Ойлера

Нехай R — будь-яке комутативне кільце з 1. Розглянемо множину

$$R^* = \{u \in R \mid \exists v \in R \quad uv = 1\}.$$

Множину R^* будемо називати *множиною одиниць кільця R* . Виявляється, що R^* є групою відносно множення. Цю групу називають *групою одиниць кільця R* .

Твердження 4.1.2. R^* — група відносно множення.

Доведення. Перш за все покажемо, що множина R^* є замкненою відносно множення. Нехай $u_1, u_2 \in R^*$. Тоді $u_1v_1 = 1$ і $u_2v_2 = 1$ для деяких $v_1, v_2 \in R$. Тому $(u_1u_2)(v_1v_2) = (u_1v_1)(u_2v_2) = 1$ і $u_1u_2 \in R^*$. Множення в R^* асоціативне і комутативне, бо воно асоціативне і комутативне в R . Далі, очевидно, $1 \in R^*$. Для кожного $u \in R^*$ існує обернений за означенням R^* . \square

Позначимо через $|(\mathbb{Z}/n\mathbb{Z})^*|$ порядок групи одиниць $(\mathbb{Z}/n\mathbb{Z})^*$ кільця $\mathbb{Z}/n\mathbb{Z}$.

Означення 4.1.1. Функцією Ойлера називають функцію ϕ , визначену на множині ненульових натуральних чисел, для якої

$$\phi(n) = \begin{cases} 1, & \text{якщо } n = 1, \\ |(\mathbb{Z}/n\mathbb{Z})^*|, & \text{якщо } n > 1. \end{cases}$$

Теорема 4.1.3. 1) $a \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow (a, n) = 1$, тому $\phi(n) =$ кількість чисел множини $\{1, 2, \dots, n-1\}$, які взаємно прості з n .

2) $\phi(n)$ = кількість первісних коренів степеня n з 1 у полі комплексних чисел \mathbb{C} .

3) Якщо m і n взаємно прості, то $\phi(mn) = \phi(m)\phi(n)$.

4) Якщо $n = p_1^{k_1} \cdots p_s^{k_s}$ — розклад числа n на прості множники, то

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

Доведення. 1) Досить показати, що $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow (a, n) = 1$. Маємо $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \exists \bar{b} \bar{a} \cdot \bar{b} = \bar{1} \Leftrightarrow \exists b \in \mathbb{Z} ab - 1 = nl, l \in \mathbb{Z} \Leftrightarrow \exists b, l \in \mathbb{Z} ab - nl = 1 \Leftrightarrow (a, n) = 1$.

2) Якщо ξ — первісний корінь n -ої степені з одиниці, то ξ^k ($0 < k < n$) — первісний корінь n -ої степені з одиниці тоді і тільки тоді, коли $(k, n) = 1$ (див твердження 1.7.8). Тому за першою частиною теореми $\phi(n)$ = кількість первісних коренів n -го степеня з одиниці.

3) Доведемо, що добуток первісного кореня ξ n -го степеня з одиниці і первісного кореня η m -го степеня з 1 є первісним коренем nm -го степеня з одиниці. Маємо $(\xi\eta)^{nm} = (\xi^n)^m(\eta^m)^n = 1$. Якщо існує менший показник r , для якого $(\xi\eta)^r = 1$, то $r|mn$. Звідси за основною теоремою арифметики (теоремою про факторіальність кільця цілих чисел) випливає, що $r = m_1n_1$, де $m_1|m$ і $n_1|n$, і, наприклад, $0 < m_1 < m$. Тоді $1 = (\xi\eta)^{m_1n_1} = (\xi\eta)^{m_1n} = (\xi^n)^{m_1}\eta^{m_1n} = \eta^{m_1n}$. Звідси одержуємо, що $m|m_1n$, і, оскільки, $m > m_1$, то деякі прості дільники числа m повинні ділити і n . Одержано суперечність з тим, що m і n взаємно прості числа, тому $\xi\eta$ є первісним коренем степеня mn з 1.

Навпаки, кожний первісний корінь степеня mn є добутком первісних коренів степенів m і n . Справді, з умови $(m, n) = 1$ за наслідком з алгоритму Евкліда випливає, що існують цілі числа u, v , для яких $mu + nv = 1$. Тепер, якщо ξ — первісний корінь mn -го степеня з 1, то $\xi = \xi^{mu+nv} = (\xi^m)^n \cdot (\xi^n)^m$, де $\xi^{mu} \in C_n$, $\xi^{nv} \in C_m$, тобто первісний корінь mn -го степеня з 1 є добутком

коренів степенів m та n з одиниці, причому співмножники повинні бути первісними коренями, бо інакше добуток не був би первісним коренем.

Це означає, що при умові $(m, n) = 1$, первісних коренів степеня mn з одиниці буде стільки, скільки можна утворити добутків $\xi\eta$, де ξ — первісний корінь n -го степеня з 1, а η — первісний корінь m -го степеня з 1. Тому, використовуючи вже доведену властивість 2), одержимо

$$\phi(mn) = \phi(m)\phi(n).$$

4) Обчислимо $\phi(p^k)$, де p — просте число. Серед чисел $1, 2, \dots, p^k - 1$ лише $p^{k-1} - 1$ чисел, а саме, $p, 2p, \dots, p^k - p$ не є взаємно простими з p , а всі інші взаємно прості. Тому

$$\phi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Якщо $n = p_1^{k_1} \cdots p_s^{k_s}$ — розклад числа n на прості множники, то, використовуючи частину 3) теореми (мультиплікативність функції Ойлера), маємо

$$\begin{aligned} \phi(n) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_s^{k_s}) = p_1^{k_1} \cdots p_s^{k_s} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) = \\ &= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right). \end{aligned}$$

□

4.1.5. Теореми Ойлера та Ферма

Теорема 4.1.4 (Ойлер). Якщо $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, то $\bar{a}^{\phi(n)} = \bar{1}$.

Доведення. Порядок групи $(\mathbb{Z}/n\mathbb{Z})^*$ дорівнює $\phi(n)$. За наслідком із теореми Лагранжа порядок кожного елемента скінченної групи є дільником порядку всієї групи. Тому, якщо порядок елемента \bar{a} дорівнює d , то $\phi(n) = dc$, $d, c \in \mathbb{N}$. Отже, $\bar{a}^{\phi(n)} = \bar{a}^{dc} = \bar{1}^c = \bar{1}$. □

Наслідок 4.1.5 (Ферма). Якщо $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, де p — просте число, то $\bar{a}^{p-1} = \bar{1}$.

Доведення. $\phi(p) = p - 1$. Залишається застосувати теорему Ойлера. \square

Якщо a і b — цілі числа, n — додатне натуральне число, і $a - b$ ділиться на n , то за традицією пишуть

$$a \equiv b \pmod{n}.$$

З критерію рівності суміжних класів випливає, що у цих традиційних позначеннях теореми Ойлера та Ферма формулюються так:

Теорема Ойлера. Якщо $a \in \mathbb{Z}$, $(a, n) = 1$, то $a^{\phi(n)} \equiv 1 \pmod{n}$.

Теорема Ферма. Якщо p — просте число і p не є дільником a , то $a^{p-1} \equiv 1 \pmod{p}$.

Теореми Ойлера та Ферма мають широкі застосування, і не лише в математиці. На практиці доводиться обмінюватися шифрованою інформацією, використовуючи електронні засоби зв'язку, тому виникає потреба у пристосованих для цього шифрах. Для побудови деяких таких шифрів (див. 4.3.6) потрібно мати в своєму розпорядженні досить великі прості числа (зокрема такі, запис яких містить 100 і більше десяткових знаків). При пошуку простих чисел теорему Ферма можна розглядати як необхідну умову простоти числа: натуральне число n , для якого $a^{n-1} \not\equiv 1 \pmod{n}$, не є простим.

Нехай, наприклад, $n = 63$. 63 — не просте число, $63 = 3^2 \cdot 7$. Обчислимо $2^{62} = (2^6)^{10} \cdot 2^2 = 64^{10} \cdot 2^2 \equiv 2^2 \pmod{63}$. Для простого числа p ми повинні мати $a^{p-1} \equiv 1 \pmod{p}$.

Звичайно, для числа 63 немає потреби перевіряти його на простоту за допомогою теореми Ферма. Але якщо розглядати великі числа, то теорема Ферма стає справді корисною.

Варто зазначити, що з умов $(a, n) = 1$ і $a^{n-1} \equiv 1 \pmod{n}$ не обов'язково випливає, що n просте число. Наприклад, $(4, 15) = 1$ і $4^{14} = 2^{28} = (2^4)^7 \equiv 1 \pmod{15}$, але 15 не просте число.

4.1.6. Теорема Вільсона

Теорема 4.1.6 (Вільсон). p — просте число тоді й лише тоді, коли $(p-1)! \equiv -1 \pmod{p}$.

Доведення. Нехай p — просте число. Розглянемо поліном $X^{p-1} - \bar{1}$ з коефіцієнтами з поля $\mathbb{Z}/p\mathbb{Z}$. Підставивши у цей поліном будь-який ненульовий елемент $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ і врахувавши теорему Ферма, бачимо, що всі ненульові елементи $\bar{1}, \bar{2}, \dots, \bar{p-1}$ поля $\mathbb{Z}/p\mathbb{Z}$ є його коренями. Тому за теоремою Безу всі поліноми $X - \bar{1}, X - \bar{2}, \dots, X - \bar{p-1}$ є лінійними множниками полінома $X^{p-1} - \bar{1}$. Оскільки поліноми $X - \bar{1}, \dots, X - \bar{p-1}$ — попарно взаємно прості, то одержуємо рівність в кільці поліномів з коефіцієнтами в полі $\mathbb{Z}/p\mathbb{Z}$:

$$X^{p-1} - \bar{1} = (X - \bar{1})(X - \bar{2}) \dots (X - \bar{p-1}).$$

Порівнюючи вільні члени в обох частинах цієї рівності, одержуємо $\frac{(-1)^{p-1}(p-1)!}{(-1)} = \bar{1}$, тобто

$$(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}.$$

Якщо $p > 2$, то звідси одержимо

$$(p-1)! \equiv -1 \pmod{p},$$

що й вимагається.

Якщо ж $p = 2$, то умова теореми набуває вигляду $1 \equiv -1 \pmod{2}$ і, очевидно, виконується.

Навпаки, якщо p не просте, то $p = mn$, де $1 < m \leq p-1$, $1 < n \leq p-1$. Ясно, що $m|(p-1)!$. Якби $(p-1)! \equiv -1 \pmod{p}$, то звідси випливало б, що $m|1$. Отримана суперечність завершує доведення теореми. \square

4.1.7. Суми квадратів

Як приклад застосування теореми Вільсона розглянемо задачу про розклад даного натурального числа в суму квадратів двох інших натуральних чисел.

Теорема 4.1.7. Непарне просте число p можна записати у вигляді $p = m^2 + n^2$ для деяких натуральних чисел m і n тоді й лише тоді, коли $p \equiv 1 \pmod{4}$.

Доведення. (\Leftarrow) Починаємо з простого числа $p \equiv 1 \pmod{4}$. Тоді $p = 4k + 1$ для деякого натурального числа k . Якщо $a = 2k$, то

$$a! = (-1)(-2)(-3) \cdots (-2k) \equiv (p-1)(p-2) \cdots (p-2k) \pmod{p}.$$

Підставивши сюди $p = 4k + 1$ і переставивши множники $4k = p - 1, 4k - 1 = p - 2, \dots, 2k + 1 = p - 2k$ у зворотному порядку, одержимо

$$a! = (-1)(-2)(-3) \cdots (-2k) \equiv (2k+1)(2k+2) \cdots (4k) \pmod{p}.$$

Використовуючи теорему Вільсона, звідси випливає, що

$$\begin{aligned} (a!)^2 &= (-1)(-2)(-3) \cdots (-2k)(2k+1)(2k+2) \cdots (4k) = \\ &= (-1)^{2k}(p-1)! \equiv -1 \pmod{p}. \end{aligned}$$

Тепер, позначивши $a! = t$, бачимо, що існує натуральне t таке, що $t^2 + 1 \equiv 0 \pmod{p}$, тобто

$$t^2 + 1 = pb \tag{4.1.2}$$

для деякого $b \in \mathbb{N}$.

В кільці $\mathbb{Z}[i]$ цілих гаусових чисел рівність (4.1.2) можна записати у вигляді

$$(t+i)(t-i) = pb.$$

Якщо просте число p залишається простим у кільці $\mathbb{Z}[i]$, то використовуючи факторіальність кільця $\mathbb{Z}[i]$ (в п. 3.2.2 було показано, що $\mathbb{Z}[i]$ евклідове кільце, а евклідові кільця факторіальні), одержуємо, що $p|t+i$ або $p|t-i$. Нехай, наприклад, $p|t+i$. Тоді $t+i = p(k+li)$, $k, l \in \mathbb{Z}$. Звідси $pl = 1$. Приходимо до суперечності. Тому p не є дільником $t+i$ і так само p не є дільником $t-i$.

Отже, p не є простим елементом в кільці $\mathbb{Z}[i]$, а розкладається на множники:

$$p = (c + di)(e + fi), \quad c, e, d, f \in \mathbb{Z}, \quad c^2 + d^2 \neq 1, \quad e^2 + f^2 \neq 1. \quad (4.1.3)$$

Переходячи в (4.1.3) до спряжених комплексних чисел, одержимо

$$p = (c - di)(e - fi). \quad (4.1.4)$$

Перемножимо почленно (4.1.3) і (4.1.4):

$$p^2 = (c^2 + d^2)(e^2 + f^2).$$

Ця рівність можлива лише тоді, коли $p = c^2 + d^2$, і достатня умова теореми доведена.

Нехай $p \not\equiv 1 \pmod{4}$. Тоді $p \equiv 3 \pmod{4}$ і $p = 4k + 3$. Якби $p = c^2 + d^2$ для натуральних c і d , то, тим більше,

$$p \equiv c^2 + d^2 \pmod{4}. \quad (4.1.5)$$

Але

c^2	\equiv	$\begin{cases} 0 \pmod{4}, & \text{якщо } c = 2m, \\ 1 \pmod{4}, & \text{якщо } c = 2m + 1 \end{cases}$	i, аналогічно,
d^2	\equiv	$\begin{cases} 0 \pmod{4}, & \text{якщо } d \text{ парне,} \\ 1 \pmod{4}, & \text{якщо } d \text{ непарне.} \end{cases}$	

Тому $c^2 + d^2$ при діленні на 4 дає в остатці 0, 1 або 2, що суперечить (4.1.5), бо $p \equiv 3 \pmod{4}$. \square

Наслідок 4.1.8. Натуральне число n є сумою двох квадратів тоді й лише тоді, коли всі прості множини r_i вигляду $4m_i + 3$ входять у розклад n на прості множини з парними показниками.

Доведення. (\Leftarrow) Для доведення достатності досить зауважити, що коли два числа є сумами двох квадратів, то і їх добуток

є сумаю двох квадратів:

$$\begin{aligned} a = c^2 + d^2 &= (c + di)(e - di), \quad b = e^2 + f^2 = (e + fi)(e - fi), \\ ab &= (c + di)(e + fi)(c - di)(e - fi) = \\ &= (ce - df + (cf + de)i)(ce - df - (cf + de)i) = \\ &= (ce - df)^2 + (cf + de)^2. \end{aligned}$$

Крім цього, добуток суми двох квадратів на квадрат є сумаю двох квадратів

$$(c^2 + d^2)p^2 = (cp)^2 + (dp)^2.$$

Нехай просте число p входить в розклад $n = p_1^{k_1} \dots p_s^{k_s}$ з непарним показником і нехай $n = c^2 + d^2$. Розділивши, якщо потрібно, обидві частини рівності $n = c^2 + d^2$ на квадрат найбільшого спільного дільника c і d , можна вважати, що $(c, d) = 1$. Тепер, якщо $p|n$, то $c^2 + d^2 \equiv 0 \pmod{p}$, $cd \not\equiv 0 \pmod{p}$. Оскільки $c^{p-1} \equiv 1 \pmod{p}$ за теоремою Ферма, то $(c^{p-2}d)^2 = c^{2p-4}d^2 \equiv -c^{2p-2} = -(c^{p-1})^2 \equiv -1 \pmod{p}$. Отже, існує ціле число $t \in \mathbb{Z}$, таке що $t^2 \equiv -1 \pmod{p}$, $t^4 \equiv 1 \pmod{p}$, тобто t має порядок 4 у мультиплікативній групі поля $\mathbb{Z}/p\mathbb{Z}$. За наслідком з теореми Лагранжа число 4 є дільником числа $p - 1$ — порядку мультиплікативної групи поля $\mathbb{Z}/p\mathbb{Z}$. Тому $p - 1 = 4l$ і $p = 4l + 1$. \square

4.2. Конгруенції

4.2.1. Конгруенції та діофантові рівняння

Під *діофантовим рівнянням* розуміють рівняння

$$f(X_1, \dots, X_n) = 0, \tag{4.2.1}$$

де $f(X_1, \dots, X_n)$ — поліном з цілими коефіцієнтами. Розв'язати діофантове рівняння (4.2.1) означає знайти всі цілі (або раціональні) значення невідомих, що перетворюють його в правильну рівність. Діофантові рівняння складають один з найважливіших

розділів теорії чисел. Досить згадати про проблему Ферма, яка полягає, по-суті, у знаходженні розв'язків діофантових рівнянь

$$X^n + Y^n = Z^n.$$

Під *конгруенцією за $\mod m$* розуміють рівняння вигляду (4.2.1), де поліном $f(X_1, \dots, X_n)$ розглядається як поліном з коефіцієнтами кільця $\mathbb{Z}/m\mathbb{Z}$ (або з кільця цілих чисел \mathbb{Z} , якщо дімовитись розглядати цілі числа a , що є коефіцієнтами полінома $f(X_1, \dots, X_n)$ як елементи \bar{a} з кільця $\mathbb{Z}/m\mathbb{Z}$). Розв'язати конгруенцію — означає розв'язати відповідне рівняння в кільці $\mathbb{Z}/m\mathbb{Z}$, тобто знайти всі впорядковані послідовності $(\bar{c}_1, \dots, \bar{c}_n)$ з n елементів кільця $\mathbb{Z}/m\mathbb{Z}$, такі що $f(\bar{c}_1, \dots, \bar{c}_n) = \bar{0}$ в кільці $\mathbb{Z}/m\mathbb{Z}$.

Конгруенції за $\mod m$ прийнято записувати у вигляді

$$f(X_1, \dots, X_n) \equiv 0 \pmod{m}, \quad (4.2.2)$$

де $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$.

Повну множину розв'язків кожної конгруенції можна знайти за скінченну кількість кроків методом перебору. Щоб розв'язати конгруенцію (4.2.2), досить підставити кожну з m^n можливих послідовностей $(\bar{c}_1, \dots, \bar{c}_n)$, $\bar{c}_i \in \mathbb{Z}/m\mathbb{Z}$ у (4.2.2) і подивитися, одержується рівність чи ні. Звичайно, такий метод є найменш раціональним; у теорії чисел розроблені методи, які дозволяють розв'язувати широкі класи конгруенцій набагато швидше, ніж це дозволяє метод перебору.

Конгруенції бувають досить корисними при дослідженні діофантових рівнянь. Наприклад, розглянемо діофантове рівняння

$$5X^3 + 11Y^3 + 13Z^3 = 0. \quad (4.2.3)$$

Доведемо, що рівняння (4.2.3) не має інших розв'язків у цілих числах, крім розв'язку $(0, 0, 0)$. Якби це рівняння мало ненульовий ціличисельний розв'язок, то воно мало б і розв'язок (x, y, z) , у якому x, y і z попарно взаємно прості. Далі, якщо $(x, y, z) \in$

розв'язком рівняння (4.2.3) з попарно взаємно простими x, y і z , то (x, y, z) — ненульовий розв'язок конгруенції

$$5X^3 + 11Y^3 + 13Z^3 \equiv 0 \pmod{m} \quad (4.2.4)$$

за довільним модулем m .

Спробуємо взяти у (4.2.4) $m = 13$. Одержано конгруенцію

$$5X^3 + 11Y^3 \equiv 0 \pmod{13}. \quad (4.2.5)$$

Будемо шукати розв'язки (x, y) конгруенції (4.2.5), для яких $xy \not\equiv 0 \pmod{13}$. Конгруенція (4.2.5) є однорідним рівнянням над полем $\mathbb{Z}/13\mathbb{Z}$. Позначивши $\frac{x}{y} = t$, одержимо $5t^3 \equiv -2 \pmod{13}$ або

$$t^3 \equiv -5^{-1} \cdot 2 \equiv -8 \cdot 2 \equiv -3 \pmod{13}. \quad (4.2.6)$$

Знайдемо тепер куби всіх ненульових елементів поля $\mathbb{Z}/13\mathbb{Z}$:

t	1	2	3	4	5	6	7	8	9	10	11	12
t^2	1	4	9	3	-1	-3	-3	-1	3	9	4	1
t^3	1	8	1	12	8	8	5	5	1	12	5	12

Бачимо, що $-3 = 10$ не є кубом в $\mathbb{Z}/13\mathbb{Z}$, тому конгруенція (4.2.6) неможлива. Отже, діофантове рівняння (4.2.3) не має ненульових розв'язків у цілих числах.

Зауваження 4.2.1. У загальному випадку, якщо діофантове рівняння $f(X_1, \dots, X_n) = 0$ має розв'язок, то для всіх натуральних чисел m конгруенції $f(X_1, \dots, X_n) \equiv 0 \pmod{m}$ мають розв'язок. Це дає нескінченну серію необхідних умов існування розв'язків діофантових рівнянь. У деяких випадках ці умови є й достатніми. Зокрема, якщо $f(X_1, \dots, X_n) = \sum_{i,j=1}^n a_{ij}X_iX_j$ — квадратична форма з цілими коефіцієнтами a_{ij} , то відома теорема Мінковського-Хассе (див., наприклад, книгу [[?], Розділ I]) стверджує, що рівняння $\sum_{i,j=1}^n a_{ij}X_iX_j = 0$ має ненульовий розв'язок у цілих числах тоді й лише тоді, коли конгруенції $\sum_{i,j=1}^n a_{ij}X_iX_j \equiv 0 \pmod{m}$ мають ненульові розв'язки для всіх

натуральних чисел m . Причому виявляється, що коли ці конгруенції мають ненульові розв'язки для всіх чисел m , які менші від деякого числа, яке може бути явно вказане і залежить від коефіцієнтів a_{ij} , то вони мають ненульові розв'язки і для всіх інших m . Тому задача існування ненульового розв'язку діофантового рівняння $\sum_{i,j=1}^n a_{ij}X_iX_j = 0$ зводиться до існування ненульових розв'язків скінченного числа конгруенцій вигляду $\sum_{i,j=1}^n a_{ij}X_iX_j \equiv 0 \pmod{m}$ і тому може бути розв'язана за скінченне число кроків (наприклад методом перебору, якщо ми не використовуємо ефективніших методів).

Зауважимо, що для кубічних форм твердження теореми Мінковського-Хассе невірне. Зельмер показав (Selmer E.S., The diophantine equation $aX^3 + by^3 + cz^3 = 0$, Acta Math. 85, no.3-4, 1951, 203-312), що діофантове рівняння $3X^3 + 4Y^3 + 5Z^3 = 0$ не має ненульових розв'язків у цілих числах, а конгруенції $3X^3 + 4y^3 + 5z^3 \equiv 0 \pmod{m}$ мають ненульові розв'язки для всіх натуральних чисел m .

У вправі 17 до цього розділу пропонується дослідити частковий випадок теореми Мінковського-Хассе для квадратичної форми від трьох змінних.

4.2.2. Рівняння над полем $\mathbb{Z}/p\mathbb{Z}$ (конгруенції за \pmod{p})

Позначимо, для скорочення записів, поле $\mathbb{Z}/p\mathbb{Z}$ через \mathbb{F}_p і суму $\sum_{x \in \mathbb{F}_p} x^m$ через $S(x^m)$. Домовимося вважати, що $x^0 = 1$ для всіх елементів поля \mathbb{F}_p , зокрема $0^0 = 1$. Вірний наступний результат.

Лема 4.2.1.

$$S(x^m) = \begin{cases} -1, & \text{якщо } m \geq 1 \text{ і } (p-1)|m, \\ 0, & \text{в іншому випадку.} \end{cases}$$

Доведення. Якщо $m = 0$, то кожний доданок суми $S(x^0)$ дорівнює 1, отже, $S(x^0) = p \cdot 1 = 0$.

Якщо $m \geq 1$ і $p-1|m$, то для кожного $x \in \mathbb{F}_p^*$ $x^m = x^{(p-1)d} = 1$ і $0^m = 0$. Тому $S(x^m) = p - 1 = -1$.

Нехай тепер $m \geq 1$ і $p - 1$ не ділить m . Використаємо той факт, що ненульові елементи поля \mathbb{F}_p утворюють циклічну групу відносно множення. Нехай a — твірний елемент цієї групи. Зрозуміло, що $a^m \neq 1$. Далі, коли x пробігає всі елементи поля \mathbb{F}_p , то й ax пробігає всі елементи поля \mathbb{F}_p , бо з рівності $ax_1 = ax_2$, $a \neq 0$ у кільці без дільників нуля випливає рівність $x_1 = x_2$. Звідси одержуємо

$$S(x^m) = \sum_{x \in \mathbb{F}_p} x^m = \sum_{x \in \mathbb{F}_p} (ax)^m = a^m \sum_{x \in \mathbb{F}_p} x^m = a^m S(x^m).$$

Отже, $(1 - a^m)S(x^m) = 0$, а тому $S(x^m) = 0$. \square

Теорема 4.2.1 (Варнінг, Шевалле). *Нехай $F_i(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$, $1 \leq i \leq k$, — многочлени від n змінних, такі що $\sum \deg F_i < n$, $V \subset \mathbb{F}_p^n$ — множина розв'язків системи рівнянь*

$$\begin{cases} F_1(X_1, \dots, X_n) = 0, \\ \dots \\ F_k(X_1, \dots, X_n) = 0 \end{cases} \quad (4.2.7)$$

над полем \mathbb{F}_p . Тоді $|V| \equiv 0 \pmod{p}$, де $|V|$ означає кількість елементів множини V .

Доведення. Теорема стверджує, що кількість розв'язків системи алгебраїчних рівнянь (4.2.7) над скінченним полем \mathbb{F}_p ділиться на p . Для доведення теореми розглянемо поліном

$$F(X_1, \dots, X_n) = \prod_{i=1}^k (1 - F_i^{p-1}(X_1, \dots, X_n)). \quad (4.2.8)$$

Нехай $\bar{a} = (a_1, \dots, a_n) \in \mathbb{F}_p^n$. Якщо $\bar{a} \in V$, то $F_i(a_1, \dots, a_n) = 0$ для всіх $1 \leq i \leq k$. Тому

$$F(a_1, \dots, a_n) = 1.$$

Якщо ж $F_i(a_1, \dots, a_n) \neq 0$ хоч для одного i , то $F_i^{p-1}(a_1, \dots, a_n) = 1$ за теоремою Ферма; тому з (4.2.8) одержуємо, що $F(a_1, \dots, a_n) = 0$.

Введемо наступне позначення: для полінома $G(X_1, \dots, X_n)$ з коефіцієнтами з поля \mathbb{F}_p через $S(G)$ позначимо суму $\sum_{(x_1, \dots, x_n) \in \mathbb{F}_p^n} G(x_1, \dots, x_n)$ і розглянемо суму

$$S(F) = \sum_{(x_1, \dots, x_n) \in \mathbb{F}_p^n} F(x_1, \dots, x_n)$$

для полінома F . За попередніми міркуваннями сума $S(F)$ є сумою стількох одиниць, скільки розв'язків має система (4.2.7), тому досить довести, що $S(F) = 0$ у полі \mathbb{F}_p . Це означатиме, що кількість елементів множини V є кратною p , що й стверджує теорема Варнінга-Шевалле.

Поліном F є сумою мономів $X_1^{m_1} \cdots X_n^{m_n}$. Доведемо, що $S(X_1^{m_1}, \dots, X_n^{m_n}) = 0$ у полі \mathbb{F}_p . Для цього зауважимо, що

$$S(X_1^{m_1} \cdots X_n^{m_n}) = S(X_1^{m_1}) \cdots S(X_n^{m_n}). \quad (4.2.9)$$

Далі, оскільки за умовою теореми $\sum \deg F_i < n$ для всіх i , то $\deg F < n(p-1)$, а тому $m_1 + \cdots + m_n < n(p-1)$. Звідси випливає, що принаймні один з показників m_1, \dots, m_n менший від $p-1$. Тоді, за лемою 4.2.1, хоч один з множників у правій частині (4.2.9) дорівнює 0 (у полі \mathbb{F}_p). Тому з рівності (4.2.9) одержуємо, що $S(X_1^{m_1} \cdots X_n^{m_n}) = 0$ для довільного одночлена $S(X_1^{m_1} \cdots X_n^{m_n})$ полінома F . Звідси випливає, що $S(F) = 0$. Отже, $|V| \equiv 0 \pmod{p}$. \square

Наслідок 4.2.2. Якщо $F(X_1, \dots, X_n) \in \mathbb{F}_p[X_1, \dots, X_n]$, $\deg F < n$, то кількість розв'язків рівняння $F(X_1, \dots, X_n) = 0$ над полем \mathbb{F}_p ділиться на p .

Доведення. Наслідок одержується з теореми при $k = 1$. \square

Наслідок 4.2.3. Якщо, в умовах теореми Варнінга-Шевалле, вільні члени поліномів F_i є нульовими, то система рівнянь (4.2.7) має ненульовий розв'язок.

Доведення. Якби множина V розв'язків системи (4.2.7) складалася лише з нульового розв'язку, то $|V| = 1 \not\equiv 0 \pmod{p}$, що суперечило б теоремі. \square

Наслідок 4.2.4. Якщо $F(X_1, \dots, X_n) \in \mathbb{F}_p[X_1, \dots, X_n]$ — однорідний поліном степеня $r < n$, то рівняння $F(X_1, \dots, X_n) = 0$ має ненульовий розв'язок.

Доведення випливає з попереднього наслідку.

Наслідок 4.2.5. Якщо $F(X_1, \dots, X_n) \in \mathbb{F}_p[X_1, \dots, X_n]$ — однорідний поліном від трьох і більше змінних над полем \mathbb{F}_p , то рівняння $F(X_1, \dots, X_n) = 0$ має нетривіальний розв'язок.

Зауваження 4.2.2. Всі результати цього п., починаючи з леми і закінчуючи наслідком 4.2.5, справедливі у випадку довільного скінченного поля \mathbb{F}_q , а не лише поля \mathbb{F}_p .

4.2.3. Конгруенції за модулем p^n

Нехай a — ціле число, m — натуральне число. Число a визначає єдиний клас лишків $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$, який для спрощення позначень домовимося позначати тою ж буквою a . Якщо $a, b \in \mathbb{Z}/m\mathbb{Z}$ і $b \in (\mathbb{Z}/m\mathbb{Z})^*$, тобто b — елемент групи одиниць кільця $\mathbb{Z}/m\mathbb{Z}$, то для елемента b існує обернений b^{-1} , $ab^{-1} \in \mathbb{Z}/m\mathbb{Z}$. Далі ми інколи будемо писати $\frac{a}{b}$ замість ab^{-1} .

Критерій рівності суміжних класів показує, що умови

$$a = b \text{ в кільці } \mathbb{Z}/m\mathbb{Z} \text{ та } a \cong b \pmod{m}$$

рівносильні. Тут a і b означають класи лишків у першій умові та цілі числа у другій.

Нехай $f(X)$ — поліном з цілими коефіцієнтами, a і b — цілі числа. Якщо $a \equiv b \pmod{m}$, то $f(a) \equiv f(b) \pmod{m}$. Зокрема, звідси випливає, що, за умови $a \equiv b \pmod{m}$, $f(a) \equiv 0 \pmod{m}$ тоді й лише тоді, коли $f(b) \equiv 0 \pmod{m}$.

Зауважимо, що коли $f(X) \in \mathbb{Z}[X]$ і $a \in \mathbb{Z}$, то поліном $f(X)$ можна записати у вигляді

$$f(X) = a + f'(a)(X - a) + h(X)(X - a)^2, \quad (4.2.10)$$

де $h(X) \in \mathbb{Z}[X]$. Справді, поділімо $f(X)$ з остачею на $(X - a)^2$. Нехай $h(X)$ — частка від ділення. Розділивши їй остачу $r(X)$ на $X - a$ з остачею, одержимо

$$f(X) = a + d(X - a) + h(X)(X - a)^2.$$

Тепер обчислимо похідну від обох частин цієї рівності для $X = a$. Одержано, що $d = f'(a)$, тобто рівність (4.2.10).

Зауважимо, що рівність (4.2.10) є частковим випадком повної формули Тейлора (див. вправу 7 розділу 3)

$$f(X) = a + f'(a)(X - a) + \frac{f''(a)}{2}(X - a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(X - a)^n.$$

Далі p означає просте число, $f(X)$ — поліном з цілими коефіцієнтами.

Покажемо, що з розв'язків конгруенції $f(X) \equiv 0 \pmod{p}$ можна, за деяких умов, одержувати розв'язки конгруенцій $f(X) \equiv 0 \pmod{p^n}$ для всіх натуральних n .

Теорема 4.2.6. *Нехай $f(X) \in \mathbb{Z}[X]$, $f'(X)$ — похідна полінома $f(X)$. Нехай $x_0 \in \mathbb{Z}$ таке, що $f(x_0) \equiv 0 \pmod{p}$ і $f'(x_0) \not\equiv 0 \pmod{p}$. Тоді існує послідовність цілих чисел $x_0, x_1, \dots, x_n, \dots$ така, що*

$$0 \leq x_n < p^{n+1}, \quad (4.2.11)$$

$$f(x_n) \equiv 0 \pmod{p^{n+1}}, \quad (4.2.12)$$

$$x_n \equiv x_{n-1} \pmod{p^n}. \quad (4.2.13)$$

Доведення. Побудуємо послідовність $x_0, x_1, \dots, x_n, \dots$ за допомогою рекурентної формули

$$x_n \equiv x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})} \pmod{p^{n+1}}, \quad (4.2.14)$$

де $\frac{f(x_{n-1})}{f'(x_{n-1})}$ означає яке-небудь ціле число – представник класу лишків $f(x_{n-1})f'(x_{n-1})^{-1} \in \mathbb{Z}/p^n\mathbb{Z}$ (ми незабаром переконаємося в тому, що $f'(x_{n-1})$ оборотний елемент кільця $\mathbb{Z}/p^n\mathbb{Z}$).

Для $n = 0$ перевірки потребує лише властивість (4.2.12), яка в цьому випадку вірна за умовами теореми. Нехай елементи x_0, x_1, \dots, x_{n-1} вже побудовані; знайдемо елемент x_n . Перш за все, оскільки $x_{n-1} \equiv x_{n-2} \equiv \dots \equiv x_1 \equiv x_0 \pmod{p}$ і $f'(x_0) \not\equiv 0 \pmod{p}$, то й $f'(x_{n-1}) \not\equiv 0 \pmod{p}$, а тому $f'(x_{n-1})$ та p^n взаємно прості. Згідно твердження 1 теореми 5.1.4 $f'(x_{n-1}) \in (\mathbb{Z}/\mathbb{Z})^*$. Запишемо рівність (4.2.10) для $a = x_{n-1}$:

$$f(X) = f(X_{n-1}) + f'(x_{n-1})(X - x_{n-1}) + h(X)(X - x_{n-1})^2.$$

Підставивши сюди x_n з формули (4.2.14) замість X , одержимо

$$f(x_n) \equiv \left(\frac{f(x_{n-1})}{f'(x_{n-1})} \right)^2 \equiv 0 \pmod{p^{2n}}.$$

Але, $n \geq 1$, тому $2n \geq n+1$. Отже,

$$f(x_n) \equiv \left(\frac{f(x_{n-1})}{f'(x_{n-1})} \right)^2 h(x_n) \equiv 0 \pmod{p^{n+1}},$$

бо $\frac{f(x_{n-1})}{f'(x_{n-1})} \equiv 0 \pmod{p^n}$ за припущенням індукції. Таким чином, x_n є розв'язком конгруенцій (4.2.12) і (4.2.13). Нарешті, x_n визначається умовою (4.2.14) за $\pmod{p^{n+1}}$, тому x_n можна вибрати так, щоб $0 \leq x_n < p^{n+1}$. \square

Наслідок 4.2.7. Якщо для цілих x_1^0, \dots, x_m^0 і полінома $F(X_1, \dots, X_n)$ з цілими коефіцієнтами для деякого i ($1 \leq i \leq m$) виконуються умови

$$\begin{aligned} F(x_1^0, \dots, x_m^0) &\equiv 0 \pmod{p}, \\ F'_{x_i}(X_1^0, \dots, x_m^0) &\not\equiv 0 \pmod{p}, \end{aligned}$$

де F'_{X_i} – часткова похідна полінома F за змінною X_i , то для кожного натурального n існує розв'язок конгруенції

$$F(X_1, \dots, X_m) \equiv 0 \pmod{p^n}.$$

Доведення. Досить позначити $X_i = X$, розглянути поліном

$$f(X) = F(x_1^0, \dots, x_{i-1}^0, X, x_{i+1}^0, \dots, x_m^0)$$

від однієї змінної X і застосувати попередню теорему. \square

Зауваження 4.2.3. Послідовності цілих чисел $x_0, x_1, \dots, x_n, \dots$ такі, що $0 \leq x_n < p^n$ і $x_n \equiv x_{n-1} \pmod{p^{n+1}}$ (а саме такі послідовності виникають у теоремі 4.2.6, при розв'язуванні конгруенцій за $\pmod{p^n}$, називають *циліми p -адичними числами*). Такі числа є важливим інструментом сучасної теорії чисел.

4.2.4. Конгруенції за модулем m

Нехай m — натуральне число. Розглянемо конгруенцію першого степеня

$$aX \equiv b \pmod{m}. \quad (4.2.15)$$

Теорема 4.2.8. Нехай d — найбільший спільний дільник чисел a і m . Конгруенція (4.2.15) має d розв'язків, якщо $d | b$ і не має розв'язків, якщо $d \nmid b$.

Доведення. Конгруенція (4.2.15) має єдиний розв'язок, якщо $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$, тобто якщо $(a, m) = 1$. Цим єдиним розв'язком є клас лишків з представником $a^{\phi(m)-1}b$, де ϕ — функція Ойлера. Конгруенція (4.2.15), очевидно, не має розв'язку, якщо $(a, m) = d > 1$ і d не є дільником b . У випадку $(a, m) = d > 1$ і $d \mid b$ конгруенція (4.2.15) має d розв'язків $x_0, x_0 + \frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}$ за модулем m , де $x_0 \pmod{\frac{m}{d}}$ — розв'язок конгруенції

$$\frac{a}{d}X \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \quad (4.2.16)$$

Існування та єдиність розв'язку $x_0 \pmod{\frac{m}{d}}$ випливає із взаємної простоти чисел $\frac{a}{d}$ та $\frac{m}{d}$. \square

Розв'язування конгруенцій за модулем m зводиться до розв'язування конгруенцій за кількома модулями, які є степенями простих чисел. Це робиться за допомогою наступної теореми, яку називають *китайською теоремою про остачі*.

Теорема 4.2.9. Якщо m_1, m_2, \dots, m_s — попарно взаємно прості числа, $m = m_1 \cdot m_2 \cdots m_s$ і a_1, a_2, \dots, a_s — будь-які цілі числа, то існує ціле число a , для якого $a \equiv a_i \pmod{m}$ для всіх $i = 1, \dots, s$.

Доведення. Розглянемо числа $m'_i = \frac{m}{m_i}$. З попарної взаємної простоти чисел m_1, m_2, \dots, m_s випливає, що $(m'_i, m_i) = 1$. Тому конгруенція $m'_i X \equiv 1 \pmod{m_i}$ має єдиний розв'язок. Позначивши цей розв'язок через m''_i , одержимо

$$m'_i m''_i \equiv 1 \pmod{m_i}. \quad (4.2.17)$$

З іншого боку, зрозуміло, що для $i \neq j$, $1 \leq j \leq s$,

$$m'_j m''_j \equiv 0 \pmod{m_i}. \quad (4.2.18)$$

Ціле число $a = m'_1 m''_1 a_1 + m'_2 m''_2 a_2 + \cdots + m'_s m''_s a_s$ задовольняє вимогам теореми. Справді,

$$a - a_i \equiv \sum_{j \neq i} m'_j m''_j a_j + (m'_i m''_i - 1)a_i \equiv 0 \pmod{m_i},$$

бо кожний доданок суми $\sum_{j \neq i} m'_j m''_j a_j$ конгруентний нулю за модулем m_i згідно (4.2.18), а доданок $(m'_i m''_i - 1)a_i$ конгруентний нулю за модулем m_i згідно (4.2.17). Значить $a - a_i$ ділиться на всі числа m_i , а тому воно ділиться і на добуток $m_1 \cdots m_s$ цих чисел, бо m_1, \dots, m_s попарно взаємно прості числа. \square

Нехай $m = p_1^{k_1} \cdots p_s^{k_s}$ — розклад числа m на прості множники. Розглянемо конгруенцію

$$f(X) \equiv 0 \pmod{m}, \quad (4.2.19)$$

де $f(X)$ поліном із цілими коефіцієнтами. Поряд з конгруенцією (4.2.19) розглянемо систему конгруенцій

$$\begin{cases} f(X) \equiv 0 \pmod{p_1^{k_1}}, \\ \dots \\ f(X) \equiv 0 \pmod{p_s^{k_s}}. \end{cases} \quad (4.2.20)$$

Зрозуміло, що кожний розв'язок конгруенції (4.2.19) є розв'язком системи (4.2.20). Навпаки, якщо $a_i \pmod{p_i^{k_i}}$ розв'язок i -ої конгруенції системи (4.2.20), то елемент $a \pmod{m}$, обчислений за допомогою китайської теореми про остачі (при обчисленні ми приймаємо $m_i = p_i^{k_i}$), є розв'язком конгруенції (4.2.19). Тому задача розв'язування конгруенцій за довільним модулем може бути зведена до задачі розв'язування конгруенцій за модулем, що є степенем простого числа. А задача знаходження розв'язків конгруенцій за $\pmod{p^n}$ зводиться при певних умовах, як було показано у п. 4.2.3, до розв'язування конгруенцій за простим модулем p .

4.2.5. Двочленні конгруенції за \pmod{p}

Згадаємо, що для кожного скінченного поля \mathbb{F}_q мультиплікативна група \mathbb{F}_q^* є циклічною. Зокрема, якщо p — просте число, то мультиплікативна група поля $\mathbb{Z}/p\mathbb{Z}$ циклічна. Будь-яку твірну g групи $(\mathbb{Z}/p\mathbb{Z})^*$ називають *первісним коренем за модулем p* . Ми вже знаємо, що кожні дві циклічні групи однакового порядку ізоморфні між собою. Тому група $(\mathbb{Z}/p\mathbb{Z})^*$ ізоморфна групі $\mathbb{Z}/(p-1)\mathbb{Z}$. Якщо ми маємо який-небудь первісний корінь g за \pmod{p} , то можемо задати ізоморфізм (позначимо його через ind_g):

$$\text{ind}_g: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{Z}/(p-1)\mathbb{Z},$$

де для $a \in (\mathbb{Z}/p\mathbb{Z})^*$ $\text{ind}_g(a) = \bar{i} \in \mathbb{Z}/(p-1)\mathbb{Z}$ тоді і тільки тоді, коли $a = g^i$.

Відображення ind_g біективне. Справді, воно сюр'ективне, бо для кожного елемента $\bar{i} \in \mathbb{Z}/(p-1)\mathbb{Z}$ ми можемо вказати його прообраз, а саме, елемент $g^i \in (\mathbb{Z}/p\mathbb{Z})^*$; якщо $\text{ind}_g(g^i) = \text{ind}_g(g^j)$, тобто $\bar{i} = \bar{j}$, то $j = d(p-1) + i$, звідки отримуємо $g^j = g^i(g^{p-1})^d = g^i$, а це означає, що відображення ind_g ін'ективне.

Перевіримо, що відображення ind_g є гомоморфізмом груп $(\mathbb{Z}/p\mathbb{Z})^*$ і $\mathbb{Z}/(p-1)\mathbb{Z}$:

$$\text{ind}_g(ab) = \text{ind}_g(a) + \text{ind}_g(b).$$

Справді, якщо $a = g^i$, $b = g^j$, то

$$\text{ind}_g(ab) = \text{ind}_g(g^i g^j) = \text{ind}_g(g^{i+j}) = \overline{i + j} = \bar{i} + \bar{j} = \text{ind}(a) + \text{ind}(b).$$

Так само просто доводиться рівність $\text{ind}_g(a^k) = k \text{ind}_g(a)$.

Зрозуміло, що тут маємо аналогію з логарифмами. Індекси так само корисні для проведення обчислень у полі $\mathbb{Z}/p\mathbb{Z}$, як звичайні логарифми корисні для проведення обчислень у полі дійсних чисел.

Дослідимо за допомогою індексів двочленну конгруенцію

$$X^m \equiv a \pmod{p}. \quad (4.2.21)$$

Припустимо, що ця конгруенція має деякий розв'язок x . Виберемо первісний корінь g за $\text{mod } p$. Нехай $\bar{\alpha} = \text{ind}_g a$, $\bar{\xi} = \text{ind}_g x$. Тоді маємо

$$g^{\xi m} \equiv g^\alpha \pmod{p}. \quad (4.2.22)$$

Звідси, за означенням індексу, $\xi m \equiv \alpha \pmod{p-1}$, тобто ξ є розв'язком конгруенції

$$mY \equiv \alpha \pmod{p-1}. \quad (4.2.23)$$

Навпаки, якщо ξ є розв'язком конгруенції (4.2.23), то для ξ вірна умова (4.2.22), а тому $x = g^\xi$ є розв'язком конгруенції (4.2.21).

Таким чином, дослідження двочленних конгруенцій за модулем p зводиться до дослідження лінійних конгруенцій за модулем $p-1$.

Нехай $d = (p-1, m)$ — найбільший спільний дільник $p-1$ і m . Застосовуючи теорему 4.2.9, одержуємо, що конгруенція (4.2.23) має d розв'язків, якщо $d|\alpha$, і не має розв'язків в іншому випадку. Будь-який розв'язок конгруенції (4.2.23) задовольняє (4.2.22), а, отже, і (4.2.21). В кінцевому рахунку, бачимо, що задача знаходження розв'язків конгруенції (4.2.21) рівносильна задачі знаходження розв'язків лінійної конгруенції (4.2.23). Це дозволяє сформулювати таку теорему.

Теорема 4.2.10. а) Нехай p — просте число, $m \in \mathbb{Z}$, $m > 0$ і $a \in \mathbb{Z}$, p не ділить a . Нехай $d = (p-1, m)$. Конгруенція

$$X^m \equiv a \pmod{p}. \quad (4.2.24)$$

або має d розв'язків, або не має жодного.

б) Ця конгруенція має розв'язки тоді й лише тоді, коли

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

Існує $\frac{p-1}{d}$ значень $a \in \mathbb{Z}/p\mathbb{Z}$, для яких конгруенція (4.2.24) має розв'язки.

Доведення. Твердження а) випливає з попередніх міркувань, що зводять розв'язування конгруенції (4.2.24) до розв'язування лінійної Твердження) випливає з попередніх міркувань, що зводять розв'язування конгруенції (4.2.24) до розв'язування лінійної конгруенції (4.2.23).

Залишається довести б). Якщо $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, g — первісний корінь за \pmod{p} , і $\alpha = \text{ind}_g(a)$, то $\alpha^{\frac{p-1}{d}} \equiv 0 \pmod{p-1}$, тобто $\alpha^{\frac{p-1}{d}} = (p-1)s$ для деякого цілого s . Звідси $\frac{\alpha}{d} = s$, тобто α ділиться на d і конгруенція (4.2.23) має розв'язки, тому і конгруенція (4.2.24) має розв'язки.

Навпаки, нехай $b \in (\mathbb{Z}/p\mathbb{Z})^*$ розв'язок конгруенції (4.2.24). Тоді $a^{\frac{p-1}{d}} \equiv b^{m \frac{p-1}{d}} = (b^{p-1})^{\frac{m}{d}} \equiv 1 \pmod{p}$.

Для завершення доведення досить зауважити, що конгруенція $X^{\frac{p-1}{d}} \equiv 1 \pmod{p}$ має рівно $\frac{p-1}{d}$ розв'язків $g^d, g^{2d}, \dots, g^{p-1-d}$, $g^{p-1} = 1$, де g — первісний корінь за \pmod{p} . \square

4.3. Квадратичний закон взаємності

4.3.1. Символ Лежандра

Розглянемо конгруенцію

$$X^2 \equiv a \pmod{p}, \quad (4.3.1)$$

де p означає непарне просте число, p не ділить a .

Введемо символ $(\frac{a}{p})$, який називають *символом Лежандра* і означають так:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо конгруенція (4.3.1) має розв'язок,} \\ -1, & \text{в іншому випадку.} \end{cases}$$

Означення символу Лежандра можна сформулювати і в інших термінах:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо } a \text{ — квадрат у полі } \mathbb{Z}/p\mathbb{Z}, \\ -1, & \text{в іншому випадку.} \end{cases}$$

Із теореми 4.2.10 випливає, що в полі $\mathbb{Z}/p\mathbb{Z}$ існує $\frac{p-1}{2}$ ненульових квадратів і стільки ж ненульових неквадратів.

Для дослідження властивостей символу Лежандра корисний наступний простий результат.

Теорема 4.3.1 (критерій Ойлера). $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Доведення. За теоремою Ферма $a^{p-1} - 1 = 0$ в полі $\mathbb{Z}/p\mathbb{Z}$. З іншого боку $a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$. Звідси $a^{\frac{p-1}{2}} = 1$ або $a^{\frac{p-1}{2}} = -1$. Теорема 4.2.10 стверджує, що $a^{\frac{p-1}{2}} = 1$ тоді й лише тоді, коли конгруенція (4.3.1) має розв'язок, а це означає, що $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ в полі $\mathbb{Z}/p\mathbb{Z}$. \square

4.3.2. Лема Гаусса

Розглянемо непарне просте число p . Мультиплікативна група $(\mathbb{Z}/p\mathbb{Z})^*$ поля $\mathbb{Z}/p\mathbb{Z}$ є об'єднанням множин $S = \{1, 2, \dots, \frac{p-1}{2}\}$ та $-S = \{-1, -2, \dots, -\frac{p-1}{2}\}$. Ці множини мають порожній перетин: $S \cap (-S) = \emptyset$.

Якщо $x \in S$ і $a \in (\mathbb{Z}/p\mathbb{Z})^*$, то ax можна записати у вигляді:

$$ax = e_x x_a, \quad (4.3.2)$$

де $e_x = \pm 1$ і $x_a \in S$.

Лема 4.3.1. $\left(\frac{a}{p}\right) = \prod_{x \in S} e_x$.

Доведення. Нехай $x, x' \in S$ і $x \neq x'$. Тоді $x_a \neq x'_a$, бо в протилежному випадку ми мали б $ax = -ax'$, тобто $x + x' = 0$, а це неможливо за вибором множини S . Звідси випливає, що відображення $x \rightarrow x_a$ є біективним відображенням множини S в себе. Перемноживши рівності (4.3.2) для всіх $x \in S$, одержимо

$$a^{\frac{p-1}{2}} \prod_{x \in S} x = \left(\prod_{x \in S} e_x \right) \cdot \prod_{x \in S} x_a = \left(\prod_{x \in S} e_x \right) \cdot \prod_{x \in S} x.$$

Звідси, скоротивши на $\prod_{x \in S} x$, одержуємо:

$$a^{\frac{p-1}{2}} = \prod_{x \in S} e_x.$$

Але $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$, тому $\left(\frac{a}{p}\right) = \prod_{x \in S} e_x$, що й потрібно було довести. \square

4.3.3. Властивості символу Лежандра

Теорема 4.3.2. 1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

2) $\left(\frac{1}{p}\right) = 1$;

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Доведення. 1) $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2) Очевидно, бо 1 завжди є квадратом.

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ за критерієм Ойлера.

Для доведення властивостей 1), 2), 3) ми застосували критерій Ойлера. Для доведення властивості 4) застосуємо лему Гауса.

З рівності (4.3.2) випливає при $a = 2$:

$e_x = 1$, якщо $2x \leq \frac{p-1}{2}$, тобто $x \leq \frac{p-1}{4}$;

$e_x = -1$, якщо $2x > \frac{p-1}{2}$, тобто $x > \frac{p-1}{4}$.

Тому за лемою Гауса $\left(\frac{2}{p}\right) = (-1)^{n(p)}$, де $n(p)$ — кількість таких цілих чисел x , що

$$\frac{p-1}{4} < x \leq \frac{p-1}{2}. \quad (4.3.3)$$

Число p може мати один з чотирьох виглядів: $p = 8k \pm 1$ або $p = 8k \pm 3$.

Якщо $p = 8k \pm 1$, то з (4.3.3) випливає, що $n(p) = 2k$, а якщо $p = 8k \pm 3$, то з цієї ж нерівності випливає, що $n(p) = 2k \pm 1$. Отже,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p = 8k \pm 1, \\ -1, & p = 8k \pm 3 \end{cases} = (-1)^{\frac{p^2-1}{8}},$$

бо $\frac{p^2-1}{8}$ є парним числом для $p = 8k \pm 1$ і непарним для $p = 8k \pm 3$. \square

4.3.4. Закон взаємності

Теорема 4.3.3. Якщо p і q — різні непарні прості числа, то $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Доведення. Нехай $p = 2n + 1$, $q = 2m + 1$. Застосуємо лему Гауса до $a = q$ та множини $S = \{1, 2, \dots, n = \frac{p-1}{2}\}$. Нехай $1 \leq x \leq n$, тоді $qx \equiv e_x x_q \pmod{p}$, де $x_q \in S$.

Далі, $e_x = -1$ тоді й лише тоді, коли $qx = py - x_q$. Звідси $py = qx + x_q$, тобто $y > 0$ і $y \leq \frac{qx+x_q}{p} \leq \frac{qn+n}{p} = \frac{(q+1)\frac{p-1}{2}}{p} < \frac{q+1}{2} = m + 1$. Це означає, що $e_x = -1$ тоді і тільки тоді, коли існує таке $y \in \{1, 2, \dots, \frac{q-1}{2} = m\}$, що

$$0 < py - qx = x_q \leq n. \quad (4.3.4)$$

Зауважимо, що для заданого x з властивістю $e_x = -1$ число y визначається однозначно.

Розглянемо множину $B_1 = \{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq m, 0 < py - qx \leq n\}$ і позначимо через k_1 кількість елементів

множини B_1 . З леми Гауса випливає, що

$$\left(\frac{q}{p}\right) = (-1)^{k_1}. \quad (4.3.5)$$

Аналогічно, розглянувши елемент $a = p$ та множину $S_1 = \{1, 2, \dots, m = \frac{q-1}{2}\}$, одержимо, що для $y \in S_1$ $e_y = -1$ тоді і тільки тоді, коли існує елемент $x \in \{1, 2, \dots, n = \frac{p-1}{2}\}$, для якого

$$0 < qx - py \leq m. \quad (4.3.6)$$

Розглянемо множину

$$B_2 = \{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq m, -m \leq py - qx < 0\}.$$

Якщо k_2 — кількість елементів множини B_2 , то з леми Гауса одержуємо

$$\left(\frac{p}{q}\right) = (-1)^{k_2}. \quad (4.3.7)$$

З нерівностей (4.3.4) і (4.3.6) випливає, що $B_1 \cap B_2 = \emptyset$, отже, множина

$$B = B_1 \cup B_2 = \{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq m, -m \leq py - qx \leq n\}$$

складається з $k_1 + k_2$ елементів.

Нехай $A = \{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq m\}$. Множина $C = A \setminus B$ розбивається на дві підмножини

$$C_1 = \{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq m, py - qx > n\},$$

$$C_2 = \{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq m, py - qx < -m\}.$$

Нехай l_1 — кількість елементів множини C_1 , а l_2 — кількість елементів множини C_2 . Доведемо, що $l_1 = l_2$. Для цього перевіримо, що правило $(x, y) \mapsto (n+1-x, m+1-y) = (x', y')$ задає біективне відображення f з множини C_1 на множину C_2 .

Якщо $(x, y) \in C_1$, то зрозуміло, що $(x', y') \in A$ і, крім цього (нагадаємо, що $p = 2n + 1, q = 2m + 1$),

$$\begin{aligned} py' - qx' &= (2n+1)(m+1-y) - (2m+1)(n+1-x) = \\ &= (2n+1)(m+1) - (2m+1)(n+1) - py + qx = n-m-py+qx < -m, \end{aligned}$$

тобто $(x', y') \in C_2$. Навпаки, якщо $(x', y') \in C_2$, то

$$\begin{aligned} py - qx &= (2n + 1)(m + 1 - y') - (2m + 1)(n + 1 - x') = \\ &= n - m - py' + qx' > n, \end{aligned}$$

тобто $(x, y) \in C_1$.

Так само перевіряємо, що правило $(x', y') \mapsto (n+1-x', m+1-y')$ задає відображення g з множини C_1 у множину C_2 . Нарешті, легко перевірити, що відображення f і g є взаємно оберненими. Таким чином, відображення $f: C_1 \rightarrow C_2$ біективне, а тому $l_1 = l_2$.

Множини B_1 , B_2 , C_1 і C_2 попарно не перетинаються, а їх об'єднання дає всю множину A , отже,

$$k_1 + k_2 + 2l_1 = nm = \frac{p-1}{2} \cdot \frac{q-1}{2}. \quad (4.3.8)$$

Перемноживши (4.3.5) і (4.3.7), і використавши (4.3.8), одержуємо

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{k_1+k_2} = (-1)^{k_1+k_2+2l_1} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

що й потрібно було довести. \square

Щойно доведену теорему, яка стверджує, що для довільних двох непарних простих чисел p і q вірна рівність $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$, називають *квадратичним законом взаємності*, а рівності $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ та $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ називають *доповненнями до квадратичного закону взаємності*. Сформулюємо квадратичний закон взаємності та його доповнення у зручному для обчислень вигляді:

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, якщо хоч одне з простих чисел p або q має вигляд $4k + 1$.
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, якщо обидва числа p і q мають вигляд $4k + 3$.

- $(\frac{-1}{p}) = \begin{cases} 1, & \text{якщо } p = 4k + 1, \\ -1, & \text{якщо } p = 4k + 3. \end{cases}$
- $(\frac{2}{p}) = \begin{cases} 1, & \text{якщо } p = 8k + 1 \text{ або } p = 8k + 7, \\ -1, & \text{якщо } p = 8k + 3 \text{ або } p = 8k + 5. \end{cases}$

Закон взаємності був відкритий Л.Ойлером у 1772 р. і опублікований без доведення у 1783 р. Лежандр у 1775 р. сформулював закон взаємності у трохи іншій, ніж Ойлер, формі і навів доведення, яке не було, однак, повним. Перше повне доведення квадратичного закону взаємності одержав К.Ф. Гаус у віці 19 років у 1796 році. Це доведення було опубліковане Гаусом разом із ще одним доведенням у 1801 році в його знаменитому трактаті "Disquisitiones arithmeticæ". Пізніше Гаус опублікував ще декілька різних доведень цього закону.

Відзначимо, що закон взаємності не є просто математичним кур'юзом. Це глибока теорема, яка має серйозні застосування. Приклади найбільш простих застосувань будуть наведені у наступному п. 4.3.5. Квадратичний закон взаємності та його різноманітні узагальнення (найбільш загальні закони взаємності були дослідженні І.Р. Шафаревичем вже в середині 20-го століття) складають один з найважливіших розділів теорії чисел.

4.3.5. Деякі застосування закону взаємності

a) *Обчислення символу Лежандра.*

Нехай нам потрібно вияснити, чи має розв'язок конгруенція

$$x^2 \equiv 488 \pmod{1997}.$$

1997 — просте число, $488 = 2^3 \cdot 61$. Обчислюємо символ Лежандра, використовуючи $1997 \equiv 5 \pmod{8}$. Маємо

$$\begin{aligned} \left(\frac{488}{1997}\right) &= \left(\frac{2}{1997}\right)^3 \left(\frac{61}{1997}\right) = -\left(\frac{61}{1997}\right) = -\left(\frac{1997}{61}\right) = \\ &= -\left(\frac{45}{61}\right) = -\left(\frac{3}{61}\right)^2 \cdot \left(\frac{5}{61}\right) = -\left(\frac{5}{61}\right) = -\left(\frac{61}{5}\right) = -\left(\frac{1}{5}\right) = -1. \end{aligned}$$

Тут використано конгруенції $1997 \equiv 45 \pmod{61}$, $61 \equiv 1 \pmod{4}$ і мультиплікативність символу Лежандра $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ для $a, b \in \mathbb{Z}$.

б) *Обчислення простих чисел, для яких дане число a є квадратичним лишком.*

Розглянемо рівність $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. Ця рівність стверджує, що число 2 є квадратичним лишком для тих простих чисел p , які належать до арифметичних прогресій $\{8k+1 \mid k \in \mathbb{N}\}$ або $\{8k+7 \mid k \in \mathbb{N}\}$, і є квадратичним нелишком для тих простих p , які належать до прогресій $\{8k+3 \mid k \in \mathbb{N}\}$ або $\{8k+5 \mid k \in \mathbb{N}\}$.

Розглянемо тепер таку задачу. Знайти всі прості числа p , для яких дане просте число q є квадратичним лишком. Для розв'язання цієї задачі, як і у випадку $q=2$, розглянемо арифметичні прогресії $\{4qk+r \mid k \in \mathbb{N}, 0 < r < 4q\}$.

Маємо для $p = 4qk + r$:

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{r}{q}\right)(-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}}, \\ \left(\frac{-q}{p}\right) &= \left(-\frac{1}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{r}{q}\right)(-1)^{\frac{r-1}{2} \cdot \frac{q+1}{2}}. \end{aligned}$$

Звідси бачимо, що для фіксованого простого числа q символи Лежандра $(\frac{q}{p})$ та $(\frac{-q}{p})$ залежать лише від остачі від ділення числа p на $4q$. Множина тих простих p , для яких $(\frac{q}{p})$ є квадратичним лишком, міститься в арифметичних прогресіях $4qk+r$, $0 < r < 4q$, для яких $(\frac{r}{q})(-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}} = 1$, а множина тих простих p , для яких $(\frac{-q}{p})$ є квадратичним лишком, міститься в арифметичних прогресіях $4qk+r$, $0 < r < 4q$, для яких $(\frac{r}{q})(-1)^{\frac{r-1}{2} \cdot \frac{q+1}{2}} = 1$.

Тепер розглянемо конкретний приклад. Знайдемо ті прості числа $p > 3$, для яких конгруенція $X^2 \equiv 3 \pmod{p}$ має розв'язки.

Нехай $p = 12k + r$, де $r = 1, 5, 7, 11$.

$$\left(\frac{3}{p}\right) = (-1)^{\frac{r-1}{2}} \left(\frac{r}{3}\right) = \begin{cases} 1, & \text{якщо } r = 1, 11, \\ -1, & \text{якщо } r = 5, 7. \end{cases} \quad (4.3.9)$$

Наша конгруенція має розв'язок для $p \equiv 1 \pmod{12}$ і $p \equiv 11 \pmod{12}$ і не має розв'язків, якщо $p \equiv 5 \pmod{12}$ і $p \equiv 7 \pmod{12}$.

Одержаній результат можна сформулювати так: прості множники цілих чисел вигляду $a^2 - 3$ належать арифметичним прогресіям $12k + 1$ і $12k + 11$, де $k \in \mathbb{N}$.

в) *Відшукання простих множників деяких чисел.*

Спочатку доведемо наступну теорему:

Теорема 4.3.4. *Нехай $n = ax_0^2 + by_0^2$, де $a, b, x_0, y_0 \in \mathbb{Z} \setminus \{0\}$, $(ax_0, by_0) = 1$ і p – непарний простий множник числа n . Тоді $\left(\frac{-ab}{p}\right) = 1$.*

Доведення. З умов, наведених у формулюванні теореми випливає, що конгруенція $X^2 \equiv -ab \pmod{p}$ має розв'язок. Справді, умова $ax_0^2 + by_0^2 \equiv 0 \pmod{p}$ означає, що $-abx_0^2 \equiv (by_0)^2 \pmod{p}$. Звідси одержуємо $(x_0^{-1}y_0b)^2 \equiv -ab \pmod{p}$, де x_0^{-1} – розв'язок конгруенції $x_0X \equiv 1 \pmod{p}$. Тому $\left(\frac{-ab}{p}\right) = 1$. \square

Наведемо один приклад застосування цієї теореми.

Розклади на прості множники число

$$11021 = 3 \cdot 11^2 + 2 \cdot 73^2. \quad (4.3.10)$$

За теоремою, якщо $p|11021$, то $\left(\frac{-6}{p}\right) = 1$, $\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right)$. Числа p , для яких 2 і 3 є квадратичними лишками за модулем p , лежать в арифметичних прогресіях з різницями 8 і 12. Для того, щоб одночасно розглядати ці арифметичні прогресії, розглянемо арифметичну прогресію $24k + r$, $0 < r < 24$.

Нас цікавить значення $\left(\frac{-6}{p}\right)$ для різних простих чисел p . Так як $\left(\frac{-6}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{3}{p}\right)$, то досить обчислити $\left(\frac{-2}{p}\right)$ і $\left(\frac{3}{p}\right)$. Обчислимо спочатку символ $\left(\frac{-2}{p}\right)$:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{якщо } p \equiv 1, 7, 17, 23 \pmod{24}, \\ -1, & \text{якщо } p \equiv 5, 11, 13, 19 \pmod{24}, \end{cases}$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1, 5, 13, 17 \pmod{24}, \\ -1, & p \equiv 7, 11, 19, 23 \pmod{24}. \end{cases}$$

Порівнюючи значення $\left(\frac{2}{p}\right)$ і $\left(\frac{-1}{p}\right)$ і використовуючи $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)$, одержуємо

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{якщо } p \equiv 1, 11, 17, 19 \pmod{24}, \\ -1, & \text{якщо } p \equiv 5, 7, 13, 23 \pmod{24}. \end{cases} \quad (4.3.11)$$

Тепер обчислимо $(\frac{3}{p})$. Використаємо (4.3.9):

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{якщо } p \equiv 1, 11, 13, 23 \pmod{24}, \\ -1, & \text{якщо } p \equiv 5, 7, 17, 19 \pmod{24}. \end{cases}$$

Звідси і з (4.3.11) одержуємо остаточно:

$$\left(\frac{-6}{p}\right) = \begin{cases} 1, & \text{якщо } p \equiv 1, 5, 7, 11 \pmod{24}, \\ -1, & \text{якщо } p \equiv 13, 17, 19, 23 \pmod{24}. \end{cases}$$

Повертаючись до нашого числа 11021, бачимо, що прості дільники $p \leq \sqrt{11021}$ містяться серед чисел: 5, 7, 11, 29, 31, 53, 59, 73, 79, 83, 97, 101, 103.

З (4.3.10) бачимо, що 5, 11, 73 не є дільниками цього числа. Далі, використовуючи безпосереднє ділення, одержуємо, що серед чисел 7, 29, 31, 53, 59, 73, 79, 83, 97, 101, 103 лише 103 ділить 11021 і $11021 = 103 \cdot 107$. Ми розкладали число 11021 на прості множники. Зауважимо, що існує 24 простих чисел, більших від 5, які не перевищують 103. Використовуючи результат доведеної вище теореми, нам потрібно було випробувати лише 11 з них. Тому час розв'язання задачі про розклад на прості множники цього числа скорочується більше, ніж у 2 рази в порівнянні з тим, якби ми пробували підряд ділити на всі прості числа, що не перевищують 103 (не враховуючи часу, затраченого на виділення арифметичних прогресій, яким належать прості множники цього числа).

Звичайно, для такого невеликого числа як 11021 наведений метод відшукання простих множників виглядає не дуже переконливо. Адже можна було б за допомогою безпосереднього ділення випробувати всі 24 прості числа 7, 11, 13, 17, ..., 103, тим більше, що на знаходження 11 простих чисел 7, 29, ..., 103 теж було затрачено час.

Цей метод стає справді корисним, коли його застовувати до великих чисел. Наприклад, якщо маємо число $36671021 = 2 \cdot 2251^2 + 3 \cdot 2221^2$ (це навіть не дуже велике число), то для знаходження його простого множника методом ділення підряд на послідовні прості числа, потрібно було б перевірити (якщо не повезе!) кожне з простих чисел, яке не перевищує числа $\lceil \sqrt{36671021} \rceil$, де $[a]$ означає цілу частину числа a . $\lceil \sqrt{36671021} \rceil = 6055$. Існує

приблизно 800 (більше ніж 780) простих чисел, не більших ніж 6055, і тільки приблизно половина з них конгруентні з 1, 5, 7, 11 за модулем 24. Таким чином, потрібно перевіряти лише приблизно 400 чисел, а не 800. Звичайно, для того, щоб виділити множину цих простих чисел, потрібно попередньо знаходити остачі від ділення на 24, але ясно, що трохи легше (принаймні вручну) розділити, наприклад, просте число 5879 на 24 з остаточею, ніж розділити з остаточею 36671021 на 5879.

Зауважимо, що проблема розкладу великих чисел на прості множники є важливою прикладною проблемою. Вміння швидко розкладати великі числа на прості множники відіграє важливу роль у теорії шифрування, зокрема в так званих шифрах з відкритим ключем.

4.3.6. Шифри з відкритим ключем

Нехай задана деяка множина об'єктів U_1, U_2, \dots (об'єктами тут можуть бути особи, уряди, банки і т.п.) і нехай пари цих об'єктів обмінюються між собою інформацією, яка повинна бути секретною для всіх інших об'єктів. Інакше кажучи, якщо U_1 адресує деяке шифроване повідомлення до U_2 , то зміст цього повідомлення повинен бути недоступним для U_3, U_4, \dots .

Порівняно недавно були побудовані методи шифрування інформації, які називають *шифрами з відкритим ключем*. Характерною рисою цих шифрів є те, що метод шифрування інформації публікується і є, таким чином, доступним для всіх. Але, навіть володіючи методом шифрування, сторонній особі надзвичайно важко розшифрувати зашифрований текст. Для побудови деяких таких шифрів використовують кільце $\mathbb{Z}/n\mathbb{Z}$. Розглянемо побудову одного із найвідоміших шифрів з відкритим ключем, а саме так званого *RSA*-шифру.

1. Кожний об'єкт U_i вибирає два великих простих числа p_i і q_i і два класи лішків $e_i, d_i \pmod{n_i}$, де $n_i = p_i \cdot q_i$. Числа e_i та d_i вибирають так, щоб $e_i d_i \equiv 1 \pmod{\phi(n_i)}$, де $\phi(n_i) = (p_i - 1)(q_i - 1)$, ϕ — функція Ойлера.

2. Числа e_i, n_i публікують у доступному для всіх довіднику.

3. Якщо U_i хоче передати U_j шифроване повідомлення M , яке є, наприклад, послідовністю нулів і одиниць, то він робить так. Розбиває свою послідовність на блоки довжини $\lceil \log_2 n_j \rceil$, замінюює послідовність нулів і одиниць кожного блоку числом m , розглядаючи послідовність, яку він замінює, як запис числа m у двійковій системі числення. Зрозуміло, що $0 \leq m < n_j$. Тоді U_i передає числа $b = m^{e_j} \pmod{n_j}$, беручи e_j і n_j з довідника.

4. Одержаніши шифроване повідомлення і маючи ключ розшифрування d_j , U_j розшифровує $b \pmod{n_j}$ за допомогою піднесення b до степеня d_j . Виявляється, що $b^{d_j} \equiv m \pmod{n_j}$, тобто U_j правильно розшифрував надісланий йому шифрований текст. Справді, якщо $(m, n_j) = 1$, то правильність відновлення початкового тексту гарантується теоремою Ойлера

$$b^{d_j} \equiv m^{e_j d_j} \equiv m^{\phi(n_j)k+1} \equiv m \pmod{n_j}. \quad (4.3.12)$$

Нескладне міркування показує, що властивість (4.3.12) залишається в силі, якщо навіть $(m, n_j) > 1$, тобто правильне дешифрування гарантоване завжди. Справді, нехай $n = pq$ є добутком різних простих чисел p і q , і $a \equiv 1 \pmod{\phi(n)}$. Тоді $a = (p-1)(q-1)k+1$ для деякого цілого числа k . Тому $m^a = m^{(p-1)(q-1)k} \cdot m \equiv m \pmod{p}$ за теоремою Ферма, якщо $p \nmid m$ (якщо $p|m$, то конгруенція $m^a \equiv m \pmod{p}$ очевидна). Так само доводимо, що $m^a \equiv m \pmod{q}$, а тому $m^a \equiv m \pmod{pq}$ за китайською теоремою про остатці.

Якщо хто-небудь захоче розшифрувати не адресоване йому секретне повідомлення, то він повинен знати ключ d_j . Задача знаходження ключа d_j за відомими e_j і n_j зводиться до задачі розкладу числа n_j на прості множники. Але відомо, що розклад на прості множники великих натуральних чисел, наприклад з 100-ма десятковими знаками, вимагає десятків років машинного часу для найдосконаліших комп'ютерів, а розклад на прості множники чисел з 200-ма знаками вимагав би (на час написання цього тексту) мільярдів років машинного часу.

З іншого боку, розроблені методи, які дозволяють для даного великого натурального числа легко встановити, чи є це натуральне число простим.

У зв'язку з шифрами з відкритим ключем в теорії чисел виникають дві природні задачі:

Задача 1. Як одержувати у великій кількості великі прості числа? Причому ці великі прості числа повинні бути досить “випадковими”, щоб U_i , знайшовши для себе два простих числа p_i і q_i , був впевненим, що інший U_j їх не знайде.

Задача 2. Як швидко розкладати великі числа на прості множники? Цю задачу повинен розв'язувати суперник, який хоче заволодіти секретною інформацією.

Для більш детального ознайомлення з теорією шифрування та методами проникнення в таємницю зашифрованої інформації ми рекомендуємо книгу [37].

Зауваження 4.3.1. Кільце класів лишків використовують не тільки для захисту інформації. Існує ще одна важлива технічна проблема передачі інформації з гарантією, що в процесі передачі вона не буде спотворена. Із цією метою створюють різноманітні коди, при побудові яких широко використовують поля $\mathbb{Z}/p\mathbb{Z}$ та більш загальні скінченні поля. Докладніше про це можна прочитати у книгах [6], [23].

4.4. Вправи

- 1) Сформулювати і довести ознаки подільності на 3, 9, 11, 13.
- 2) Нехай $(a, m) = 1$. Показати, що $a^{r_1} \equiv a^{r_2} \pmod{m}$ тоді і тільки тоді, коли $r_1 \equiv r_2 \pmod{\phi(m)}$.
- 3) Показати, що $2730|(n^{13} - n)$ для кожного натурального n .
(Вказівка: $n^{12} = n^{\phi(13)} = n^{2\phi(7)} = n^{3\phi(5)} = n^{6\phi(3)} = n^{12\phi(2)}$, $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$).
- 4) *Узагальнення теореми Ойлера.* Узагальненою функцією Ойлера $L(m)$ називається функція, визначена для всіх дода-

тних натуральних чисел m наступним способом: $L(1) = 1$, а для $m > 1$

$$L(m) = \text{H.C.K.}(p_1^{k_1-1}(p_1-1), p_2^{k_2-1}(p_2-1), \dots, p_s^{k_s-1}(p_s-1)),$$

де $m = p_1^{k_1}p_2^{k_2}\dots p_s^{k_s}$ — канонічний розклад числа m . Довести, що для кожного m і кожного цілого a , $(a, m) = 1$, справедливе твердження

$$a^{L(m)} \equiv 1 \pmod{m}.$$

- 5) Довести, що $\sum_{d|m} \phi(d) = m$.
- 6) *Функцією Мебіуса* називається функція μ , визначена для всіх додатних натуральних чисел m так: $\mu(m) =$

$$= \begin{cases} 1, & n = 1, \\ (-1)^s, & якщо m — добуток s різних простих чисел, \\ 0, & якщо m ділиться на квадрат, більший від 1. \end{cases}$$

Довести:

- a) $\mu(mn) = \mu(m)\mu(n)$, якщо $(m, n) = 1$.
- b) $\sum_{d|m} \mu(d) = 0$ для $m > 1$.
- 7) *Формули обернення Мебіуса.* Нехай f і g довільні функції з \mathbb{N} у довільну комутативну групу G і нехай функції f і g зв'язані умовою $f(n) = \prod_{d|n} g(d)$. Довести рівність $g(n) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}$. (Якщо групову операцію у G записуємо адитивно, то цю вправу можна переформулювати так: Показати, що з рівності $f(n) = \sum_{d|n} g(d)$ випливає рівність $g(n) = \sum_{d|n} \mu(\frac{n}{d})f(d)$).
- 8) Використати вправи 5 і 7 для доведення формули $\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_n})$.
- 9) Нехай p є непарним простим дільником числа $a^{2^n} + 1$, де $n \geq 1$. Показати, що $p \equiv 1 \pmod{2^{n+1}}$.

- 10) Нехай m — будь-яке непарне ціле число. Довести, що $1^m + 2^m + \dots + (m-1)^m \equiv 0 \pmod{m}$.
- 11) Нехай a і b додатні цілі числа і $a = 2^\alpha 5^\beta m$, де $(m, 10) = 1$. Довести, що десятковий розклад числа $\frac{b}{a}$ є періодичним дробом, причому довжина періоду ділить $\phi(m)$. Довести також, що коли не існує періоду довжини, меншої за $m-1$, то m просте число.
- 12) Знайти яку-небудь твірну g групи $(\mathbb{Z}/13\mathbb{Z})^*$. Виписати значення $\text{ind}_g a$ для всіх $a \in (\mathbb{Z}/13\mathbb{Z})^*$. Знайти всі твірні групи $(\mathbb{Z}/13\mathbb{Z})^*$.
- 13) Нехай $f(X)$ і $g(X)$ — поліноми з цілими коефіцієнтами, p — просте число. Довести, що конгруенції $f(X) \equiv 0 \pmod{p}$ і $f(X) - (X^p - X)g(X) \equiv 0 \pmod{p}$ рівносильні, тобто кожний розв'язок першої є розв'язком другої і навпаки. Вивести звідси, що алгебраїчна конгруенція з одним невідомим рівносильна алгебраїчній конгруенції, степінь якої менший, ніж p .
- 14) Довести, що кількість розв'язків алгебраїчної конгруенції степеня n за простим модулем p не перевищує $\min\{n, p\}$. Для порівняння знайдіть кількість розв'язків конгруенції $X^2 \equiv 1 \pmod{8}$.
- 15) Розв'язати конгруенцію $X^3 - 2X^2 - 30X + 41 \equiv 0 \pmod{125}$.
- 16) Нехай $f(X) \in \mathbb{Z}[X]$, $a \in \mathbb{Z}$, p — просте число і нехай $f(a) \equiv 0 \pmod{p^k}$. Довести, що:
- Якщо $p^{k+1} \nmid f(a)$, то в класі лишків $\bar{a} \in \mathbb{Z}/p^k\mathbb{Z}$ немає жодного числа, що є розв'язком конгруенції
- $$f(X) \equiv 0 \pmod{p^{k+1}}. \quad (4.4.1)$$
- Якщо $p^{k+1} \mid f(a)$, то всі числа з класу $\bar{a} \in \mathbb{Z}/p^k\mathbb{Z}$ є розв'язками конгруенції (4.4.1).

- 17) *Теорема Лежандра.* Довести, що квадратична форма $ax^2 + by^2 - cz^2 = 0$, де a, b, c — попарно взаємно прості і вільні від квадратів додатні натуральні числа (тобто жодне з них не ділиться на квадрат натурального числа) має ненульовий розв'язок в цілих числах тоді і тільки тоді, коли всі конгруенції $ax^2 + by^2 - cz^2 \equiv 0 \pmod{p}$, де p — просте число і $p|abc$, мають ненульовий розв'язок.

Вказівки:) Якщо, наприклад, $p|c$, то показати, що конгруенція $ax^2 + by^2 \equiv 0 \pmod{p}$ має ненульовий розв'язок (x_0, y_0) . Припустивши, наприклад, що $y_0 \not\equiv 0 \pmod{p}$, одержати

$$ax^2 + by^2 - cz^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Аналогічно, для кожного простого дільника числа abc знайти лінійні однорідні одночлени $L_p(x, y, z)$ і $M_p(x, y, z)$ такі, що

$$ax^2 + by^2 - cz^2 \equiv L_p(x, y, z)M_p(x, y, z) \pmod{p}.$$

- б) Використовуючи китайську теорему про остачі, довести, що існують лінійні однорідні поліноми $L(x, y, z)$ і $M(x, y, z)$ з цілими коефіцієнтами, для яких

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}.$$

- в) Довести, що існують дві різні трійки (x_1, y_1, z_1) та (x_2, y_2, z_2) за $\text{mod}(abc)$, для яких

$$L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}$$

$$\text{i } 0 \leq x_1, x_2 < \sqrt{bc}, 0 \leq y_1, y_2 < \sqrt{ac}, 0 \leq z_1, z_2 < \sqrt{ab}.$$

- г) Вивести звідси, що для $x_0 = x_1 - x_2, y_0 = y_1 - y_2, z_0 = z_1 - z_2$

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \text{ або } ax_0^2 + by_0^2 - cz_0^2 = abc.$$

- д) Якщо $ax_0^2 + by_0^2 - cz_0^2 = abc$, то $a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0^2) - c(z_0^2 + ab)^2 = 0$ і $z_0^2 + ab \neq 0$.
- 18) Нехай C — повна система лишків за простим модулем p , тобто система цілих чисел, взятих по одному з кожного класу лишків. Довести, що

$$\sum_{x \in C} \xi^{xy} = \begin{cases} p, & \text{якщо } y \equiv 0 \pmod{p}, \\ 0, & \text{якщо } y \not\equiv 0 \pmod{p}, \end{cases}$$

де ξ означає первісний корінь p -го степеня з 1.

- 19) Нехай $F(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$. Довести, використовуючи позначення та твердження вправи 18, що для числа N розв'язків конгруенції

$$F(X_1, \dots, X_n) \equiv 0 \pmod{p}$$

справедлива рівність

$$N = \frac{1}{p} \sum_{x, x_1, \dots, x_n \in C} \xi^{xF(x_1, \dots, x_n)}.$$

- 20) Використовуючи властивості символу Лежандра, довести, що конгруенція $(X^2 - 13)(X^2 - 17)(X^2 - 221) \equiv 0 \pmod{m}$ має розв'язок для кожного модуля m . Очевидно, рівняння $(X^2 - 13)(X^2 - 17)(X^2 - 221) = 0$ нерозв'язне в цілих числах.
- 21) Застосувавши формулу бінома Ньютона, довести за індукцією, що для непарного простого p

$$(1 + px)^{p^n} \equiv 1 + p^{n+1}x \pmod{p^{n+2}}.$$

Вивести звідси, що коли елемент r є первісним коренем за модулем p , то він є первісним коренем за модулем p^n (тобто його порядок дорівнює $\phi(p^n)$) тоді і тільки тоді, коли p^2 не ділить $r^{p-1} - 1$. В усіх випадках або r , або $r + p$ є первісним коренем за модулем p^n .

- 22) Нехай p — непарне просте число, $(a, p) = 1$. Показати, що конгруенція $aX^2 + bX + c \equiv 0 \pmod{p}$ має два розв'язки, один або жодного в залежності від того, чи $b^2 - 4ac$ квадратичним лишком, нулем або нелишком за модулем p .
- 23) Довести, що коли a є непарне число і $n > 2$, то конгруенція $x^2 \equiv a \pmod{2^n}$ має розв'язки тоді і тільки тоді, коли $a \equiv 1 \pmod{8}$. (*Вказівка:* застосувати індукцію за n , враховуючи, що коли x є розв'язком, то або x , або $x + 2^{n-1}$ є розв'язком конгруенції $y^2 \equiv a \pmod{2^{n+1}}$).
- 24) Якщо для простого числа $p > 2$ число $q = \frac{p-1}{2}$ також просте і $q \equiv 1 \pmod{4}$, то 2 є первісним коренем за модулем p .
- 25) Нехай a — ненульове ціле число. Довести, що коли p і q — непарні прості числа, що не ділять a , і $p \equiv q \pmod{4|a|}$, то $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. (*Вказівка:* записати $a = n^2b$, де b — вільне від квадратів і застосувати квадратичний закон взаємності.)
- 26) Нехай b — натуральне число, $b > 1$. $b = p_1p_2 \dots p_s$ — розклад b на прості множники. Для цілого числа a означають символ Якобі

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \dots \cdot \left(\frac{a}{p_s}\right).$$

Довести, що для символу Якобі виконуються рівності:

- a) $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$, якщо a і b непарні натуральні числа, більші від 1.
- б) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$, де $b \in \mathbb{N}$, $b = 2k + 1$.
- в) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$, де $b \in \mathbb{N}$, $b = 2k + 1$.

Розділ 5

Ланцюгові дроби та їх застосування

5.1. Ланцюгові дроби

5.1.1. Скінченні ланцюгові дроби

Розглянемо раціональне число $\frac{a}{b} \in \mathbb{Q}$. Можна вважати, що $b > 0$. Застосуємо до пари цілих чисел a і b алгоритм Евкліда для знаходження найбільшого спільного дільника:

$$\begin{aligned} a &= bd_0 + r_1, \\ b &= r_1d_1 + r_2, \\ r_1 &= r_2d_2 + r_3, \\ &\dots\dots\dots \\ r_{n-2} &= r_{n-1}d_{n-1} + r_n, \\ r_{n-1} &= r_nd_n. \end{aligned} \tag{5.1.1}$$

Тут r_n — остання ненульова остача. Зазначимо, що $r_n < r_{n-1}$, тому $d_n > 1$ для $n > 0$. Враховуючи першу рівність з (5.1.1), маємо

$$\frac{a}{b} = d_0 + \frac{r_1}{b} = d_0 + \frac{1}{\frac{r_1}{d_1}}.$$

Далі, $\frac{b}{r_1} = d_1 + \frac{r_2}{r_1}$ за другою рівністю з (5.1.1). Тому

$$\frac{a}{b} = d_0 + \frac{1}{d_1 + \frac{r_2}{r_1}} = d_0 + \frac{1}{d_1 + \frac{1}{\frac{r_1}{r_2}}} = d_0 + \frac{1}{d_1 + \frac{1}{d_2 + \frac{r_3}{r_2}}}.$$

Продовжуючи таким способом використовувати рівності з (5.1.1), одержимо для $\frac{a}{b}$ такий вираз:

$$\frac{a}{b} = d_0 + \frac{1}{d_1 + \frac{1}{d_2 + \frac{1}{d_3 + \dots + \frac{1}{d_n}}}}. \quad (5.1.2)$$

Означення 5.1.1. Нехай $d_0, d_1, \dots, d_n \in \mathbb{Z}$, $d_i > 0$, $1 \leq i \leq n$, $d_n > 1$, якщо $n > 0$. Вираз

$$d_0 + \frac{1}{d_1 + \frac{1}{d_2 + \dots + \frac{1}{d_n}}} \quad (5.1.3)$$

називають (звичайним) *скінченим ланцюговим дробом*. Для скорочення запису (та економії місця) ланцюговий дріб (5.1.3) будемо записувати у вигляді

$$[d_0, d_1, \dots, d_n]. \quad (5.1.4)$$

Цілі числа d_0, d_1, \dots, d_n називають *неповними частками* ланцюгового дробу (5.1.4).

Теорема 5.1.1. а) *Кожне раціональне число дорівнює деякому ланцюговому дробу.*

- б) Існує лише один скінчений ланцюговий дріб, що дорівнює даному раціональному числу.

Доведення. Твердження а) теореми вже доведено (див. формулу (5.1.2)). Залишається довести твердження б). Для цього припустимо, що існують два різних скінчених ланцюгових дроби, які дорівнюють раціональному числу $\frac{a}{b}$:

$$[a_0, a_1, \dots, a_n] = [a'_0, a'_1, \dots, a'_m] = \frac{a}{b}. \quad (5.1.5)$$

Будемо вважати, що $n \leq m$. Доведення проводимо індукцією за m . Якщо $m = 0$, то твердження теореми очевидне: $n = m = 0$ і $a_0 = a'_0 = \frac{a}{b}$. Нехай єдиність доведено для всіх ланцюгових дробів, що мають не більше ніж m неповних часток, де $m \geq 0$. Тепер, якщо ми маємо рівність (5.1.5), у яку входить $m + 1$ неповних часток, то легко зрозуміти, що $a_0 = a'_0 = [\frac{a}{b}]$ — ціла частина числа $\frac{a}{b}$. З рівності (5.1.5) випливає

$$[a_1, a_2, \dots, a_n] = [a'_1, a'_2, \dots, a'_m] = \left(\frac{a}{b} - a_0\right)^{-1}. \quad (5.1.6)$$

За припущенням індукції з (5.1.6) випливає, що $m = n$, $a_i = a'_i$, $1 \leq i \leq m$. \square

5.1.2. Підхідні дроби ланцюгового дробу

Означення 5.1.2. *Підхідними дробами* ланцюгового дробу $[d_0, d_1, \dots, d_n]$ називають ланцюгові дроби $[d_0, d_1, \dots, d_k]$, $0 \leq k \leq n$. Підхідний дріб $[d_0, d_1, \dots, d_k]$ позначають $\frac{P_k}{Q_k}$, де $P_k, Q_k \in \mathbb{Z}$, $Q_k > 0$.

Маємо

$$\frac{P_0}{Q_0} = \frac{d_0}{1}, \quad \frac{P_1}{Q_1} = d_0 + \frac{1}{d_1} = \frac{d_0 d_1 + 1}{d_1}, \dots, \frac{P_n}{Q_n} = [d_0, d_1, \dots, d_n].$$

Дослідимо найпростіші властивості підхідних дробів.

Теорема 5.1.2. а)

$$P_k = d_k P_{k-1} + P_{k-2}, \quad (5.1.7)$$

$$Q_k = d_k Q_{k-1} + Q_{k-2} \quad (5.1.8)$$

для всіх $k, 2 \leq k \leq n$.

б)

$$P_k Q_{k-1} - Q_k P_{k-1} = (-1)^{k-1} \quad (5.1.9)$$

зокрема, $(P_k, Q_k) = 1$ для всіх $k, 1 \leq k \leq n$. Інакше каєсучи, підхідні дроби $\frac{P_k}{Q_k}$ нескоротні.

в)

$$\left| \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} \right| = \frac{1}{Q_{k-1}} Q_k \quad (5.1.10)$$

г)

$$\frac{P_{2k}}{Q_{2k}} < \frac{P_{2k+2}}{Q_{2k+2}} \quad i \quad \frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}}, \quad (5.1.11)$$

тобто парні підхідні дроби утворюють строго зростаючу послідовність, а непарні — строго спадну послідовність. Коєсний парний підхідний дріб менший від коєсного непарного.

Доведення. (а) Застосуємо метод математичної індукції. Для $k = 2$ маємо

$$\begin{aligned} \frac{P_2}{Q_2} &= d_0 + \frac{1}{d_1 + \frac{1}{d_2}} = \frac{d_0 d_1 d_2 + d_0 + d_2}{d_1 d_2 + 1} = \\ &= \frac{d_2(d_0 d_1 + 1) + d_0}{d_2 d_1 + 1} = \frac{d_2 P_1 + P_0}{d_2 Q_1 + Q_0}, \end{aligned}$$

тобто рівності (5.1.6) і (5.1.7) вірні для $k = 2$.

Нехай тепер $k > 2$. Припустимо, що рівності (5.1.6) і (5.1.7) вірні для всіх менших значень k . З означення ланцюгового дробу

та підхідних дробів видно, що $\frac{P_k}{Q_k}$ одержується з $\frac{P_{k-1}}{Q_{k-1}}$ за допомогою заміни d_{k-1} , що входить у $\frac{P_{k-1}}{Q_{k-1}}$, на $d_{k-1} + \frac{1}{d_k}$. Отже, маємо

$$\begin{aligned}\frac{P_k}{Q_k} &= \frac{(d_k - 1 + \frac{1}{d_k})P_{k-2} + P_{k-3}}{(d_{k-1} + \frac{1}{d_k})Q_{k-2} + Q_{k-3}} = \\ &= \frac{d_k(d_{k-1}P_{k-2} + P_{k-3}) + P_{k-2}}{d_k(d_{k-1}Q_{k-2} + Q_{k-3}) + Q_{k-2}} = \frac{d_kP_{k-1} + P_{k-2}}{d_kQ_{k-1} + Q_{k-2}}.\end{aligned}$$

Це завершує доведення твердження (а).

б) Формулу (5.1.9) теж доводимо методом математичної індукції. Для $k = 1$ маємо

$$P_1Q_0 - Q_1P_0 = (d_0d_1 + 1) \cdot 1 - d_1d_0 = 1.$$

Важаючи тепер, що формула (5.1.9) вірна для всіх менших значень k , одержуємо, використовуючи вже доведені раніше формулі (5.1.7) і (5.1.8),

$$\begin{aligned}P_kQ_{k-1} - Q_kP_{k-1} &= \\ &= (d_kP_{k-1} + P_{k-2})Q_{k-1} - (d_kQ_k - 1 + Q_{k-2})P_{k-1} = \\ &= d_k(P_{k-1}Q_{k-1} - P_{k-2}Q_{k-1}) + (Q_{k-1}P_{k-2} - P_{k-1}Q_{k-2}) = \\ &= -(P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1}) = (-1)^{k-1}.\end{aligned}$$

Твердження про найбільший спільний дільник P_k і Q_k , очевидно, одержується з формули (5.1.9)

в) Формула (5.1.10) випливає з уже доведеної формули (5.1.9):

$$\left| \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} \right| = \left| \frac{P_kQ_{k-1} - Q_kP_{k-1}}{Q_kQ_{k-1}} \right| = \frac{1}{Q_kQ_{k-1}}.$$

(г) Розглянемо різницю

$$\begin{aligned}\frac{P_n}{Q_n} - \frac{P_{n-2}}{Q_{n-2}} &= \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} + \frac{P_{n-1}}{Q_{n-1}} - \frac{P_{n-2}}{Q_{n-2}} = \\ &= \frac{P_nQ_{n-1} - Q_nP_{n-1}}{Q_nQ_{n-1}} + \frac{P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}}{Q_{n-1}Q_{n-2}}.\end{aligned}$$

Використовуючи (5.1.9), звідси одержуємо

$$\frac{P_n}{Q_n} - \frac{P_{n-2}}{Q_{n-2}} = \frac{(-1)^{n-1}}{Q_n Q_{n-1}} + \frac{(-1)^{n-2}}{Q_{n-1} Q_{n-2}} = (-1)^n \frac{(Q_n - Q_{n-2})}{Q_{n-2} Q_{n-1} Q_n}.$$

Скориставшись тепер тим, що послідовність Q_0, Q_1, \dots є строго зростаючою, з останнього обчислення маємо

$$\frac{P_n}{Q_n} - \frac{P_{n-2}}{Q_{n-2}} = (-1)^n a,$$

де $a > 0$. З цієї рівності одержуємо, що $\frac{P_{2n}}{Q_{2n}} - \frac{P_{2n-2}}{Q_{2n-2}} > 0$, а $\frac{P_{2n+1}}{Q_{2n+1}} - \frac{P_{2n-1}}{Q_{2n-1}} < 0$. Залишається показати, що кожний непарний підхідний дріб більший від кожного парного. Ми вже довели, що послідовність парних підхідних дробів є строго монотонно зростаючою, а послідовність непарних підхідних дробів є строго монотонно спадною. Використовуючи це, маємо у випадку $m \geq n$:

$$\begin{aligned} \frac{P_{2m+1}}{Q_{2m+1}} - \frac{P_{2n}}{Q_{2n}} &= \left(\frac{P_{2m+1}}{Q_{2m+1}} - \frac{P_{2m}}{Q_{2m}} \right) + \left(\frac{P_{2m}}{Q_{2m}} - \frac{P_{2n}}{Q_{2n}} \right) = \\ &= \frac{1}{Q_{2m+1} Q_{2m}} + \left(\frac{P_{2m}}{Q_{2m}} - \frac{P_{2n}}{Q_{2n}} \right) > 0. \end{aligned}$$

Якщо $m < n$, то маємо

$$\frac{P_{2m+1}}{Q_{2m+1}} - \frac{P_{2n}}{Q_{2n}} > \frac{P_{2n+1}}{Q_{2n+1}} - \frac{P_{2n}}{Q_{2n}} = \frac{1}{Q_{2n+1} Q_{2n}} > 0.$$

Це завершує доведення теореми. \square

Якщо доозначити $P_{-1} = 1$, $Q_{-1} = 0$, то формулами (5.1.7), (5.1.8) і (5.1.9) можна користуватися для всіх $k \geq 1$. Знаючи неповні частки d_0, d_1, \dots, d_n для раціонального числа $\frac{a}{b}$, обчислення підхідних дробів $\frac{P_i}{Q_i}$ зручно робити, по послідовно заповнюючи таку таблицю:

d_i		d_0	d_1	\dots	d_k	\dots	d_n
P_i	1	$P_0 = d_0$	$d_1 P_0 + 1$	\dots	$d_k P_{k-1} + P_{k-2}$	\dots	a
Q_i	0	$Q_0 = 1$	$d_1 Q_0 + 0$	\dots	$d_k Q_{k-1} + Q_{k-2}$	\dots	b

Розглянемо конкретний приклад. Нехай $\frac{a}{b} = -\frac{250}{117}$. Застосовуючи алгоритм Евкліда, як на початку цього параграфу, знаходимо неповні частки $-3, 1, 6, 3, 5$. Всі підхідні дроби одержуємо, заповнюючи таблицю:

d_i		-3	1	6	3	5
P_i	1	-3	-2	-15	-47	-250
Q_i	0	1	1	7	22	117

5.1.3. Означення нескінчених ланцюгових дробів

Повернемось ще раз до означення скінченного ланцюгового дробу. Для того, щоб записати раціональне число $\frac{a}{b}$ у вигляді ланцюгового дробу, нам потрібно знати всі неповні частки, які ми одержували за допомогою алгоритму Евкліда (5.1.1). З іншого боку, зрозуміло, що $d_0 = [\frac{a}{b}], d_1 = [\frac{b}{r_1}], d_2 = [\frac{r_1}{r_2}], \dots, d_n = [\frac{r_{n-1}}{r_n}]$, де $[\alpha]$ означає цілу частину числа α . Користуючись цим спостереженням, спробуємо означити ланцюговий дріб для довільного дійсного числа α , не обов'язково раціонального. Отже, нехай α — іrrаціональне число, $d_0 = [\alpha]$ — його ціла частина. Тоді $0 < \alpha - d_0 < 1$, і якщо $\alpha_1 = (\alpha - d_0)^{-1}$, то $d_1 = [\alpha_1]$. Далі, $\alpha_2 = (\alpha_1 - d_1)^{-1}, d_2 = [\alpha_2]$. І так далі, вважаючи числа $d_0, d_1, \dots, d_{n-1}, \alpha_1, \dots, \alpha_{n-1}$ вже визначеними, приймемо $\alpha_n = (\alpha_{n-1} - d_{n-1})^{-1}, d_n = [\alpha_n]$. Цей прийом дозволяє записати іrrаціональне дійсне число α у вигляді

$$\alpha = d_0 + \cfrac{1}{d_1 + \cfrac{1}{d_2 + \cfrac{1}{d_3 + \cdots + \cfrac{1}{d_n + \cfrac{1}{\alpha_{n+1}}}}}}, \quad (5.1.12)$$

де $\alpha_n - d_n = \frac{1}{\alpha_{n+1}}$. Цей процес не можна було б продовжити лише в одному випадку, коли б на n -му кроці ми одержали $\alpha_n = d_n$.

Але це неможливо, тому що в такому випадку ми одержали б

$$\alpha = [d_0, d_1, \dots, d_n],$$

тобто $\alpha \in \mathbb{Q}$, а це суперечить ірраціональності числа α . Як і у випадку скінчених ланцюгових дробів, цілі числа $d_0, d_1, \dots, d_n, \dots$ будемо називати *неповними частками* (зауважимо, що $d_0 \in \mathbb{Z}$, $d_i \in \mathbb{Z}$, $d_i > 0$ для $i \geq 1$). Числа $\alpha_0 = \alpha, \alpha_1, \alpha_2, \dots, \alpha_n, \dots$ називають *залишками* ланцюгового дробу для α . Ланцюговий дріб (5.1.12) скорочено записують у вигляді

$$\alpha = [d_0, d_1, \dots, d_n, \alpha_{n+1}], \quad (5.1.13)$$

де d_0, d_1, \dots, d_n — неповні частки, і α_{n+1} — залишок. Продовжуючи процес, за допомогою якого ми отримали (5.1.12), одержимо *нескінчений ланцюговий дріб*

$$d_0 + \cfrac{1}{d_1 + \cfrac{1}{d_2 + \cfrac{1}{d_3 + \cdots + \cfrac{1}{d_k}}}} + \dots, \quad (5.1.14)$$

або в скороченій формі запису

$$[d_0, d_1, \dots, d_n, \dots]. \quad (5.1.15)$$

Зауважимо, що застосувавши описану процедуру до раціонального числа $\frac{a}{b}$, одержимо запис цього раціонального числа у вигляді скінченного ланцюгового дробу: $\frac{a}{b} = [d_0, d_1, \dots, d_n]$.

Неповні частки ланцюгового дробу (5.1.14) ми визначили, виходячи із заданого дійсного числа α . Але можна почати з послідовності $d_0, d_1, \dots, d_n, \dots$, де $d_i \in \mathbb{Z}$, $d_i > 0$ для $i > 0$, і для цієї послідовності записати ланцюговий дріб (5.1.14).

Означення 5.1.3. Нехай $d_0, d_1, \dots, d_n, \dots$ — послідовність цілих чисел, причому $d_i > 0$ для $i > 1$. Назовемо цю послідовність

некінченним ланцюговим дробом, а числа d_i — його *неповними частками*. Нескінчений ланцюговий дріб записуємо у вигляді (5.1.15). Раціональні числа $d_0, [d_0, d_1], \dots,$

$$[d_0, d_1, \dots, d_n] = d_0 + \cfrac{1}{d_1 + \cfrac{1}{\dots + \cfrac{1}{d_n}}}$$

називають *підхідними дробами* нескінченного ланцюгового дробу (5.1.15). Як і у випадку скінчених ланцюгових дробів, для підхідних дробів використовують позначення $\frac{P_n}{Q_n} = [d_0, d_1, \dots, d_n]$.

Наша мета тепер — надати точного змісту виразам (5.1.14) і (5.1.15).

5.1.4. Підхідні дроби нескінченних ланцюгових дробів

Теорема 5.1.3. а) Для підхідних дробів нескінченного ланцюгового дробу вірні всі властивості, доведені в теоремі 5.1.2 для підхідних дробів скінчених ланцюгових дробів.

б) Послідовність підхідних дробів $\left\{\frac{P_n}{Q_n}\right\}_{n \in \mathbb{N}}$ збіжна. Якщо

$$\alpha = \lim_{n \rightarrow \infty} \frac{P_n}{Q_n}, \text{ то}$$

$$\frac{P_{2n}}{Q_{2n}} < \alpha < \frac{P_{2n+1}}{Q_{2n+1}}. \quad (5.1.16)$$

Доведення. Перше твердження теореми доводиться дослівним повторенням міркувань, наведених для доведення теореми про підхідні дроби скінчених ланцюгових дробів. Залишається довести твердження б). З твердження а) випливає, що ми маємо послідовність $\left[\frac{P_{2n}}{Q_{2n}}, \frac{P_{2n+1}}{Q_{2n+1}}\right]$ вкладених відрізків, довжини яких $\frac{P_{2n+1}}{Q_{2n+1}} - \frac{P_{2n}}{Q_{2n}} = \frac{1}{Q_{2n}Q_{2n+1}}$ прямують до нуля, бо знаменники Q_m

підхідних дробів утворюють строго зростаючу послідовність натуральних чисел. Використовуючи відому з аналізу теорему про вкладені відрізки, одержуємо, що існує

$$\lim_{n \rightarrow \infty} \frac{P_{2n}}{Q_{2n}} = \lim_{n \rightarrow \infty} \frac{P_{2n+1}}{Q_{2n+1}} = \lim_{n \rightarrow \infty} \frac{P_n}{Q_n} = \alpha.$$

Звідси, очевидно, випливає також, що

$$\frac{P_{2n}}{Q_{2n}} < \alpha < \frac{P_{2n+1}}{Q_{2n+1}}$$

для всіх $n \in \mathbb{N}$. □

Означення 5.1.4. Якщо дійсне число α є границею послідовності підхідних дробів ланцюгового дробу $[d_0, d_1, \dots, d_n, \dots]$, то кажуть, що α дорівнює ланцюговому дробу $[d_0, d_1, \dots, d_n, \dots]$ або α розкладається в ланцюговий дріб $[d_0, \dots, d_n, \dots]$, і записують

$$\alpha = [d_0, d_1, \dots, d_n, \dots]. \quad (5.1.17)$$

Зауважимо, що з рівності (5.1.16) випливає, зокрема,

$$d_0 < \alpha < d_0 + \frac{1}{d_1}, \quad (5.1.18)$$

де $d_1 \geq 1$, отже, $d_0 = [\alpha]$.

Нехай $\alpha_n = [d_n, d_{n+1}, \dots, d_{n+m}, \dots]$ — залишок ланцюгового дробу (5.1.17). Тоді за аналогією з (5.1.18) маємо $d_n < \alpha_n < d_n + \frac{1}{d_{n+1}}$, отже, $d_n = [\alpha_n]$.

Для доведення того, що різні нескінчені ланцюгові дроби збігаються до різних дійсних чисел, нам буде потрібний такий простий результат.

Лема 5.1.1. *Нехай $\alpha = [d_0, d_1, \dots, d_{n-1}, d_n, \dots]$ і $\alpha_n = [d_n, d_{n+1}, \dots]$ — залишок ланцюгового дробу для α . Тоді*

$$\alpha = \frac{P_{n-1}\alpha_n + P_{n-2}}{Q_{n-1}\alpha_n + Q_{n-2}}. \quad (5.1.19)$$

Доведення. Маємо $\alpha = [d_0, d_1, \dots, d_{n-1}, d_n, \dots] =$

$$= d_0 + \cfrac{1}{d_1 + \cdots + \cfrac{1}{d_{n-1} + \cfrac{1}{[d_n, d_{n+1}, \dots, d_{n+m}, \dots]}}}. \quad (5.1.20)$$

(Нагадаємо, що рівність $\alpha = [d_0, \dots, d_n, \dots]$ означає, що α є границею послідовності підхідних дробів.) Запишемо (5.1.20) у вигляді

$$\alpha = d_0 + \cfrac{1}{d_1 + \cdots + \cfrac{1}{d_{n-1} + \cfrac{1}{\alpha_n}}}. \quad (5.1.21)$$

Рівність (5.1.21) показує, що число α може бути одержане з підхідного дробу

$$\frac{P_{n-1}}{Q_{n-1}} = \frac{P_{n-2}d_{n-1} + P_{n-3}}{Q_{n-2}d_{n-1} + Q_{n-3}}$$

заміною d_{n-1} на $d_{n-1} + \frac{1}{\alpha_n}$. Отже,

$$\begin{aligned} \alpha &= \frac{P_{n-2}(d_{n-1} + \frac{1}{\alpha_n}) + P_{n-3}}{Q_{n-2}(d_{n-1} + \frac{1}{\alpha_n}) + Q_{n-3}} = \\ &= \frac{(P_{n-2}d_{n-1} + P_{n-3})\alpha_n + P_{n-2}}{(Q_{n-2}d_{n-1} + Q_{n-3})\alpha_n + Q_{n-2}} = \frac{P_{n-1}\alpha_n + P_{n-2}}{Q_{n-1}\alpha_n + Q_{n-2}}. \end{aligned}$$

Лему доведено. \square

Теорема 5.1.4. *Кожне дійсне число дорівнює лише одному ланцюговому дробу. Поставивши у відповідність кожному дійсному числу рівний йому ланцюговий дріб, одержуємо біективне відображення множини дійсних чисел на множину ланцюгових дробів.*

Доведення. За теоремою 5.1.1 можна обмежитися іrrаціональними числами і, відповідно, нескінченними ланцюговими дробами. Поставимо у відповідність дійсному числу $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ланцюговий дріб $[d_0, d_1, \dots, d_n, \dots]$, де $d_0 = [\alpha]$, $\alpha_1 = (\alpha - d_0)^{-1}$, $d_1 = [\alpha_1], \dots, \alpha_n = (\alpha_{n-1} - d_{n-1})^{-1}$, $d_n = [\alpha_n], \dots$, тобто так як в п.5.1.3. З теореми 5.1.3 випливає, що так одержаний дріб дорівнює даному дійсному числу α . Справді, відкинувши у формулі (5.1.21) $\frac{1}{\alpha_n}$, ми збільшуємо дріб

$$d_{n-2} + \frac{1}{d_{n-1} + \frac{1}{\alpha_n}},$$

отже, зменшуємо дріб

$$\begin{aligned} & d_{n-3} + \frac{1}{d_{n-2} + \frac{1}{d_{n-1} + \frac{1}{\alpha_n}}}, \\ & \vdots \end{aligned}$$

і т.д. В результаті ми зменшуємо вираз з правої частини (5.1.21) у випадку, коли n непарне, і збільшуємо цей вираз у випадку парного n . Це й означає, що

$$\frac{P_{2k}}{Q_{2k}} < \alpha < \frac{P_{2k+1}}{Q_{2k+1}},$$

тобто $\alpha = \lim \frac{P_n}{Q_n}$. Ми поставили у відповідність іrrаціональному дійсному числу α нескінчений ланцюговий дріб $[d_0, d_1, \dots, d_n, \dots]$, причому $\alpha = [d_0, d_1, \dots, d_n, \dots]$. Покажемо, що ця відповідність між іrrаціональними числами та рівними їм ланцюговими дробами задає відображення з $\mathbb{R} \setminus \mathbb{Q}$ у множину $\{[d_0, d_1, \dots] \mid d_i \in \mathbb{Z}, d_i > 0 \text{ для } i > 0\}$ нескінчених ланцюгових дробів. Для цього досить довести, що два ланцюгових дроби не можуть дорівнювати одному і тому ж числу. Міркуємо від супротивного. Нехай

$$\alpha = [d_0, d_1, \dots, d_{n-1}, d_n, \dots] = [d'_0, d'_1, \dots, d'_{n-1}, d'_n, \dots]. \quad (5.1.22)$$

Якщо ланцюгові дроби у (5.1.22) різні, то нехай n – перше значення індексу, для якого $d_n \neq d'_n$. Інакше кажучи, рівність (5.1.22) має вигляд $\alpha = [d_0, d_1, \dots, d_{n-1}, d_n, \dots] = [d_0, d_1, \dots, d_{n-1}, d'_n, \dots]$, причому $d_n \neq d'_n$. За лемою 5.1.1 звідси одержуємо

$$\alpha = \frac{P_{n-1}\alpha_n + P_{n-2}}{Q_{n-1}\alpha_n + Q_{n-2}} = \frac{P_{n-1}\alpha'_n + P_{n-2}}{Q_{n-1}\alpha'_n + Q_{n-2}}, \quad (5.1.23)$$

де $\alpha_n = [d_n, d_{n+1}, \dots]$, $\alpha'_n = [d'_n, d'_{n+1}, \dots]$. Перепишемо (5.1.23) у вигляді

$$\begin{aligned} & P_{n-1}Q_{n-1}\alpha_n\alpha'_n + P_{n-1}Q_{n-2}\alpha_n + P_{n-2}Q_{n-1}\alpha'_n + P_{n-2}Q_{n-2} = \\ & = P_{n-1}Q_{n-1}\alpha_n\alpha'_n + P_{n-2}Q_{n-1}\alpha_n + P_{n-1}Q_{n-2}\alpha'_n + P_{n-2}Q_{n-2}; \end{aligned}$$

звідси бачимо, що $(P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1})\alpha_n = (P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1})\alpha'_n$, і, використовуючи теорему 5.1.2 (6), одержуємо $\alpha_n = \alpha'_n$, тому і $d_n = [\alpha_n] = [\alpha'_n] = d'_n$, що суперечить нашому припущення. Отже, ми маємо відображення з множини $\mathbb{R} \setminus \mathbb{Q}$ на множину нескінчених ланцюгових дробів. Це відображення має обернене, яке нескінченному ланцюговому дробу ставить у відповідність границю послідовності його підхідних дробів. \square

Приклад 5.1.1. Розкладемо $\sqrt{7}$ в ланцюговий дріб. Маємо

$$d_0 = [\sqrt{7}] = 2,$$

$$d_1 = \left[\frac{1}{\sqrt{7}-2} \right] = \left[\frac{\sqrt{7}+2}{3} \right] = 1,$$

$$d_2 = \left[\frac{1}{\frac{\sqrt{7}+2}{3}-1} \right] = \left[\frac{3}{\sqrt{7}-1} \right] = \left[\frac{\sqrt{7}+1}{2} \right] = 1,$$

$$d_3 = \left[\frac{1}{\frac{\sqrt{7}+1}{2}-1} \right] = \left[\frac{2}{\sqrt{7}-1} \right] = \left[\frac{\sqrt{7}+1}{3} \right] = 1,$$

$$d_4 = \left[\frac{1}{\frac{\sqrt{7}+1}{3}-1} \right] = \left[\frac{3}{\sqrt{7}-2} \right] = [\sqrt{7}+2] = 4,$$

$$d_5 = \left[\frac{1}{\sqrt{7}-2} \right] = \left[\frac{\sqrt{7}+2}{3} \right] = 1$$

Порівнюючи залишки α_1 і α_5 , бачимо $\alpha_1 = \alpha_5 = \frac{\sqrt{7}+2}{3}$, тому наступні неповні частки будуть періодично повторюватися, тобто $d_n = d_{n+4}$ для всіх $n \geq 1$. Розклад $\sqrt{7}$ у нескінченній ланцюговий дріб має вигляд

$$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots].$$

Інакше кажучи, ланцюговий дріб для $\sqrt{7}$ періодичний. Зараз ми переконаємося у тому, що це не випадково.

5.1.5. Квадратичні іrrаціональноті та періодичні ланцюгові дроби

Означення 5.1.5. Дійсне число α називається *квадратичною іrrаціональністю*, якщо α — іrrаціональний корінь квадратного рівняння

$$aX^2 + bX + c = 0 \quad (5.1.24)$$

з цілими коефіцієнтами.

Зрозуміло, що коли корені рівняння (5.1.24) іrrаціональні, то $b^2 - 4ac$ не є квадратом раціонального числа. Коефіцієнти a, b, c рівняння (5.1.24) можна взяти взаємно простими; у цьому випадку дискримінант $b^2 - 4ac$ рівняння (5.1.24) будемо називати *дискримінантом* числа α . Згадуючи формулу для коренів квадратного рівняння, ми бачимо, що кожна дійсна квадратична іrrаціональність може бути записана у вигляді $\frac{P+\sqrt{D}}{Q}$ або $\frac{P-\sqrt{D}}{Q}$, де $P, Q, D \in \mathbb{Z}$, $D > 0$, $Q > 0$.

Приклад 5.1.2. $\alpha = \frac{1+\sqrt{17}}{3}$ — квадратична іrrаціональність, оскільки, α є коренем квадратного рівняння $9X^2 - 6X - 16 = 0$. У той же час $\sqrt[3]{7}$, наприклад, не є квадратичною іrrаціональністю, інакше ми мали б $\sqrt[3]{7} = \frac{P+\sqrt{D}}{Q}$. Підносячи останню рівність до куба, ми одержимо, що \sqrt{D} є раціональним числом, тобто D є квадратом раціонального числа. Це суперечить означення квадратичної іrrаціональності.

Означення 5.1.6. Нескінчений ланцюговий дріб $[d_0, d_1, \dots, d_n, \dots]$ називається *періодичним*, якщо існують числа $m, s \in \mathbb{N}$, такі що $d_n = d_m + s$ для всіх $n \geq m$. Число s називається *довжиною періоду*.

Введемо для періодичних ланцюгових дробів наступне позначення:

$$\begin{aligned} [d_0, d_1, \dots, d_m, d_{m+1}, \dots, d_{m+s-1}, d_m, d_{m+1}, \dots] &= \\ &= [d_0, \dots, d_{m-1}, \overline{d_m, \dots, d_{m+s-1}}]. \end{aligned}$$

Перший результат, який ми доведемо, — це критерій періодичності ланцюгового дробу.

Теорема 5.1.5. *Ланцюговий дріб $[d_0, d_1, \dots, d_n, \dots]$ є періодичним з довжиною періоду s тоді й лише тоді, коли для деякого m для залишків цього ланцюгового дробу вірна рівність $\alpha_m = \alpha_{m+s}$.*

Доведення. Нехай ланцюговий дріб

$$\alpha = [d_0, \dots, d_m - 1, \overline{d_m, \dots, d_{m+s-1}}]$$

періодичний. Тоді для залишків α_m і α_{m+s} , очевидно, маємо

$$\alpha_m = [\overline{d_m, \dots, d_{m+s-1}}] = \alpha_{m+s}.$$

Навпаки, якщо для деяких залишків α_m і α_{m+s} вірна рівність $\alpha_m = \alpha_{m+s}$, то, використовуючи теорему 5.1.4 про однозначність зображення дійсних чисел ланцюговими дробами, одержуємо

$$\begin{aligned} \alpha_m &= [d_m, d_{m+1}, \dots, d_{m+s-1}, d_{m+s}, \dots], \\ \alpha_{m+s} &= [d_{m+s}, d_{m+s+1}, \dots, d_{m+2s-1}, d_{m+2s}, \dots]. \end{aligned}$$

З рівності $\alpha_m = \alpha_{m+s}$ одержуємо $d_n = d_{n+s}$ для $m \leq n \leq m+s-1$, тому $\alpha_{m+s} = \alpha_{m+2s}$. Звідси, в свою чергу, одержимо $d_n = d_{n+s}$ для $m+s \leq n \leq m+2s-1$, і так далі. Отже, ланцюговий дріб для α є періодичним з довжиною періоду s . \square

Теорема 5.1.6. *Кожний нескінчений періодичний ланцюговий дріб $[d_0, \dots, d_n, \dots]$ дорівнює деякій квадратичній іrrаціональності.*

Доведення. Нехай $\alpha = [d_0, \dots, d_n, \dots]$. За теоремою 5.1.5 існують два різних залишки α_m і α_{m+s} ($s \geq 1$) дробу $[d_0, \dots, d_n, \dots]$, такі що $\alpha_m = \alpha_{m+s}$. Застосуємо до залишків α_m і α_{m+s} властивість (5.1.19):

$$\alpha = \frac{P_{m-1}\alpha_m + P_{m-2}}{Q_{m-1}\alpha_m + Q_{m-2}}, \quad \alpha = \frac{P_{m+s-1}\alpha_{m+s} + P_{m+s-2}}{Q_{m+s-1}\alpha_{m+s} + Q_{m+s-2}}$$

(тут $P_{-1} = 1$, $Q_{-1} = 0$, $P_{-2} = 0$, $Q_{-2} = 1$), і виразимо α_m і α_{m+s} через α :

$$\alpha_m = \frac{P_{m-2} - \alpha Q_{m-2}}{\alpha Q_{m-1} - P_{m-1}}, \quad \alpha_{m+s} = \frac{P_{m+s-2} - \alpha Q_{m+s-2}}{\alpha Q_{m+s-1} - P_{m+s-1}}.$$

Звідси одержуємо рівність

$$\frac{P_{m-2} - \alpha Q_{m-2}}{\alpha Q_{m-1} - P_{m-1}} = \frac{P_{m+s-2} - \alpha Q_{m+s-2}}{\alpha Q_{m+s-1} - P_{m+s-1}},$$

яка дає після зведення до спільного знаменника

$$A\alpha^2 + B\alpha + C = 0, \quad (5.1.25)$$

де $A = Q_{m-1}Q_{m+s-2} - Q_{m-2}Q_{m+s-1}$. Перевіримо, що $A \neq 0$. Якщо $m = 0$, то $A = Q_{-1}Q_{s-2} - Q_{-2}Q_{s-1} = -Q_{s-1} \neq 0$. Якщо $m = 1$, то $A = Q_0Q_{s-1} - Q_{-1}Q_s = Q_{s-1} \neq 0$. Якби $Q_{m-1}Q_{m+s-2} - Q_{m-2}Q_{m+s-1} = 0$ для $m > 1$, то

$$\frac{Q_{m-1}}{Q_{m-2}} = \frac{Q_{m+s-1}}{Q_{m+s-2}}. \quad (5.1.26)$$

Обидва дроби в рівності (5.1.26) є нескоротними, бо будь-які два сусідні члени послідовності $Q_0, Q_1, \dots, Q_n, \dots$ є взаємно прости ми числами за властивістю (5.1.9). З основної теореми арифметики (факторіальність кільця цілих чисел \mathbb{Z}) і з (5.1.26) одержуємо, що $Q_{m-1} = Q_{m+s-1}$ і $Q_{m-2} = Q_{m+s-2}$, що неможливо, бо в

послідовності

$$Q_0 \leq Q_1 < Q_2 < Q_3 \cdots < Q_n < \dots$$

може бути не більше однієї пари одинакових елементів. Одержанна суперечність показує, що в (5.1.25) $A \neq 0$. Тому α є коренем квадратного рівняння (5.1.25) з цілими коефіцієнтами. Якби число α було раціональним числом, то це суперечило б тому факту, що α дорівнює нескінченному ланцюговому дробові. \square

Трохи складніше доводиться обернена теорема про те, що кожна дійсна квадратична ірраціональність дорівнює нескінченному періодичному ланцюговому дробові. Якщо α — будь-яке алгебраїчне число (тобто корінь полінома з раціональними коефіцієнтами), то часто зручно розглядати мінімальний поліном $m(X)$ для числа α . За означенням, $m(X)$ є поліномом найменшого степеня з раціональними коефіцієнтами, що має коренем α , і старший коефіцієнт полінома $m(X)$ дорівнює 1. Легко зрозуміти, що мінімальний поліном однозначно визначається елементом α . Справді, якщо $m_1(X), m_2(X) \in \mathbb{Q}[X]$ — два мінімальні поліноми для α , то, розділивши $m_1(X)$ на $m_2(X)$ з остачею, одержимо

$$m_1(X) = m_2(X)d(X) + r(X).$$

Підставимо у цю рівність α замість X . Одержано $r(\alpha) = 0$. З мінімальності полінома $m_2(X)$ випливає $r(X) = 0$, а тому $m_2(X)|m_1(X)$. Так само доводимо, що $m_1(X)|m_2(X)$. Таким чином, $m_1(X) = am_2(X)$, де $a \in \mathbb{Q}$. Але старші коефіцієнти поліномів $m_1(X)$ і $m_2(X)$ дорівнюють 1, отже $a = 1$, і $m_1(X) = m_2(X)$.

Якщо α — квадратична ірраціональність, то мінімальний поліном для α має вигляд $X^2 + pX + q$, де $p, q \in \mathbb{Q}$. Домножимо поліном $X^2 + pX + q$ на найменший додатний спільний знаменник раціональних чисел p і q . Одержано поліном $AX^2 + BX + C \in \mathbb{Z}[X]$, $A > 0$, з цілими коефіцієнтами, з додатним старшим коефіцієнтом і такий, що найбільший спільний дільник коефіцієнтів A, B

і C дорівнює 1. Зрозуміло, що такий поліном елементом α визначається однозначно. Дискримінант цього полінома ми вже назвали раніше дискримінантом елемента α . Нехай $m, n, d \in \mathbb{Q}$, і $\alpha = m + n\sqrt{d}$ — квадратична іrrаціональність. Число $\alpha' = m - n\sqrt{d}$ називають *спряженим* до α .

Означення 5.1.7. Дійсна квадратична іrrаціональність β називається *редукованою*, якщо $\beta > 1$ і $-\frac{1}{\beta'} > 1$.

Лема 5.1.2. а) Якщо α_n — залишок дійсної квадратичної іrrаціональності α , то α_n — теж квадратична іrrаціональність, причому α і α_n мають однакові дискримінанти.

б) Починаючи з деякого значення n всі залишки α_n є редукованими.

Доведення. а) Нехай α — корінь квадратного рівняння $A_0x^2 + B_0x + C_0 = 0$ з цілими, взаємно простими коефіцієнтами. Доведемо індукцією за n , що залишок α_n квадратичної іrrаціональності α є коренем квадратного рівняння $A_nX^2 + B_nX + C_n = 0$ з цілими, взаємно простими коефіцієнтами і $B_n^2 - 4A_nC_n = B_0^2 - 4A_0C_0$. Для $n = 0$ маємо $\alpha_0 = \alpha$ і доводити нічого. Вважаючи, що твердження а) леми доведено для всіх залишків α_k , $k < n$, $n > 0$, доведемо його для залишку α_n . За припущенням індукції α_{n-1} є коренем квадратного рівняння

$$A_{n-1}X^2 + B_{n-1}X + C_{n-1} = 0 \quad (5.1.27)$$

і $B_{n-1}^2 - 4A_{n-1}C_{n-1} = B_0^2 - 4A_0C_0$. Підставимо $\alpha_{n-1} = d_{n-1} + \frac{1}{\alpha_n}$ у рівняння (5.1.27). Одержано рівність

$$A_{n-1}\left(d_{n-1} + \frac{1}{\alpha_n}\right)^2 + B_{n-1}\left(d_{n-1} + \frac{1}{\alpha_n}\right) + C_{n-1} = 0,$$

з якої після нескладних перетворень одержуємо, що α_n є коренем квадратного рівняння

$$A_nx^2 + B_nx + C_n = 0,$$

де $A_n = A_{n-1}d_{n-1}^2 + B_{n-1}d_{n-1} + C_{n-1}$, $B_n = 2A_{n-1}d_{n-1} + B_{n-1}$, $C_n = A_{n-1}$. Легко переконатися, що із взаємної простоти A_{n-1} , B_{n-1} , C_{n-1} випливає взаємна простота A_n , B_n і C_n . Покажемо, що дискримінант елемента α_n дорівнює дискримінанту елемента α .

$$\begin{aligned} B_n^2 - 4A_nC_n &= (2A_{n-1}d_{n-1} + B_{n-1})^2 - \\ &\quad - 4(A_{n-1}d_{n-1}^2 + B_{n-1}d_{n-1} + C_{n-1})A_{n-1} \\ &= 4A_{n-1}^2d_{n-1}^2 + 4A_{n-1}B_{n-1}d_{n-1} + B_{n-1}^2 - \\ &\quad - 4A_{n-1}^2d_{n-1}^2 - 4A_{n-1}B_{n-1}d_{n-1} - 4A_{n-1}C_{n-1} \\ &= B_{n-1}^2 - 4A_{n-1}C_{n-1} = B_0^2 - 4A_0C_0. \end{aligned}$$

6) Оскільки $\alpha_n = d_n + \frac{1}{\alpha_{n+1}}$, то $\alpha_n > 1$ для $n \geq 1$. Тому потрібно лише показати, що, починаючи з деякого n , вірна нерівність $\frac{1}{\alpha'_n} < -1$. За властивістю (5.1.19) для залишку α_{n+1} маємо:

$$\alpha = \frac{P_n\alpha_{n+1} + P_{n-1}}{Q_n\alpha_{n+1} + Q_{n-1}}.$$

Звідси одержуємо, що $\alpha_{n+1}(P_n - Q_n\alpha) = -(P_{n-1} - Q_{n-1}\alpha)$. Взявши спряжені до обох частин цієї рівності (пропонуємо самостійно переконатися у тому, що для $\alpha = a + b\sqrt{d}$ і $\beta = c + d\sqrt{d}$ вірні властивості $(\alpha + \beta)' = \alpha' + \beta'$ і $(\alpha\beta)' = \alpha'\beta'$), одержимо

$$\alpha'_{n+1}(P_n - Q_n\alpha') = -(P_{n-1} - Q_{n-1}\alpha').$$

Звідси маємо

$$\frac{1}{\alpha'_{n+1}} = -\frac{P_n - Q_n\alpha'}{P_{n-1} - Q_{n-1}\alpha'} = -\frac{P_nQ_{n-1} - Q_nQ_{n-1}\alpha'}{Q_{n-1}(P_{n-1} - Q_{n-1}\alpha')}.$$

За властивістю (5.1.9) підхідних дробів (згадаймо теорему 5.1.3) ми можемо підставити в чисельник останнього дробу $P_nQ_{n-1} =$

$= (-1)^{n-1} + Q_n P_{n-1}$. Одержано

$$\begin{aligned}\frac{1}{\alpha'_{n+1}} &= -\frac{(-1)^{n-1} + Q_n P_{n-1} - Q_n Q_{n-1} \alpha'}{Q_{n-1}(P_{n-1} - Q_{n-1} \alpha')} = \\ &= -\frac{1}{Q_{n-1}} \left[\frac{(-1)^{n-1}}{Q_{n-1} \left(\frac{P_{n-1}}{Q_{n-1}} - \alpha' \right)} + Q_n \right],\end{aligned}$$

а тому

$$\frac{1}{\alpha'_{n+1}} + 1 = -\frac{1}{Q_{n-1}} \left[\frac{(-1)^{n-1}}{Q_{n-1} \left(\frac{P_{n-1}}{Q_{n-1}} - \alpha' \right)} + (Q_n - Q_{n-1}) \right].$$

Перший доданок у квадратних дужках прямує до 0, коли $n \rightarrow \infty$, оскільки $\lim_{n \rightarrow \infty} \frac{P_{n-1}}{Q_{n-1}} = \alpha \neq \alpha'$ та $\lim_{n \rightarrow \infty} Q_{n-1} = \infty$. Тому для досить великих n вираз у квадратних дужках є додатним ($Q_n - Q_{n-1} > 0$ при $n > 1$). Таким чином, $\frac{1}{\alpha'_{n+1}} + 1 < 0$, тобто $\frac{1}{\alpha'_{n+1}} < -1$. \square

Лема 5.1.3. Існує лише скінчена кількість редукованих квадратичних ірраціональностей з даним дискримінантом d .

Доведення. Нехай β — редукована квадратична ірраціональність з дискримінантом d . Число β є одним з коренів полінома $Ax^2 - Bx - C$, де $A, B, C \in \mathbb{Z}$, $\text{НСД}(A, B, C) = 1$, $A > 0$. Нехай $d = B^2 + 4AC$. Тоді $\beta = \frac{B+\sqrt{d}}{2A}$ або $\beta = \frac{B-\sqrt{d}}{2A}$. Оскільки $-\frac{1}{\beta'} > 1$, то $0 < -\beta' < 1$, тому $\beta - \beta' > 0$ і $\beta + \beta' > 0$. Якщо $\beta = \frac{B-\sqrt{d}}{2A}$, то $\beta - \beta' = \frac{B-\sqrt{d}}{2A} - \frac{B+\sqrt{d}}{2A} < 0$. Одержано суперечність показує, що $\beta = \frac{B+\sqrt{d}}{2A}$. Далі, $\beta + \beta' = \frac{B+\sqrt{d}}{2A} + \frac{B-\sqrt{d}}{2A} = \frac{B}{A} > 0$. Тому $B > 0$ і $-\beta' = \frac{\sqrt{d}-B}{2A}$. Таким чином,

$$0 < B < \sqrt{d}. \quad (5.1.28)$$

Умова $\beta > 1$ означає $B + \sqrt{d} > 2A$. Звідси, враховуючи нерівність $B < \sqrt{d}$, одержуємо

$$0 < A < \sqrt{d}. \quad (5.1.29)$$

Оскільки β редукована квадратична ірраціональність, то $-\frac{1}{\beta} = -\frac{2A}{-B+\sqrt{d}} = \frac{B+\sqrt{d}}{2C} > 1$. З нерівності $\frac{B+\sqrt{d}}{2C} > 1$ випливає, враховуючи (5.1.28), що

$$0 < C < \sqrt{d}. \quad (5.1.30)$$

Нерівності (5.1.28)–(5.1.30) показують, що існує лише скінчена кількість квадратних тричленів $Ax^2 - Bx - C$, таких що $A, B, C \in \mathbb{Z}$, $\text{НСД}(A, B, C) = 1$, $A > 0$, і коренями яких є редуковані квадратичні ірраціональності з даним дискримінантом d . Тому існує лише скінчена кількість редукованих квадратичних ірраціональностей з даним дискримінантам d . \square

Теорема 5.1.7. а) *Кожна дійсна квадратична ірраціональність розкладається в періодичний ланцюговий дріб.*

б) *Якщо α редукована квадратична ірраціональність, то α розкладається в чисто періодичний ланцюговий дріб.*

Доведення. За лемою 5.1.2 залишки α_n квадратичної ірраціональності α стають редукованими при досить великих n і мають один і той же дискримінант. За лемою 5.1.3 існує лише скінчена кількість різних редукованих залишків α_n . Тому для деяких $n \geq 0$ і $s \geq 1$ ми повинні мати $\alpha_n = \alpha_{n+s}$, і твердження а) теореми випливає з теореми 5.1.5.

Якщо α редукована квадратична ірраціональність, то для всіх $n \geq 0$ і деякого $s \geq 1$ будемо мати $\alpha_n = \alpha_{n+s}$, тобто α розкладається в чисто періодичний ланцюговий дріб.

Справді, ми вже знаємо, що для деяких $n \geq 0$ і $s \geq 1$ справедлива рівність $\alpha_n = \alpha_{n+s}$. Перевіримо, що у випадку редукованої квадратичної ірраціональності звідси випливає $\alpha_{n-1} = \alpha_{n-1+s}$, якщо $n > 1$. Повторюючи це n разів, одержимо $\alpha_0 = \alpha_s$, а це означає, що α розкладається в чисто періодичний ланцюговий дріб.

Міркуючи за індукцією, припустимо, що α_{n-1} редукована ірраціональність. Тоді з рівності $\alpha_{n-1} = [\alpha_{n-1}] + \frac{1}{\alpha_n}$ одержуємо

$\alpha_n > 1$, і $i - \frac{1}{\alpha'_n} = [\alpha_{n-1}] + \left(-\frac{1}{\alpha'_{n-1}}\right)^{-1}$ (' означає, як і раніше, переход до спряженого числа). Звідси одержуємо, що $-\frac{1}{\alpha'_n} > 1$, тобто α_n редукована ірраціональність, і $\alpha_n - 1 = \left[-\frac{1}{\alpha'_n}\right] + \frac{1}{\alpha_n}$, тобто залишок $\alpha_n - 1$ однозначно визначається залишком α_n . Тому з $\alpha_n = \alpha_{n+s}$ випливає $\alpha_{n-1} = \alpha_{n-1+s}$. \square

5.2. Діофантові наближення

5.2.1. Порядок наближення дійсних чисел раціональними

Діофантові наближення складають багатий на глибоки результати розділ теорії чисел. Метою цього параграфу є знайомство з найпростішими класичними результатами про діофантові наближення. Одною з основних задач цього розділу теорії чисел є вивчення нерівностей

$$\left| \alpha - \frac{p}{q} \right| < c\phi(q), \quad (5.2.1)$$

де $\alpha \in \mathbb{R}$, $c \in \mathbb{R}$, $\phi(x)$ — дійсна функція від x , p, q — цілі числа, $q > 0$. Величина $\left| \alpha - \frac{p}{q} \right|$ — це похибка наближення дійсного числа α раціональним числом p/q . Основне питання, що постає у зв'язку з нерівністю (5.2.1) є таким: для заданих α , $\phi(x)$ і c знайти всі $p \in \mathbb{Z}$ і $q \in \mathbb{N}$, для яких вірна нерівність (5.2.1). Описання всіх розв'язків нерівності (5.2.1) є важкою задачею, тому ставлять легшу, але теж досить важку задачу: чи множина розв'язків нерівності (5.2.1) є скінченою чи нескінченою? На роль функції ϕ , як правило, беруть функцію $\phi(q) = \frac{1}{q^\nu}$, $\nu > 0$, і в цьому випадку мають справу з дослідженням нерівностей

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^\nu}. \quad (5.2.2)$$

Для заданих α, c, ν множина розв'язків нерівності (5.2.2), тобто множина пар $p \in \mathbb{Z}$, $q \in \mathbb{N}$, що задовольняють (5.2.2), відображає суттєві властивості числа α (наприклад, властивість α бути

раціональним чи ірраціональним, алгебраїчним чи трансцендентним). Крім того, за допомогою результатів про діофантові наближення, тобто результатів, звязаних із дослідженням нерівностей типу (5.2.2), вдається одержувати результати про розв'язки діофантових рівнянь від двох змінних

$$f(X, Y) = 0, \quad f(X, Y) \in \mathbb{Z}[X, Y],$$

в цілих числах. У кінці цього параграфа буде показано як це робиться. А тепер введемо основні означення.

Означення 5.2.1. Нехай $\nu > 0$. Кажуть, що дійсне число α *допускає наближення порядку v* рациональними числами, якщо існує константа c , залежна від α , для якої нерівність $|\alpha - \frac{p}{q}| < \frac{c}{q^v}$ має нескінченну кількість розв'язків у числах $p \in \mathbb{Z}$ і $q \in \mathbb{N}$.

Означення 5.2.2. Кажуть, що $v > 0$ є *найкращий порядок наближення* дійсного числа дійсного числа α рациональними числами, якщо α допускає наближення порядку v і існує константа $c_1 > 0$, яка залежить від α , для якої нерівність

$$\left| \alpha - \frac{p}{q} \right| < \frac{c_1}{q^v} \quad (5.2.3)$$

має лише скінченну кількість розв'язків в числах $p \in \mathbb{Z}$ і $q \in \mathbb{N}$.

Якщо v — найкращий порядок наближення дійсного числа α , то існує константа c_2 , для якої $|\alpha - \frac{p}{q}| \geq \frac{c_2}{q^v}$ для всіх $\frac{p}{q} \neq \alpha$. Справді, досить взяти

$$c_2 = \min \left\{ \left| \alpha - \frac{p_i}{q_i} \right| \mid \left| \alpha - \frac{p_i}{q_i} \right| < \frac{c_1}{q^v}, i = 1, \dots, N \right\},$$

де $\frac{p_1}{q_1}, \dots, \frac{p_N}{q_N}$ — скінченна множина розв'язків нерівності (5.2.3).

Приклад 5.2.1. $1.v = 1$ є *найкращим порядком наближення рациональних чисел рациональними числами*. Справді, нехай $\alpha \in \mathbb{Q}$. Тоді записавши число α у вигляді нескоротного дробу $\frac{a}{b}$ з додатним знаменником, одержуємо

$$\left| \frac{a}{b} - \frac{p}{q} \right| = \frac{|aq - bp|}{bq}.$$

Будемо шукати такі цілі числа p і q , щоб $aq - bp = \pm 1$. Для цього розкладемо $\alpha = \frac{a}{b}$ в ланцюговий дріб $\frac{a}{b} = \frac{P_n}{Q_n}$, де $\frac{P_n}{Q_n}$ — останній підхідний дріб. Тоді $q_0 = Q_{n-1}$, $p_0 = P_{n-1}$ є розв'язком в цілих числах одного із двох рівнянь

$$aq - bp = \pm 1.$$

Але з розв'язку (q_0, p_0) можна одержати нескінченну множину розв'язків $\{(q_0 + tb, p_0 + ta) \mid t \in \mathbb{Z}\}$. Тому рівняння $\left| \frac{a}{b} - \frac{p}{q} \right| = \frac{1}{bq}$ має нескінченну множину розв'язків $p \in \mathbb{Z}$, $q \in \mathbb{N}$, тим більше нерівність $\left| \frac{a}{b} - \frac{p}{q} \right| \leq \frac{2}{bq}$ з $c = \frac{2}{b}$ має нескінченну множину розв'язків, отже, раціональні числа допускають наближення порядку 1.

Виявляється, що 1 є найкращий порядок наближення раціональних чисел раціональними числами. Маємо для $\alpha = \frac{a}{b}$

$$\left| \frac{a}{b} - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq} \text{ для } \frac{a}{b} \neq \frac{p}{q}.$$

Тому нерівність $\left| \frac{a}{b} - \frac{p}{q} \right| \leq \frac{1}{2bq}$ з $c = \frac{1}{2b}$ не має раціональних розв'язків $\frac{p}{q}$, $\frac{p}{q} \neq \frac{a}{b}$.

2. Покажемо, що іrrаціональні числа мають порядок наближення (не обов'язково найкращий) 2. Нехай α іrrаціональне дійсне число. Розглянемо його послідовність підхідних дробів. Ця послідовність містить нескінченну кількість підхідних дробів. За нерівністю (5.1.16) з попереднього параграфа маємо

$$\left| \alpha - \frac{P_n}{Q_n} \right| < \left| \frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}} \right| = \frac{|P_n Q_{n+1} - Q_n P_{n+1}|}{Q_n Q_{n+1}} = \frac{1}{Q_n Q_{n+1}} < \frac{1}{Q_n^2}$$

(тут ми використали $P_{n+1}Q_n - P_nQ_{n+1} = (-1)^n$ і $Q_n < Q_{n+1}$). Тому існує нескінченна кількість дробів $\frac{p}{q}$, для яких вірна нерівність $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$. Це є означає, що іrrаціональні числа допускають раціональні наближення порядку 2. Пізніше ми побачимо, що $v = 2$ є найкращим порядком наближення для квадратичних іrrаціональностей.

3. Існують дійсні числа, що допускають наближення як завгодно великого порядку.

Нехай N — додатне дійсне число. Розглянемо нескінчений ланцюговий дріб

$$[a_0, a_1, a_2, \dots, a_k, \dots], \quad (5.2.4)$$

де $a_0 \in \mathbb{Z}$ — будь-яке, а інші елементи задовільняють рекурентне спiввiдношення

$$a_{k+1} > Q_k^{k-2}, \quad k = 0, 1, \dots$$

(тут Q_k — знаменники пiдхiдних дробiв ланцюгового дробу (5.2.4)). Якщо α — дійсне число, яке дорiвнює ланцюговому дробу (5.2.4), то, як i в попередньому прикладi,

$$\begin{aligned} \left| \alpha - \frac{P_n}{Q_n} \right| &< \frac{1}{Q_n Q_{n+1}} = \frac{1}{Q_n (Q_n a_{n+1} + Q_{n-1})} = \\ &= \frac{1}{Q_n^2 (a_{n+1} + \frac{Q_{n-1}}{Q_n})} < \frac{1}{Q_n^2 a_{n+1}} < \frac{1}{Q_n^2 Q_n^{n-2}} = \frac{1}{Q_n^n}. \end{aligned}$$

Звiдси випливає, що для всiх $k \geq n$ маємо $|\alpha - \frac{P_k}{Q_k}| < \frac{1}{Q_k^k} \leq \frac{1}{Q_k^n}$, тобто нерiвнiсть $|\alpha - \frac{p}{q}| < \frac{1}{q^n}$ має нескiнченну кiлькiсть розв'язкiв p, q . Пiзniше в п. 5.2.3 ми розглянемо ще один приклад дiйсних чисел, що допускають наближення як завгодно великого порядку.

5.2.2. Найкращi наближення та ланцюговi дроби

Нехай α — дiйсне число. Позначимо через $\|\alpha\|$ вiдстань вiд α до найближчого цiлого числа. Так $\|17/10\| = 0,3$, $\|\sqrt{3}\| = 2 - \sqrt{3}$, $\|\pi\| = \pi - 3$. Зауважимо, що, взагалi кажучи, $\|\alpha\|$ не дорiвнює дробовiй частинi $\{\alpha\}$ числа α (якщо $0 \leq \{\alpha\} \leq \frac{1}{2}$, то $\|\alpha\| = \{\alpha\}$, а якщо $\{\alpha\} > \frac{1}{2}$, то $\|\alpha\| = 1 - \{\alpha\}$).

Якщо цiлi числа p i q такi, що $|q\alpha - p| \leq \frac{1}{2}$, то $|q\alpha - p| = \|\alpha\|$.

Означення 5.2.3. Найкращим наближенням до числа α називається дріб p/q ($p, q \in \mathbb{Z}$, $q > 0$) для якого $\|q\alpha\| = |q\alpha - p|$ і $\|q'\alpha\| > \|q\alpha\|$ для всіх q' , $1 \leq q' < q$.

Найкраще наближення числа $\frac{p}{q}$ є необхідно нескоротним дробом. В іншому випадку ми мали б $p = p'd$, $q = q'd$, $d > 1$ і $|q'\alpha - p'| < d|q'\alpha - p'| = |q\alpha - p|$, а це суперечить тому, що $\frac{p}{q}$ – найкраще наближення числа α . Найкращі наближення дуже тісно пов’язані з ланцюговими дробами. Про це свідчить наступна теорема.

Теорема 5.2.1. Коjsne найкраще наближення дійсного числа α є підхідним дробом числа α . Навпаки, для $n \geq 1$ підхідні дроби $\frac{P_n}{Q_n}$ числа α є найкращими наближеннями α .

У доведенні цієї теореми буде використана наступна лема.

Лема 5.2.1. Якщо $\frac{P_n}{Q_n}$ – підхідний дріб для дійсного числа α , то

- a) $|Q_n\alpha - P_n| = \|Q_n\alpha\|$, якщо $n \geq 1$,
- b) $\|Q_n\alpha\| < \|Q_{n-1}\alpha\|$, якщо $n \geq 2$.

Доведення. а) Якщо $\alpha = \frac{P_n}{Q_n}$, то $\|Q_n\alpha\| = |Q_n\alpha - P_n| = 0$. Якщо ж $\alpha \neq \frac{P_n}{Q_n}$, то існує підхідний дріб $\frac{P_{n+1}}{Q_{n+1}}$, $Q_{n+1} \geq 2$. Тоді за теоремами 5.1.2 та 5.1.3 $\frac{P_n}{Q_n} < \alpha < \frac{P_{n+1}}{Q_{n+1}}$, якщо n парне, і $\frac{P_{n+1}}{Q_{n+1}} < \alpha < \frac{P_n}{Q_n}$, якщо n непарне, а тому

$$\left| \alpha - \frac{P_n}{Q_n} \right| < \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n Q_{n+1}} < \frac{1}{2Q_n},$$

отже, $|Q_n\alpha - P_n| < \frac{1}{2}$ і $\|Q_n\alpha\| = |Q_n\alpha - P_n|$.

б) Зауважимо, що $(\alpha - \frac{P_n}{Q_n})$ і $(\alpha - \frac{P_{n+1}}{Q_{n+1}})$ мають різні знаки, тому їй $Q_n\alpha - P_n$ та $Q_{n+1}\alpha - P_{n+1}$ мають різні знаки. За формулами (5.1.7) і (5.1.8) з п. 5.1.2 маємо

$$\begin{aligned} Q_{n+1}\alpha - P_{n+1} &= (a_n Q_n + Q_{n-1})\alpha - (a_n P_n + P_{n-1}) = \\ &= a_n(Q_n\alpha - P_n) + (Q_{n-1}\alpha - P_{n-1}). \end{aligned}$$

Оскільки $Q_n\alpha - P_n$ та $Q_{n+1}\alpha - P_{n+1}$ мають різні знаки і $a_n > 0$, то

$$|Q_{n+1}\alpha - P_{n+1}| + a_n|Q_n\alpha - P_n| = |Q_{n-1}\alpha - P_n|.$$

Використовуючи першу частину леми, перепишемо останню рівність у вигляді

$$\|Q_{n+1}\alpha\| + a_n\|Q_n\alpha\| = \|Q_{n-1}\alpha\|.$$

Звідси одержуємо, що $\|Q_n\alpha\| < \|Q_{n-1}\alpha\|$ і лему доведено. \square

Доведення теореми. Нехай α — дійсне число, $\alpha = [a_0, a_1, \dots]$ — його розклад у ланцюговий дріб і $\frac{p}{q}$ — найкраще наближення числа α . Пригадаємо, що за теоремою 5.1.3 підхідні drobi $\frac{P_n}{Q_n}$ числа α задовольняють нерівності

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \dots < \frac{P_{2k}}{Q_{2k}} \leq \alpha \leq \frac{P_{2k+1}}{Q_{2k+1}} < \dots < \frac{P_2}{Q_3} < \frac{P_1}{Q_1}. \quad (5.2.5)$$

Доведемо спочатку, що $\frac{p}{q} \in [\frac{P_0}{Q_0}, \frac{P_1}{Q_1}]$. Якщо $\frac{p}{q} < \frac{P_0}{Q_0} = a_0$, то згідно (5.2.5) $|\alpha - a_0| < |\alpha - \frac{p}{q}| \leq |q\alpha - p|$ і ми отримуємо суперечність з тим, що $\frac{p}{q}$ найкраще наближення. Так само, якщо $\frac{p}{q} > \frac{P_1}{Q_1}$, то

$$\left| \alpha - \frac{p}{q} \right| \stackrel{(5.2.5)}{>} \left| \frac{P_1}{Q_1} - \frac{p}{q} \right| = \left| \frac{P_1 q - Q_1 p}{Q_1 q} \right| \geq \frac{1}{Q_1 q}.$$

Тому $|q\alpha - p| > \frac{1}{Q_1} = \frac{1}{a_1} \geq |\alpha - a_0|$ (остання нерівність випливає з правила для одержання a_1) і ми знову приходимо до суперечності.

Отже, можна зробити висновок, що $\frac{p}{q}$ лежить у проміжку, кінцями якого є деякі два підхідні drobi $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_{n+1}}{Q_{n+1}}$. Залишається довести, що $\frac{p}{q}$ дорівнює $\frac{P_{n-1}}{Q_{n-1}}$ або $\frac{P_{n+1}}{Q_{n+1}}$. Знову міркуємо від супротивного. Нехай $\frac{p}{q}$ лежить між $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_{n+1}}{Q_{n+1}}$. Враховуючи те,

що $\frac{P_n}{Q_n}$ лежить з іншого боку від α , ніж $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_{n+1}}{Q_{n+1}}$ (подивіться на (5.2.5)), маємо

$$\frac{1}{qQ_{n-1}} \leq \frac{|pQ_{n-1} - qP_{n-1}|}{qQ_{n-1}} = \left| \frac{p}{q} - \frac{P_{n-1}}{Q_{n-1}} \right| < \left| \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} \right| = \frac{1}{Q_n Q_{n-1}}.$$

Домножуючи цю нерівність на $qQ_{n-1}Q_n$, одержуємо

$$Q_n < q. \quad (5.2.6)$$

З іншого боку,

$$\frac{1}{qQ_{n+1}} \leq \frac{|P_n + 1q - pQ_n + 1|}{qQ_{n+1}} = \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{p}{q} \right| < \left| \alpha - \frac{p}{q} \right|$$

($\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_{n+1}}{Q_{n+1}}$ лежать з одного боку від α , а $\frac{p}{q}$ лежить між $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_{n+1}}{Q_{n+1}}$).

Домножуючи на q , одержуємо звідси, що $\frac{1}{Q_{n+1}} \leq |q\alpha - p|$. Але $|Q_n\alpha - P_n| = Q_n|\alpha - \frac{P_n}{Q_n}| < Q_n \left| \frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}} \right| = \frac{Q_n|P_n Q_{n-1} - P_{n+1} Q_n|}{Q_n Q_{n+1}} = \frac{1}{Q_{n+1}}$, і тому $|Q_n\alpha - P_n| < |q\alpha - p|$, а це, згідно (5.2.6), суперечить тому, що $\frac{p}{q}$ є найкращим наближенням числа α . Отже, для $\frac{p}{q}$ не залишається нічого іншого як збігатися або з $\frac{P_{n-1}}{Q_{n-1}}$ або з $\frac{P_{n+1}}{Q_{n+1}}$. Це доводить першу частину теореми.

Другу частину теореми доводимо індукцією за n . Не існує q' з властивістю $1 \leq q' < Q_0 = 1$, тому формально або підхідний дріб $\frac{P_0}{Q_0}$ або дріб $\frac{P_0}{Q_0} + 1$ задовольняє означення найкращого наближення числа α . Припустимо, що $n \geq 0$ і ми вже довели, що $\frac{P_n}{Q_n}$ або $\frac{P_{n+1}}{Q_{n+1}}$ є найкращим наближенням числа α . Зазначимо, що у випадку $n > 0$, з леми 5.2.1 а) випливає, що найкращим наближенням буде підхідний дріб $\frac{P_n}{Q_n}$, а не дріб $\frac{P_{n+1}}{Q_{n+1}}$. Виберемо найменше натуральне q , таке, що $q > Q_n$ і $\|q\alpha\| < \|Q_n\alpha\|$. Натуральні числа q , які задовольняють останню нерівність, існують. У випадку раціонального числа α це очевидно (якщо, звичайно, $\|Q_n\alpha\| \neq 0$; у випадку $\|Q_n\alpha\| = 0$ дріб $\frac{P_n}{Q_n}$ є останнім підхідним дробом раціонального числа α), а у випадку, коли число α іrrаціональне,

це випливає з того, що $\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k Q_{k+1}}$ і $Q_n \rightarrow \infty$. Нехай $p \in \mathbb{Z}$ таке, що $|q\alpha - p| = \|q\alpha\|$. Тоді дріб $\frac{p}{q}$ є найкращим наближенням числа α , і за першою частиною теореми цей дріб $\frac{p}{q}$ є підхідним дробом до числа α . Але згідно леми 5.2.1, $\|Q_{n+1}\alpha\| < \|Q_n\alpha\|$. Отже, $q = Q_{n+1}$ і $p = P_{n+1}$, що й потрібно було довести. \square

Наслідок 5.2.2. Якщо $\frac{p}{q}$ — нескоротний дріб з $q > 0$ і такий, що $\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2}$, то $\frac{p}{q}$ є підхідним дробом числа α .

Доведення. Покажемо, що $\frac{p}{q}$ — найкраще найближення числа α . Нехай $\frac{p'}{q'}$ — дріб, у якому $q' > 0$, $\frac{p}{q} \neq \frac{p'}{q'}$, $|q'\alpha - p'| \leq |q\alpha - p| < \frac{1}{2q}$. Тоді

$$\begin{aligned} \frac{1}{qq'} &\leq \left| \frac{p'}{q'} - \frac{p}{q} \right| = \left| \frac{p'}{q'} - \alpha + \alpha - \frac{p}{q} \right| \leq \\ &\leq \left| \alpha - \frac{p'}{q'} \right| + \left| \alpha - \frac{p}{q} \right| < \frac{1}{2qq'} + \frac{1}{2q^2} = \frac{q+q'}{2q^2q'}. \end{aligned}$$

Звідси одержуємо $2q < q+q'$, або $q < q'$. Це означає, що $\frac{p}{q}$ — найкраще наближення, а тому, за доведеною теоремою, це підхідний дріб. \square

5.2.3. Теорема Ліувілля

Комплексне число α називають *алгебраїчним числом степеня n* , якщо α є коренем полінома степеня n із раціональними коефіцієнтами і не є коренем жодного полінома з раціональними коефіцієнтами степеня меншого, ніж n .

Зауважимо, що в цьому означенні можна говорити про поліноми з цілими коефіцієнтами замість поліномів із раціональними коефіцієнтами (використовуючи домноження полінома на спільний знаменник його коефіцієнтів).

Наведемо приклади алгебраїчних чисел. Всі раціональні числа є алгебраїчними числами степеня 1, числа вигляду $a + b\sqrt{d}$,

де $a, b, d \in \mathbb{Q}$ і d не є квадратом, є алгебраїчними числами степеня 2. $\sqrt[n]{a}$ є алгебраїчним числом степеня n , якщо поліном $X^n - a$ мінімальний для $\sqrt[n]{a}$. Суть теореми Ліувілля полягає в тому, що алгебраїчні числа не можуть бути “надто добре наближені раціональними числами”.

Теорема 5.2.3 (Ліувілль). *Для кожного дійсного алгебраїчного числа α степеня n існує дійсне додатне число c , що залежить тільки від α , і таке, що для всіх раціональних чисел $\frac{p}{q}$, $\frac{p}{q} \neq \alpha$, вірна нерівність $|\alpha - \frac{p}{q}| \geq \frac{c}{q^n}$.*

Доведення. Нехай $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ — мінімальний поліном з цілими коефіцієнтами, коренем якого є α . Використовуючи теорему Безу, можемо записати

$$f(X) = (X - \alpha)g(X), \quad (5.2.7)$$

де $g(X)$ — поліном з дійсними коефіцієнтами. Візьмемо довільне число $\delta > 0$. Функція $|g(X)|$ є обмеженою функцією в сегменті $[\alpha - \delta, \alpha + \delta]$. Справді, для $X \in [\alpha - \delta, \alpha + \delta]$ маємо $|g(X)| = |b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}| \leq |b_0| + |b_1| |X| + \cdots + |b_{n-1}| |X|^{n-1} \leq b(1 + |X| + \cdots + |X|^{n-1}) \leq nb\beta^{n-1} = M$, де b — максимум модулів коефіцієнтів b_i полінома $g(X)$, $\beta = \max\{1, |\alpha - \delta|, |\alpha + \delta|\}$. Отже, існує додатне дійсне число M таке, що $|g(X)| \leq M$ для всіх $X \in [\alpha - \delta, \alpha + \delta]$. (Можна було б використати той факт, що функція $g(X)$ неперервна, а отже, обмежена функція на замкненому проміжку $[\alpha - \delta, \alpha + \delta]$). Нехай $c = \min\{M^{-1}, \delta\}$, тоді $c \leq M^{-1}$ і $c \leq \delta$. Якщо $\frac{p}{q}$ — довільне раціональне число, то можливі два випадки.

1) $\frac{p}{q} \notin [\alpha - \delta, \alpha + \delta]$. У цьому випадку

$$\left| \alpha - \frac{p}{q} \right| > \delta \geq c \geq \frac{c}{q^n}. \quad (5.2.8)$$

2) $\frac{p}{q} \in [\alpha - \delta, \alpha + \delta]$. Тоді $|g(p/q)| \leq M$.

Підставивши в (5.2.7) $\frac{p}{q}$ замість X , одержимо

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|g\left(\frac{p}{q}\right)\right| \leq M \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{c} \left|\alpha - \frac{p}{q}\right|. \quad (5.2.9)$$

Враховуючи, що $f\left(\frac{p}{q}\right) \neq 0$, і $|a_0q^n + \dots + a_np^n|$ є цілим числом, більшим або рівним 1, та використовуючи (5.2.9), одержуємо

$$\frac{1}{c} \left|\alpha - \frac{p}{q}\right| \geq \left|f\left(\frac{p}{q}\right)\right| = \frac{|a_0q^n + \dots + a_np^n|}{q^n} \geq \frac{1}{q^n},$$

тобто $\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}$. \square

З теореми Ліувілля випливає, що алгебраїчне число не може надто добре наблизатися раціональними числами. А саме, за означенням 5.2.2 і за теоремою Ліувілля найкращий порядок наближення алгебраїчного числа α степеня n не більший ніж n . Справді, якби алгебраїчне число α степеня n допускало порядок наближення $m > n$ раціональними числами, то для деякої сталої c_1 існувало б нескінченна множина раціональних чисел $\frac{p}{q}$, $q > 0$, для яких $\left|\alpha - \frac{p}{q}\right| < \frac{c_1}{q^m}$. Зокрема, звідси випливало б існування раціональних чисел $\frac{p}{q}$ з як завгодно великими знаменниками, для яких $\left|\alpha - \frac{p}{q}\right| < \frac{c_1}{q^m}$. Але з теореми Ліувілля випливає, що $\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}$. Тому одержуємо $\frac{c}{q^n} < \frac{c_1}{q^m}$, тобто $q^{m-n} < \frac{c_1}{c}$ для всіх q з деякої нескінченної підмножини множини натуральних чисел. Одержані суперечність, яка показує, що найкращий порядок наближення числа α раціональними числами не перевищує n .

У прикладі 2 п.5.2.1 ми бачили, що ірраціональні числа мають порядок наближення раціональними числами не менший ніж 2. Тому порядок наближення квадратичних ірраціональностей раціональними числами дорівнює 2. Далі, у прикладі 3 п.5.2.1 ми довели існування дійсних чисел, які допускають як завгодно великий порядок наближення раціональними числами. З теореми Ліувілля випливає, що такі числа не є алгебраїчними. Інакше

кажучи, з теореми Ліувілля випливає, що існують не алгебраїчні (їх називають трансцендентними) числа. Числа, трансцендентність яких випливає з теореми Ліувілля, називають *трансцендентними числами Ліувілля*; числа з прикладу 3 п.5.2.1 є трансцендентними числами Ліувілля. Наведемо ще один приклад трансцендентних чисел Ліувілля. Нехай

$$\alpha = \frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots = 0,1100010\dots$$

Покажемо, що число α має порядок наближення більший від будь-якого дійсного числа N . Для цього виберемо будь-які дійсні числа $N \geq 1$ і $c > 0$. Візьмемо $p = 10^{k!} \left(\frac{1}{10} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{k!}} \right)$, $q = 10^{k!}$. Виберемо k настільки великим, щоб $10^{k!} \geq \frac{2}{c}$ і $k \geq N$. Тоді $|\alpha - \frac{p}{q}| = \frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \cdots < \frac{1}{10^{(k+1)!}} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \dots \right) < \frac{2}{10^{k!}} \cdot \frac{1}{10^{k!k}} \leq c \cdot q^{-N}$. Оскільки число N можна вибрати як завгодно великим, то з теореми Ліувілля випливає, що α — трансцендентне число.

Жозеф Ліувілль (1809–1882) — французький математик, відомий своїми роботами в теорії еліптичних функцій, диференціальних рівнянь і теорії чисел. Він уперше довів існування трансцендентних чисел у роботах 1844 і 1851 років. Інше доведення існування трансцендентних чисел випливає з результатів Г. Кантора (1845–1918): множина алгебраїчних чисел є зліченою, а множина всіх дійсних чисел є незліченою. Тому існує континуум трансцендентних чисел. Однак довести трансцендентність деякого конкретного, важливого для математики, числа може бути досить важкою справою. Трансцендентніться числа e було доведено у 1873р. французьким математиком Ш. Ермітом, а трансцендентність числа π довів у 1882р. німецький математик К. Ліндеман. Російський математик А.О. Гельфонд у 1934 р. розв'язав сьому проблему Гільберта, а саме, довів, що будь-яке число вигляду α^β , де α — алгебраїчне число, що не дорівнює 0 або 1, а β — алгебраїчне число степеня не меншого ніж 2, є числом трансцендентним. З цих результатів, зокрема, випливає, що десяткові логарифми всіх натуральних чисел $N \neq 10^k$ є транс-

цендентними числами. Більш детально з методами і основними результатами теорії трансцендентних чисел можна познайомитися, наприклад, за книгою [?].

5.2.4. Діофантові наближення та діофантові рівняння

Важливою проблемою в математиці протягом всього ХХ століття була задача покращення теореми Ліувілля. Один із способів її покращити — це зменшити показник n у нерівності

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^n}.$$

Можна поставити питання: для яких показників $d(n)$ для алгебраїчного числа α степеня n існує константа $c > 0$, для якої нерівність

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^{d(n)+\varepsilon}}$$

(ε — будь-яке дійсне число) не має розв'язків в цілих $p \in \mathbb{Z}$ і $q \in \mathbb{N}$? Норвежський математик А. Туе у 1909 році довів, що можна взяти $d(n) = \frac{1}{2}n + 1$, потім німецький математик К. Зігель у 1921р. зменшив $d(n)$ до $d(n) = 2\sqrt{n}$. Російський математик А.О. Гельфонд у 1948р. показав, що можна взяти $d(n) = \sqrt{2n}$. Нарешті, у 1955р. англійський математик К. Рот довів, що можна взяти $d(n) = 2$. Доведення всіх цих результатів є досить складними. Зазначимо, що К. Рот отримав за свій результат у 1958р. на Міжнародному конгресі математиків в Единбурзі Філдсівську премію — найвищу міжнародну нагороду для математиків. Всі ці результати дозволяють, зокрема, будувати нові класи трансцендентних чисел (див. впр.11). Крім того, ці результати можна застосовувати до дослідження діофантових рівнянь. Покажемо, як це робиться на прикладі теореми Туе.

Сформулюємо теорему Туе про діофантові наближення.

Теорема 5.2.4. *Нехай α — дійсне алгебраїчне число степеня $n \geq 2$, $\varepsilon > 0$ — будь-яке дійсне число. Існує константа $c > 0$*

така, що для всіх $p \in \mathbb{Z}$, $q \in \mathbb{N}$ вірна нерівність

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^{(n/2)+1+\varepsilon}}.$$

Підкреслимо, що ми не наводимо тут доведення теореми Туе про діофантові наближення (з доведенням можна ознайомитися, наприклад, у [?], [?] або в [?]). Наша мета — показати, як Туе застосував цю теорему до дослідження діофантових рівнянь.

Теорема 5.2.5 (Туе, про діофантові рівняння). *Нехай*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad (5.2.10)$$

— незвідний поліном з цілими коефіцієнтами, $a_n > 0$, $n \geq 3$. Розглянемо поліном

$$F(X, Y) = a_n X^n + a_{n-1} X^{n-1} Y + \cdots + a_1 X Y^{n-1} + a_0 Y^n, \quad (5.2.11)$$

і $m \in \mathbb{Z}$. Діофантове рівняння

$$F(X, Y) = m \quad (5.2.12)$$

або не має цілих розв'язків або має їх лише скінченну кількість.

Доведення. Якщо $m = 0$, то діофантове рівняння (5.2.12) має лише тривіальний розв'язок $(0, 0)$, бо в іншому випадку поліном (5.2.10) мав би раціональний корінь, а це суперечить тому, що він незвідний. Припустимо, що $m \neq 0$. Якщо $\alpha_1, \dots, \alpha_n$ — комплексні корені полінома (5.2.10), то

$$\frac{F(X, Y)}{Y^n} = f\left(\frac{X}{Y}\right) = a_n \left(\frac{X}{Y} - \alpha_1\right) \cdots \left(\frac{X}{Y} - \alpha_n\right)$$

або

$$F(X, Y) = a_n (X - \alpha_1 Y) \cdots (X - \alpha_n Y). \quad (5.2.13)$$

Нехай $p \in \mathbb{Z}$, $q \in \mathbb{N}$ — розв'язок рівняння (5.2.12). Покажемо, що існує константа $D > 0$ така, що

$$q \leq D, \quad (5.2.14)$$

для кожного розв'язку (p, q) рівняння (5.2.12). Звідси випливатиме скінченність множини розв'язків (p, q) з додатними q , бо для кожного q існує, зрозуміло, лише скінчена кількість p таких, що пара (p, q) є розв'язком рівняння (5.2.12).

Отже, потрібно показати, що рівняння (5.2.12) не має розв'язків $(p, q), p \in \mathbb{Z}, q \in \mathbb{N}$ з дуже великими q .

Якщо $(p, q), p \in \mathbb{Z}, q \in \mathbb{N}$ — розв'язок рівняння (5.2.12), то з (5.2.13) маємо

$$a_n |p - \alpha_1 q| \dots |p - \alpha_n q| = |m|. \quad (5.2.15)$$

Тому можна зробити висновок, що серед чисел $\alpha_1, \dots, \alpha_n$ знається число, наприклад α_1 , для якого

$$|p - \alpha_1 q| \leq \sqrt[n]{\frac{|m|}{a_n}}. \quad (5.2.16)$$

Оскільки всі корені $\alpha_1, \dots, \alpha_n$ різні (бо $f(x)$ незвідний), то знається така константа A , що

$$0 < A < \min \{ |\alpha_1 - \alpha_i| \mid 2 \leq i \leq n \}. \quad (5.2.17)$$

Використовуючи (5.2.16) і (5.2.17), маємо оцінку

$$|p - \alpha_i q| = |(\alpha_1 - \alpha_i)q + (p - \alpha_1 q)| \geq |\alpha_1 - \alpha_i|q - |p - \alpha_1 q| > Aq - \sqrt[n]{\frac{|m|}{a_n}}, \quad (5.2.18)$$

де $2 \leq i \leq n$. Пригадаємо, що ми хочемо показати відсутність розв'язків (p, q) , у яких q більше від деякої константи D . Тому припустимо, що

$$q > \frac{2 \sqrt[n]{\frac{|m|}{a_n}}}{A}. \quad (5.2.19)$$

Для таких чисел q з нерівності (5.2.18) одержимо $|p - \alpha_i q| > \frac{1}{2} Aq$, $2 \leq i \leq n$. Тому маємо

$$\prod_{i=2}^n |p - \alpha_i q| > \left(\frac{1}{2} Aq \right)^{n-1}.$$

Враховуючи цю нерівність, одержуємо з (5.2.15)

$$|p - \alpha_1 q| = \frac{|m|}{a_n \prod_{i=2}^n |p - \alpha_i q|} < \frac{|m|}{a_n \left(\frac{1}{2}A\right)^{n-1} q^{n-1}},$$

тобто, позначивши $c_1 = \frac{|m|}{a_n \left(\frac{1}{2}A\right)^{n-1}}$, одержуємо нерівність $|p - \alpha_1 q| < \frac{c_1}{q^{n-1}}$, яку запишемо у вигляді:

$$\left| \alpha_1 - \frac{p}{q} \right| < \frac{c_1}{q^n}. \quad (5.2.20)$$

Але, за теоремою Туе про діофантові наближення, існує константа c , для якої вірна нерівність

$$\left| \alpha_1 - \frac{p}{q} \right| > \frac{c}{q^{(n/2)+1+0,1}} \quad (5.2.21)$$

(ми взяли $\varepsilon = 0,1$ в формулуванні теореми Туе). З нерівностей (5.2.20) і (5.2.21) випливає (згадаємо, що $n \geq 3$)

$$\frac{c}{q^{(n/2)+1,1}} < \frac{c_1}{q^n}, \quad q < \left(\frac{c_1}{c} \right)^{\frac{2}{n-2,2}}.$$

Враховуючи (5.2.19), бачимо, що остання нерівність приведе до суперечності, якщо припустити, що існує розв'язок (p, q) рівняння (5.2.12) з

$$q > D = \max \left\{ \frac{2}{A} \sqrt[n]{\frac{|m|}{a_n}}, \left(\frac{c_1}{c} \right)^{\frac{2}{n-2,2}} \right\}.$$

Тому всі розв'язки (p, q) рівняння (5.2.12) з додатними q задовільняють умові (5.2.14), якщо $D = \max \left\{ \frac{2}{A} \sqrt[n]{\frac{|m|}{a_n}}, \left(\frac{c_1}{c} \right)^{\frac{2}{n-2,2}} \right\}$, а тому їх існує лише скінчена кількість.

Випадок від'ємних значень q зводиться до випадку додатних q заміною рівняння (5.2.12) рівнянням $F(x, -y) = m$. Теорему доказано. \square

5.3. Застосування ланцюгових дробів

5.3.1. Розв'язування конгруенцій першого степеня

Розглянемо конгруенцію

$$aX \equiv b \pmod{m}, \quad (5.3.1)$$

де вважаємо, що $(a, m) = 1$. Розкладемо раціональне число $\frac{m}{a}$ у ланцюговий дріб. Нехай $\frac{P_{n-1}}{Q_{n-1}}$ та $\frac{P_n}{Q_n} = \frac{m}{a}$ — передостанній та останній підхідні дроби цього ланцюгового дробу. За формулою (5.1.9) п.5.1.2 маємо

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^{n-1}.$$

Підставимо $P_n = m$, $Q_n = a$. Одержано $mQ_{n-1} - aP_{n-1} = (-1)^{n-1}$, тобто

$$aP_{n-1} \equiv (-1)^n \pmod{m},$$

i

$$(-1)^n aP_{n-1} \equiv 1 \pmod{m}.$$

Тому, підставивши у (5.3.1) $(-1)^n P_{n-1} b$ замість X , бачимо, що клас лишків $(-1)^n P_{n-1} b \pmod{m}$ є розв'язком конгруенції (5.3.1). Цей клас лишків є єдиним розв'язком конгруенції (5.3.1) (див. п.4.2.4).

Приклад 5.3.1. Розв'яжемо конгруенцію

$$37x \equiv 1001 \pmod{1995}.$$

Для цього розкладаємо (використовуючи алгоритм Евкліда) $\frac{1995}{37}$ у ланцюговий дріб. Одержано

$$\frac{1995}{37} = [53, 1, 11, 3].$$

Отож, $n = 3$. Знаходимо P_{n-1} за схемою, описаною в п. 5.1.2:

	53	1	11	3
1	53	54	647	1995

$P_2 = 647$. Розв'язком нашої конгруенції є клас лішиків $(-1)^3 \cdot 647 \cdot 1001 \pmod{1995} \equiv 1348 \cdot 1001 \pmod{1995} \equiv 1349348 \pmod{1995} \equiv 728 \pmod{1995}$.

5.3.2. Розв'язування діофантових рівнянь $aX + bY = c$

Розглянемо рівняння

$$aX + bY = c, \quad (5.3.2)$$

де $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$. Будемо шукати розв'язки рівняння (5.3.2) у цілих числах. Нехай $d = (a, b)$ — найбільший спільний дільник чисел a і b . Якщо $d \nmid c$, то, очевидно, рівняння (5.3.2) не має цілих розв'язків. Тому будемо вважати, що $d|c$. Тоді $a = a_1d$, $b = b_1d$ і $c = c_1d$. Розділивши рівняння (5.3.2) на d , одержимо рівняння

$$a_1x + b_1y = c_1, \quad (5.3.3)$$

де $(a_1, b_1) = 1$. Зрозуміло, що кожний розв'язок у цілих числах рівняння (5.3.2) є розв'язком рівняння (5.3.3) і навпаки. Тому надалі будемо вважати коефіцієнти a і b в рівнянні (5.3.2) взаємно простими. Крім цього, домноживши, якщо необхідно, рівняння (5.3.2) на -1 (це приводить до рівносильного рівняння), можна вважати, що коефіцієнт b при y є від'ємним. Підсумовуючи все сказане, бачимо, що можна зосередити увагу на рівняннях вигляду

$$aX - bY = c, \quad (5.3.4)$$

де $a, b \in \mathbb{Z}$, $b > 0$, $(a, b) = 1$. Припустимо, що рівняння (5.3.4) має розв'язок, і доведемо при цьому припущені просту теорему, яка описує множину всіх розв'язків.

Теорема 5.3.1. Нехай (x_0, y_0) будь-який цілий розв'язок рівняння (5.3.4). Тоді множина всіх розв'язків цього рівняння має вигляд

$$\{(x_0 + bt, y_0 + at) \mid t \in \mathbb{Z}\}. \quad (5.3.5)$$

Доведення. Нехай (\tilde{x}, \tilde{y}) — ще один розв'язок рівняння (5.3.4). Тоді $a\tilde{x} - b\tilde{y} = c$, $ax_0 - by_0 = c$. Звідси маємо

$$a(\tilde{x} - x_0) = b(\tilde{y} - y_0). \quad (5.3.6)$$

Оскільки $(a, b) = 1$, то $b|\tilde{x} - x_0$, тобто $\tilde{x} - x_0 = bt$, тому $\tilde{x} = x_0 + bt$. Підставимо \tilde{x} в (5.3.6):

$$abt = b(\tilde{y} - y_0).$$

Звідси одержуємо, що $y = y_0 + at$. Отже, всі розв'язки містяться у множині (5.3.5). Залишається перевірити, що будь-який елемент з множини (5.3.5) є розв'язком рівняння (5.3.4). У цьому дуже легко переконатися, підставивши $(x_0 + bt, y_0 + at)$ у рівняння (5.3.4). \square

Тепер доведемо існування розв'язків рівняння (5.3.4).

Теорема 5.3.2. Рівняння

$$aX - bY = c, \quad a, b \in \mathbb{Z}, b > 0, (a, b) = 1,$$

має своїм розв'язком

$$x_0 = (-1)^{n-1}Q_{n-1}c, \quad y_0 = (-1)^{n-1}P_{n-1}c,$$

де $\frac{P_{n-1}}{Q_{n-1}}$ — передостанній підхідний дріб у розкладі числа $\frac{a}{b} = \frac{P_n}{Q_n}$ у ланцюговий дріб.

Доведення. Знову використаємо рівність $P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1}$, яку перепишемо у вигляді: $aQ_{n-1} - bP_{n-1} = (-1)^{n-1}$. Домноживши останню рівність на $(-1)^{n-1}c$, одержимо

$$a((-1)^{n-1}cQ_{n-1}) - b((-1)^{n-1}cP_{n-1}) = c,$$

що й доводить теорему. \square

Приклад 5.3.2. Знайдемо розв'язок рівняння

$$1999x - 1997y = 3.$$

$(1999, 1997) = 1$. Розкладемо $\frac{1999}{1997}$ у ланцюговий дріб $\frac{1999}{1997} = [1, 998, 2]$. Отже, $n = 2$. Обчислимо підхідні дроби P_1 і Q_1 :

	1	998	2
1	1	999	
0	1	998	

$P_1 = 999$, $Q_1 = 998$. З теореми 5.3.2 випливає, що одним з розв'язків є $x_0 = -3 \cdot 998 = -2994$, $y_0 = -3 \cdot 999 = -2997$. Найменшим додатним розв'язком нашого рівняння є

$$(-2994 + 2 \cdot 1997, -2997 + 2 \cdot 1999) = (1000, 1001).$$

Зауважимо, що формули з теореми 5.3.2 зберігають свою силу і у випадку, коли $n = 0$, тобто $\frac{a}{b} = \frac{P_0}{Q_0}$. У цьому випадку $b = 1$ і розв'язок $(0, c)$ рівняння $aX - Y = c$ може бути одержаний за формулами з теореми 5.3.2, якщо згадати нашу домовленість стосовно P_{-1} і Q_{-1} : $P_{-1} = 1$, $Q_{-1} = 0$.

5.3.3. Кільце цілих чисел квадратичного поля

Розглянемо довільне ціле число $d \neq 1$, вільне від квадратів (тобто, d не ділиться на квадрат будь-якого простого числа). Легко переконатися в тому, що множина дійсних чисел $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ є полем відносно звичайних операцій додавання і множення. Покажемо, що для кожного ненульового елемента $\alpha \in \mathbb{Q}(\sqrt{d})$ існує обернений елемент відносно множення, а решту роботи, необхідної для перевірки аксіом поля, пропонуємо читачеві зробити самостійно. Нехай $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $\alpha \neq 0$. Тоді $a^2 - db^2 \neq 0$, бо інакше при $b \neq 0$ маємо $d = \left(\frac{a}{b}\right)^2$, що приводить до суперечності з тим, що d вільне від квадратів

(тут потрібно використати основну теорему арифметики). Якщо ж $b = 0$, то $a \neq 0$, і в усіх випадках елемент

$$\alpha^{-1} = \frac{a}{a^2 - bd^2} - \frac{b\sqrt{d}}{a^2 - bd^2} \in \mathbb{Q}(\sqrt{d})$$

є оберненим до α .

Означення 5.3.1. Елемент $\alpha \in \mathbb{Q}(\sqrt{d})$ називається *цілим*, якщо α є коренем полінома з цілими коефіцієнтами і старшим коефіцієнтом 1.

Зрозуміло, що кожне звичайне ціле число a є цілим елементом поля $\mathbb{Q}(\sqrt{d})$. Воно є коренем незвідного полінома $x - a$. Звичайні цілі числа називатимемо далі цілими раціональними. Якщо $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, то елемент $\alpha' = a - b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ називають *спряженим* до α . (Переконайтесь в тому, що $(\alpha + \beta)' = \alpha' + \beta'$ і $(\alpha\beta)' = \alpha'\beta'$. Ці властивості спряження будуть далі використані.) Число $\alpha = a + b\sqrt{d}$ є коренем полінома $(X - \alpha)(X - \alpha') = (X - a - b\sqrt{d})(X - a + b\sqrt{d}) = (X - a)^2 - db^2 = X^2 - 2aX + a^2 - db^2$ з раціональними коефіцієнтами $\alpha + \alpha' = 2a$, $\alpha \cdot \alpha' = a^2 - db^2$ і з дискримінантом $4db^2$, який не є точним квадратом, якщо $b \neq 0$ (d — ціле число, вільне від квадратів). Тому можна дати ще одне еквівалентне означення цілого елемента поля $\mathbb{Q}(\sqrt{d})$.

Означення 5.3.2. Нехай $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Число $\text{Tr}(\alpha) \stackrel{\text{def}}{=} \alpha + \alpha' = 2a$ називають *слідом*, а число $N(\alpha) \stackrel{\text{def}}{=} \alpha \cdot \alpha' = a^2 - db^2$ називають *нормою* числа α . Число $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ називається *цілим*, якщо його слід $\text{Tr}(\alpha) = 2a$ і його норма $N(\alpha) = a^2 - db^2$ є цілими раціональними числами.

Оскільки $(X - \alpha)(X - \alpha') = (X^2 - \text{Tr}(\alpha)X + N(\alpha))$, то еквівалентність двох означень цілого елемента є очевидною. Зручно записувати числа $\alpha \in \mathbb{Q}(\sqrt{d})$ у вигляді $\alpha = \frac{u+v\sqrt{d}}{2}$ (замість $\alpha = a + b\sqrt{d}$) з раціональними u і v .

Теорема 5.3.3. Число $\alpha = \frac{u+v\sqrt{d}}{2} \in \mathbb{Q}(\sqrt{d})$ є цілим моді і тільки моді, коли u і v є цілими раціональними і

$$\begin{aligned} u \equiv v \equiv 0 \pmod{2} \text{ при } d \equiv 2 \pmod{4} \text{ або } d \equiv 3 \pmod{4}; \\ u \equiv v \pmod{2} \text{ при } d \equiv 1 \pmod{4}. \end{aligned} \quad (5.3.7)$$

Доведення. Нехай α є цілим. Тоді $\text{Tr}(\alpha) = u$ ціле раціональне і $N(\alpha) = \frac{u^2 - dv^2}{4}$ ціле раціональне, тому ѹ $u^2 - dv^2$ ціле раціональне. Якби v не було цілим раціональним, то знаменник v^2 не міг би скоротитися з d , оскільки d вільне від квадратів. Отже, і v ціле раціональне. Далі

$$u^2 - dv^2 \equiv 0 \pmod{4}. \quad (5.3.8)$$

Квадрат цілого числа конгруентний або з 0 або з 1 за $(\text{mod } 4)$. Тому при $d \equiv 2, 3 \pmod{4}$ конгруенція (5.3.8) можлива лише при $u \equiv v \equiv 0 \pmod{2}$, а при $d \equiv 1 \pmod{4}$ конгруенція (5.3.8) можлива лише при $u \equiv v \pmod{2}$.

Навпаки, нехай u і v — цілі раціональні числа і виконуються конгруенції (5.3.7). Тоді $\text{Tr}(\alpha) = u$ є цілим раціональним і $N(\alpha) = \frac{u^2 - dv^2}{4}$, згідно (5.3.7), є цілим раціональним. За означенням 5.3.2 $\alpha = \frac{u+v\sqrt{d}}{2}$ є цілим елементом поля $\mathbb{Q}(\sqrt{d})$. \square

Тепер виділимо елемент ω поля $\mathbb{Q}(\sqrt{d})$.

$$\begin{cases} \omega = \frac{1+\sqrt{d}}{2}, & \text{якщо } d \equiv 1 \pmod{4}, \\ \omega = \sqrt{d}, & \text{якщо } d \equiv 2, 3 \pmod{4}. \end{cases} \quad (5.3.9)$$

Роль елемента ω розкриває наступна теорема.

Теорема 5.3.4. Елемент $\alpha \in \mathbb{Q}(\sqrt{d})$ є цілим моді і тільки моді, коли існують цілі числа $a, b \in \mathbb{Z}$ такі, що $\alpha = a + b\omega$.

Доведення. Нехай $\alpha = \frac{u+v\sqrt{d}}{2}$ — цілий елемент. Якщо $d \equiv 2, 3 \pmod{4}$, то за теоремою 5.3.3 $u = 2a$, $v = 2b$ і $\alpha = a + b\sqrt{d}$,

$a, b \in \mathbb{Z}$. Якщо $d \equiv 1 \pmod{4}$, то $u - v = 2a$ за теоремою 5.3.3; тому

$$\alpha = \frac{u + v\sqrt{d}}{2} = \frac{u - v + v + v\sqrt{d}}{2} = \frac{u - v}{2} + v\frac{1 + \sqrt{d}}{2} = a + v\omega,$$

де $a, v \in \mathbb{Z}$.

Навпаки, якщо $\alpha = a + b\omega$, $a, b \in \mathbb{Z}$, то за означенням 5.3.2 досить довести, що $N(\alpha)$, і $\text{Tr}(\alpha)$ є цілими раціональними числами. Прості обчислення показують, що числа

$$\begin{aligned}\text{Tr}(\alpha) &= \begin{cases} 2a, & \text{якщо } d \equiv 2, 3 \pmod{4}, \\ 2a + b, & \text{якщо } d \equiv 1 \pmod{4}, \end{cases} \\ N(\alpha) &= \begin{cases} a^2 - db^2, & \text{якщо } d \equiv 2, 3 \pmod{4}, \\ a^2 + ab + b^2 \frac{1-d^2}{4}, & \text{якщо } d \equiv 1 \pmod{4} \end{cases}\end{aligned}$$

є цілими раціональними. Теорему 5.3.4 доведено. \square

Позначимо множину цілих елементів поля $\mathbb{Q}(\sqrt{d})$ через \mathcal{O}_d або просто через \mathcal{O} , коли відомо про яке d іде мова. Виявляється, що \mathcal{O}_d є кільцем.

Теорема 5.3.5. $\mathcal{O}_d = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ є комутативним кільцем з 1 і без дільників нуля відносно звичайних операцій.

Доведення. Досить показати лише, що множина \mathcal{O}_d замкнена відносно множення, а все інше очевидне. Замкненість відносно множення зводиться до твердження, що $\omega^2 \in \mathcal{O}_d$. Перевіримо це твердження простим обчисленням:

$$\omega^2 = \begin{cases} d, & \text{якщо } d \equiv 2, 3 \pmod{4}, \\ \frac{d-1}{4} + \omega, & \text{якщо } d \equiv 1 \pmod{4}. \end{cases}$$

\square

Кільце \mathcal{O}_d має багато властивостей, схожих на властивості кільця звичайних цілих чисел \mathbb{Z} , але не всі властивості кільця \mathbb{Z} залишаються справедливими для кільца \mathcal{O}_d . Зокрема, взагалі кажучи, кільца \mathcal{O}_d не є факторіальними. Так у кільці $\mathcal{O}_{10} = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ $2, 5, \sqrt{10}$ є попарно неасоційованими простими елементами і $10 = 2 \cdot 5 = (\sqrt{10})^2$. З іншого боку, можна показати, що, наприклад, кільца $\mathcal{O}_{-3}, \mathcal{O}_5$ є факторіальними. Зauważимо, що кільца $\mathbb{Z}[\sqrt{-3}]$ та $\mathbb{Z}[\sqrt{5}]$ не факторіальні (див. вправи 15–18).

Далі нам потрібно буде використати один частковий випадок поняття кільця класів лишків для кільця цілих елементів \mathcal{O} квадратичного поля $\mathbb{Q}(\sqrt{d})$. Нехай m — натуральне число. Назовемо числа $\alpha_1 = a_1 + b_1\omega, \alpha_2 = a_2 + b_2\omega$ конгруентними за модулем m , і будемо в цьому випадку писати

$$\alpha_1 \equiv \alpha_2 \pmod{m}, \quad (5.3.10)$$

якщо $a_1 \equiv a_2 \pmod{m}$ і $b_1 \equiv b_2 \pmod{m}$. Легко перевірити (пропонуємо зробити це в якості вправи), що відношення (5.3.10) є відношенням еквівалентності на множині \mathcal{O} , тому можна розгляднути фактор-множину, яку ми позначимо через $\mathcal{O}/m\mathcal{O}$:

$$\mathcal{O}/m\mathcal{O} = \{\overline{a+b\omega} \mid a, b \in \mathbb{Z}\},$$

де $\overline{a+b\omega}$ — суміжний клас з представником $a+b\omega$.

Розділивши a і b з остачею на m ($a = md_1 + r, b = md_2 + s, 0 \leq r, s < m$), одержимо, що $\overline{a+b\omega} = \overline{r+s\omega}$. Крім того, якщо $\overline{r_1+s_1\omega} = \overline{r_2+s_2\omega}, 0 \leq r_i, s_i < m$, то $r_1 = r_2$ і $s_1 = s_2$. Це означає, що фактор-множина $\mathcal{O}/m\mathcal{O}$ складається з m^2 елементів. Пропонуємо самостійно показати, що множина $\mathcal{O}/m\mathcal{O}$ є комутативним кільцем з 1 відносно наступних операцій: $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$, $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$.

5.3.4. Одиниці у квадратичних полях

Означення 5.3.3. Одиницею квадратичного поля $\mathbb{Q}(\sqrt{d})$ називають оборотний елемент кільця цілих елементів цього поля.

Ми знаємо, що одиниці будь-якого кільця з 1 утворюють групу відносно множення. Опишемо цю групу у випадку кільця цілих квадратичного поля. Обмежимося тут випадком дійсного квадратичного поля $\mathbb{Q}(\sqrt{d})$, тобто випадком, коли $d > 0$. Випадок уявного квадратичного поля $\mathbb{Q}(\sqrt{d})$ (тобто випадок $d < 0$) значно простіший і ми пропонуємо розглянути цей випадок самостійно (відповідний результат і вказівка до нього сформульовані у вправі 14). Почнемо з простої теореми.

Теорема 5.3.6. *Елемент $\varepsilon \in \mathcal{O}$ є одиницею тоді і тільки тоді, коли $N(\varepsilon) = \varepsilon\varepsilon' = \pm 1$.*

Доведення. Нагадаємо, що штрих означає спряження: $(a + b\sqrt{d})' = a - b\sqrt{d}$. Нехай $\varepsilon \in \mathcal{O}$, і існує $\delta \in \mathcal{O}$, для якого $\varepsilon\delta = 1$. Тоді $N(\varepsilon\delta) = \varepsilon\delta\varepsilon'\delta' = N(\varepsilon)N(\delta) = N(1) = 1$. Оскільки $N(\varepsilon), N(\delta) \in \mathbb{Z}$, то остання рівність можлива тільки тоді, коли $N(\varepsilon) = \pm 1$. Навпаки, якщо $N(\varepsilon) = \varepsilon\varepsilon' = \pm 1$, то ε' або $-\varepsilon'$ є оберненим до ε . (Зауважимо, що з $\alpha = a + b\omega \in \mathcal{O}$ випливає, що $\alpha' = a + b\omega' \in \mathcal{O}$, оскільки $\omega' = -\omega$ або $\omega' = 1 - \omega$). \square

Назовемо одиницю ε *нетривіальною*, якщо $\varepsilon \neq \pm 1$.

Теорема 5.3.7. *У кожному дійсному квадратичному полі існує нетривіальна одиниця.*

Для доведення цієї теореми нам потрібна одна лема.

Лема 5.3.1. *Для кожного натурального числа n існує такий цілий елемент $\alpha \in \mathcal{O}$, що $\alpha < |\alpha| < \frac{1}{n}$ і $|N(\alpha)| \leq 1 + 2\sqrt{d}$.*

Доведення. Візьмемо елемент $-\omega$ (див. 5.3.9). Розглянемо підхідні дроби розкладу $-\omega$ у ланцюговий дріб. $-\omega$ — ірраціональне число, тому послідовність підхідних дробів $\frac{P_k}{Q_k}$ є нескінченною, а послідовність їх знаменників

$$Q_0 \leq Q_1 < Q_2 < \dots$$

є необмежено зростаючою. Для даного n вибираємо k так, щоб $Q_k \leq n < Q_{k+1}$. Тоді маємо,

$$\left| -\omega - \frac{P_k}{Q_k} \right| < \left| \frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} \right| = \frac{|P_{k+1}Q_k - Q_{k+1}P_k|}{Q_k Q_{k+1}} \leq \frac{1}{Q_k Q_{k+1}}.$$

Після домноження на Q_k одержуємо

$$|Q_k \omega + P_k| < \frac{1}{Q_{k+1}} < \frac{1}{n}.$$

$Q_k \omega + P_k \in \mathcal{O}$ за теоремою 5.3.4. Отже, ми знайшли цілий елемент $\alpha = q\omega + p$, для якого $|\alpha| < \frac{1}{n}$. Далі,

$$\alpha' = p + q\omega' = p + q\omega + q(\omega' - \omega) = \begin{cases} \alpha - q\sqrt{d}, & \text{якщо } d \equiv 1 \pmod{4}, \\ \alpha - 2q\sqrt{d}, & \text{якщо } d \equiv 2, 3 \pmod{4}. \end{cases}.$$

Звідси, використовуючи, що ми вибрали q так, щоб $q \leq n$, одержуємо

$$|\alpha'| \leq |\alpha| + 2n\sqrt{d} < \frac{1}{n} + 2n\sqrt{d},$$

і остаточно $|N(\alpha)| = |\alpha||\alpha'| < \frac{1}{n^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}$. \square

Переходимо до доведення теореми 5.3.7, яке розіб'ємо на чотири кроки.

Доведення теореми 5.3.7. 1. Існує нескінчена кількість цілих елементів $\alpha \in \mathcal{O}$, для яких $|N(\alpha)| < 1 + 2\sqrt{d}$. Справді, з леми випливає, що існує хоча б один такий ненульовий елемент α_1 . Візьмемо натуральне число n_1 , для якого $\frac{1}{n_1} < |\alpha_1|$. За лемою знову існує ненульовий елемент α_2 з $N(\alpha_2) < 1 + 2\sqrt{d}$, $|\alpha_2| < \frac{1}{n_1}$, тому $\alpha_1 \neq \alpha_2$. Припустимо, що ми вже знайшли елементи $\alpha_1, \dots, \alpha_k \in \mathcal{O}$, для яких $|\alpha_1| > |\alpha_2| > \dots > |\alpha_k|$ і $N(\alpha_i) < 1 + 2\sqrt{d}$, $1 \leq i \leq k_1$. Візьмемо n_k , для якого $\frac{1}{n_k} < |\alpha_k|$, і застосуємо лему для знаходження α_{k+1} .

2. Існують натуральні числа m , $1 \leq m < 1 + 2\sqrt{d}$, і нескінчена кількість елементів $\alpha \in \mathcal{O}$ з властивістю $|N(\alpha)| < 1 + 2\sqrt{d}$ і

таких, що $|N(\alpha)| = m$. Це твердження випливає з того, що $N(\alpha)$ є цілим числом, отже, $|N(\alpha)|$ є натуральним числом, і існує лише скінчена кількість натуральних чисел менших за $1 + 2\sqrt{d}$. Якби для кожного натурального m існувала б лише скінчена кількість α з властивістю $|N(\alpha)| = m$, то це суперечило б кроку 1.

3. Існує суміжний клас у факторкільці $\mathcal{O}/m\mathcal{O}$, який містить нескінченну кількість елементів $\alpha \in \mathcal{O}$ з властивістю $|N(\alpha)| = m < 1 + 2\sqrt{d}$. Це випливає з того, що таких елементів нескінченно багато, а різних суміжних класів усього m^2 . Отже, хоч один клас в $\mathcal{O}/m\mathcal{O}$ повинен містити нескінченну кількість елементів $\alpha \in \mathcal{O}$, для яких $|N(\alpha)| = m$.

4. Тому існують такі елементи $\alpha, \beta \in \mathcal{O}$, $\alpha \neq \pm\beta$, що

$$\begin{aligned} |N(\alpha)| &= |N(\beta)| = m, \\ \alpha &\equiv \beta \pmod{m}. \end{aligned} \tag{5.3.11}$$

Оскільки $\alpha - \beta = m\gamma$ для деякого $\gamma \in \mathcal{O}$, то $\alpha\beta' - \beta\beta' = m\gamma\beta'$, тобто

$$\alpha\beta' \equiv \beta\beta' = N(\beta) \pmod{m}.$$

Звідси маємо $\alpha\beta' = m\zeta$ для деякого $\zeta \in \mathcal{O}$, а тому, враховуючи (5.3.11), одержуємо $\frac{\alpha\beta'}{\beta\beta'} = \pm\zeta$ або $\alpha = \pm\beta\zeta$. Таким чином,

$$|N(\alpha)| = |N(\beta)| \cdot |N(\zeta)|.$$

Знову, враховуючи (5.3.11), розділимо цю рівність на m . Одержано $|N(\zeta)| = 1$, тобто $N(\zeta) = \pm 1$, тому ζ є одиницею і ця одиниця нетривіальна за нашим вибором α і β ($\alpha \neq \pm\beta$). \square

Наступна теорема описує будову групи всіх одиниць дійсного квадратичного поля.

Теорема 5.3.8. *Існує така одиниця ε дійсного квадратичного поля, що кожна одиниця δ цього поля має вигляд*

$$\delta = \pm\varepsilon^n, \quad n \in \mathbb{Z}.$$

Доведення. За попередньою теоремою існує хоча б одна нетривіальна одиниця ε_1 . Нехай, спочатку, $N(\varepsilon_1) = 1$. Тоді $\varepsilon'_1 = \varepsilon_1^{-1}$ і всі чотири числа $\pm\varepsilon_1, \pm\varepsilon_1^{-1}$ є одиницями. Дві з цих одиниць додатні; нехай це будуть $\varepsilon_1, \varepsilon_1^{-1}$. Одне з двох чисел $\varepsilon_1, \varepsilon_1^{-1}$ більше від 1. Нетривіальну одиницю, більшу від 1, називають *нормованою*. Зрозуміло, що четвірка чисел $\pm\varepsilon_1, \pm\varepsilon_1^{-1}$ може бути записана у вигляді $\frac{1}{2}(\pm u \pm v\sqrt{d})$ з $u, v \in \mathbb{N}$, і нормована одиниця тоді запишеться у вигляді

$$\frac{u + v\sqrt{d}}{2}, \quad u, v \in \mathbb{N}. \quad (5.3.12)$$

Якщо ж $N(\varepsilon_1) = -1$, то $\varepsilon'_1 = -\varepsilon_1^{-1}$, і четвірка чисел $\pm\varepsilon_1, \pm\varepsilon'_1$ теж може бути записана у вигляді $\frac{1}{2}(\pm u \pm v\sqrt{d})$ з $u, v \in \mathbb{N}$, а нормована одиниця цієї четвірки теж має вигляд (5.3.12). Тепер серед усіх нормованих одиниць вибираємо найменшу $\frac{1}{2}(u_0 + v_0\sqrt{d})$. Цей вибір можливий. Справді, ми вже знаємо, що існує хоч одна нормована одиниця: нехай це $\frac{1}{2}(u + v\sqrt{d})$. Існує також лише скінченнна кількість пар (u_1, v_1) , $u_1, v_1 \in \mathbb{N}$, $u_1 \leq u$, $0 \leq u_1$, $v_1 \leq \frac{1}{2}(u + v\sqrt{d})$. Серед цих пар (u_1, v_1) вибираємо всі пари (u_2, v_2) , які є розв'язками хоча б одного з рівнянь

$$\frac{x^2 - dy^2}{4} = \pm 1.$$

В результаті одержимо скінченну кількість нормованих одиниць $\frac{1}{2}(u_2 + v_2\sqrt{d})$, серед яких вибираємо найменшу. Позначимо її через ε . Тепер нехай γ — будь-яка нормована одиниця. Знайдеться єдине натуральне n , для якого $\varepsilon^n \leq \gamma < \varepsilon^{n+1}$. Розділивши цю нерівність на ε^n , одержимо $1 \leq \frac{\gamma}{\varepsilon^n} < \varepsilon$. Оскільки ε — найменша нормована одиниця, то звідси одержуємо $\frac{\gamma}{\varepsilon^n} = 1$, отже, $\gamma = \varepsilon^n$. Якщо тепер δ — будь-яка одиниця, то одна з чотирьох одиниць $\pm\delta, \pm\delta^{-1}$ є нормованою одиницею γ . Тоді $\pm\gamma = \pm\varepsilon^n$, $\pm\gamma^{-1} = \pm\varepsilon^{-n}$. Це означає, що довільна одиниця δ має вигляд $\delta = \pm\varepsilon^n$, де $n \in \mathbb{Z}$. \square

Зауваження 5.3.1. Доведена теорема, означає, що група одиниць дійсного квадратичного поля є прямим добутком циклічної

групи порядку 2 і нескінченної циклічної групи. Вона є частковим випадком важливої у теорії алгебраїчних чисел теореми Діріхле про одиниці, яка стверджує, що група одиниць будь-якого поля алгебраїчних чисел K є прямим добутком скінченної циклічної групи і m екземплярів групи \mathbb{Z} , де $m \geq 0$, m залежить від K . Доведення теореми Діріхле можна знайти у [?].

5.3.5. Обчислення основної одиниці

Ми вже знаємо, що в дійсному квадратичному полі $\mathbb{Q}(\sqrt{d})$ існує така одиниця $\varepsilon > 1$ (її називають *основною*), що кожна інша одиниця дорівнює $\pm\varepsilon^n$ для деякого цілого n . Виявляється, що основну одиницю можна обчислити, використовуючи ланцюгові дроби. Будемо шукати основну одиницю у вигляді $u + v\omega$, де u і v натуральні числа, а ω елемент поля $\mathbb{Q}(\sqrt{d})$, що визначений умовами (5.3.9). Взагалі, якщо δ — будь-яка одиниця, для якої $\delta > 1$ і $\delta = u + v\omega$, то u і v — додатні натуральні числа (крім випадку, коли $d = 5$, де можливий випадок $u = 0, v = 1$). Справді, спряжене до δ число δ' дорівнює або $\frac{1}{\delta}$ або $-\frac{1}{\delta}$, оскільки $N(\delta) = \delta\delta' = \pm 1$. В обох випадках $\delta - \delta' > 0$, тобто $v(\omega - \omega') > 0$, значить, $v > 0$. Далі, оскільки $|\delta'| = |u + v\omega'| < 1$ і $\omega' < -1$ (крім випадку, коли $d = 5$), то $u > -1 - v\omega' > -1 + v \geq 0$, тобто $u > 0$. У випадку $d = 5$, число $\omega = \frac{1+\sqrt{5}}{2}$ є основною одиницею.

Теорема 5.3.9. *Нехай $\frac{P_n}{Q_n}$ — підхідні дроби розкладу числа $-\omega'$ у ланцюговий дріб, $\omega \neq \frac{1+\sqrt{5}}{2}$. Тоді існують такі індекси $n \geq 0$, що елементи $P_n + \omega Q_n$ є одиницями поля $\mathbb{Q}(\sqrt{d})$, а при найменшому такому значенні n одержуємо основну одиницю.*

Доведення. Нехай $\delta = p + q\omega$ — одиниця, і $\delta > 1$. Тоді $|N(\delta)| = |p + q\omega| |p + q\omega'| = 1$. Звідси маємо

$$\left| \frac{p}{q} + \omega' \right| = \frac{1}{q(p + q\omega)}. \quad (5.3.13)$$

a) Нехай $d \equiv 1 \pmod{4}$, $d > 5$. Тоді $\omega = \frac{1}{2}(1 + \sqrt{d})$ і (5.3.13)

можна переписати так:

$$\left| \frac{p}{q} - \frac{\sqrt{d}-1}{2} \right| = \frac{1}{q^2 \left(\frac{p}{q} + \frac{\sqrt{d}+1}{2} \right)},$$

Якщо $d > 5$ і $d \equiv 1 \pmod{4}$, то $d \geq 13$, бо d — вільне від квадратів. Тому $\frac{\sqrt{d}+1}{2} > 1$. Звідси і з $\frac{p}{q} > 0$ отримуємо нерівність

$$\left| \frac{p}{q} - \frac{\sqrt{d}-1}{2} \right| < \frac{1}{2q^2}.$$

За наслідком 5.2.2 звідси випливає, що $\frac{p}{q}$ — підхідний дріб числа $\frac{1}{2}(\sqrt{d}-1)$.

б) Тепер розглянемо випадок $d \equiv 2, 3 \pmod{4}$. Тоді $-\omega' = \sqrt{d} = \omega$ і (5.3.13) можна переписати так:

$$\left| \frac{p}{q} - \sqrt{d} \right| = \frac{1}{q(p+q\sqrt{d})} = \frac{1}{q^2(p/q+\sqrt{d})}. \quad (5.3.14)$$

Нагадаємо, що $p^2 - dq^2 = N(\delta) = \pm 1$. Тому $p^2 - dq^2 \geq -1$, $(\frac{p}{q})^2 - d \geq -\frac{1}{q^2} > -1$, отже, $(\frac{p}{q})^2 > d - 1$ і $\frac{p}{q} > \sqrt{d} - 1$ (у нас $p > 0$, $q > 0$). Використовуючи (5.3.14), маємо оцінку

$$\left| \frac{p}{q} - \sqrt{d} \right| < \frac{1}{q^2(\sqrt{d}-1+\sqrt{d})} < \frac{1}{2q^2},$$

і, за тим же наслідком 5.2.2, $\frac{p}{q}$ є підхідним дробом для \sqrt{d} . Очевидно, що при найменшому n , для якого $P_n + \omega Q_n$ є одиницею (P_n і Q_n — підхідні дроби для $-\omega'$) ми одержимо основну одиницю. \square

Приклад 5.3.3. 1. Знайдемо основну одиницю поля $\mathbb{Q}(\sqrt{7})$. $7 \equiv 3 \pmod{4}$. Тому нам потрібно розкласти $\sqrt{7}$ у ланцюговий дріб і пробувати на роль основної одиниці числа $P_n + \sqrt{7}Q_n$, де P_n, Q_n — чисельник і знаменник підхідного дробу $\frac{P_n}{Q_n}$ відповідно. Ми вже бачили раніше, що $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots]$. Обчислення зручно проводити у вигляді наступної таблиці:

a_n		2	1	1	1	4	1
P_n	1	2	3	5	8		
Q_n	0	1	1	2	3		
$P_n^2 - 7Q_n^2$		-3	2	-3	1		

Обчислюємо доти, поки не одержимо в останньому рядку ± 1 .

Отже, $8 + 3\sqrt{7}$ є основною одиницею поля $\mathbb{Q}(\sqrt{7})$.

2. Знайдемо основну одиницю поля $\mathbb{Q}(\sqrt{17})$. Якщо $\alpha = p + q\frac{\sqrt{17}+1}{2}$, то $N(\alpha) = \alpha\alpha' = (p + q\frac{1+\sqrt{17}}{2})(p + q\frac{1-\sqrt{17}}{2}) = p^2 + pq - 4q^2$. Розкладемо $-\omega' = \frac{\sqrt{17}-1}{2}$ у ланцюговий дріб.

$$\begin{aligned}\frac{\sqrt{17}-1}{2} &= 1 + \frac{\sqrt{17}-3}{2}; \\ \frac{2}{\sqrt{17}-3} &= \frac{\sqrt{17}+3}{4} = 1 + \frac{\sqrt{17}-3}{4}; \\ \frac{4}{\sqrt{17}-1} &= \frac{\sqrt{17}+1}{4} = 1 + \frac{\sqrt{17}-3}{4}; \\ \frac{4}{\sqrt{17}-3} &= \frac{\sqrt{17}+3}{2} = 3 + \frac{\sqrt{17}-3}{2};\end{aligned}$$

Отже, $\frac{\sqrt{17}-1}{2} = [1, \overline{1, 1, 3}]$. Заповнююмо таблицю:

a_n		1	1	1	3	1
P_n	1	1	2	3		
Q_n	0	1	1	2		
$P_n^2 + P_n Q_n - 4Q_n^2$		-2	2	-1		

Ця таблиця показує, що основною одиницею поля $\mathbb{Q}(\sqrt{17})$ є $3 + 2\frac{1+\sqrt{17}}{2} = 4 + \sqrt{17}$.

Зauważення 5.3.2. Може виникнути питання, чи не простіше для обчислення основних одиниць не використовувати апарат ланцюгових дробів, а просто діяти методом перебору, тобто, записавши $\alpha \in \mathcal{O}$ у вигляді $\alpha = u + v\omega$, послідовно перебирати натуральні значення u і v у порядку їх зростання і перевіряти — чи норма одержаного числа дорівнюватиме ± 1 . Однак

цей метод перебору, хоч в принципі завжди приведе до основної одиниці, стає безнадійно довгим вже при не дуже великих значеннях d . Наприклад, при $d = 46$, основна одиниця ε має вигляд $\varepsilon = 24335 + 3588\sqrt{46}$, а при $d = 94$ $\varepsilon = 2143295 + 221064\sqrt{94}$. (див. таблиці, напр., у книзі [?]).

5.4. Вправи

1) Довести, що для ланцюгового дробу $[a_0, a_1, \dots, a_k]$

$$\frac{Q_k}{Q_{k-1}} = [a_k, a_{k-1}, \dots, a_1], \quad k \geq 1,$$

$$\frac{P_k}{P_{k-1}} = [a_k, a_{k-1}, \dots, a_1, a_0], \quad a_0 > 0, k \geq 1.$$

2) *Теорема Діріхле.* Нехай α і Q — дійсні числа, $Q > 1$. Тоді існує ціле число q , таке, що $1 \leq q < Q$ і $\|\alpha q\| < \frac{1}{Q}$. (*Вказівка.* Див. [?], теорема 246, або [?], теорема 1 на ст.9.)

3) Нехай $\frac{p}{q}$ — нескоротний дріб, що міститься в інтервалі, кінцями якого є підхідні дроби $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_n}{Q_n}$, $n \geq 1$. Довести, що $q > Q_n$.

4) Нехай $G = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid \det A = \pm 1\}$.

а) Показати, що G — група відносно множення матриць.

б) Якщо $\sigma \in G$ і $\alpha \in \mathbb{R}$, α — ірраціональне число, то означимо $\sigma\alpha = \frac{a\alpha+b}{c\alpha+d}$. Показати, що $\sigma(\tau\alpha) = (\sigma\tau)\alpha$ і $e(\alpha) = \alpha$, де $\sigma, \tau \in G$, e — нейтральний елемент групи G .

в) Назведемо два ірраціональні числа α і β еквівалентними, якщо існує $\sigma \in G$ таке, що $\sigma\alpha = \beta$. Показати, що це справді відношення еквівалентності.

г) Нехай α, β — ірраціональні числа і $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $\alpha = \sigma\beta = \frac{a\beta+b}{c\beta+d}$. Нехай, крім того, $\beta > 1$, $c > d > 0$. Тоді $\frac{b}{d}$ і $\frac{a}{c}$ — два послідовні підхідні дроби до α .

- 5) Нехай α — редукована квадратична ірраціональність, $\alpha = [a_0, a_1, \dots, a_{k-1}]$. Довести, що $-\frac{1}{\alpha'} = [\overline{a_{k-1}, \dots, a_1, a_0}]$. (*Вказівка.* Див. [?], ст.328.)

- 6) (Вален (1895)) Нехай $\frac{P_{n-1}}{Q_{n-1}}$, $\frac{P_n}{Q_n}$ — два послідовні підхідні дроби для дійсного числа α . Довести, що хоч один з них задовольняє нерівність $|\alpha - \frac{P}{Q}| < \frac{1}{2Q^2}$.

- 7) (Е.Борель (1903)). Нехай $\frac{P_{n-2}}{Q_{n-2}}$, $\frac{P_{n-1}}{Q_{n-1}}$, $\frac{P_n}{Q_n}$ — три послідовні підхідні дроби для дійсного числа α . Довести, що хоч один з них задовольняє нерівність $|\alpha - \frac{P}{Q}| < \frac{1}{\sqrt{5}Q^2}$.

Вказівка. Нехай α_{n+1} — залишок для α . Довести, що

$$\left| \alpha - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})} = \frac{1}{Q_n^2(\alpha_{n+1} + \beta_{n+1})},$$

де $\beta_{n+1} = \frac{Q_{n-1}}{Q_n}$. Показати, що не існує трьох цілих чисел $i = n-1, n, n+1$, для яких виконується нерівність $\alpha_i + \beta_i < \sqrt{5}$. Для цього, якщо $\alpha_{n-1} + \beta_{n-1} < \sqrt{5}$, то показати, що $\alpha_n^{-1} + \beta_n^{-1} \leq \sqrt{5}$. Вивести звідси, що β_n задовольняє нерівність $\beta_n^2 - \sqrt{5}\beta_{n+1} \leq 0$, отже, $\beta_n > \frac{1}{2}(\sqrt{5} - 1)$, звідси

$$1 \leq a_n = \frac{Q_n}{Q_{n-1}} - \frac{Q_{n-2}}{Q_{n-1}} = \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} = 1.$$

Суперечність.

- 8) Кажуть, що ірраціональне число α *погано наближаеться раціональними числами*, якщо існує константа $c = c(\alpha) > 0$ така, що $|\alpha - \frac{p}{q}| > \frac{c}{q^2}$ для кожного раціонального числа $\frac{p}{q}$. В протилежному випадку кажуть, що α *добре наближаеться раціональними числами*. Довести, що дійсне число α погано наближається раціональними числами тоді і тільки тоді, коли неповні частки a_n його розкладу в ланцюговий дріб обмежені: $|a_n| < K$ для всіх $n \in \mathbb{N}$. (*Вказівка.* Довести нерівність

$$\frac{1}{Q_n^2(a_{n+1} + 2)} \leq \left| \alpha - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n^2 a_{n+1}}.$$

9) Довести, що множина дійсних чисел, які добре наближаються раціональними, має потужність континуум і множина чисел, які погано наближаються, теж має потужність континуум.

10) *Трансцендентні числа Рота.* У п.5.2.4 ми згадували теорему Рота. Вона полягає в тому, що для алгебраїчного числа α степеня $n \geq 2$ і для кожного $\varepsilon > 0$ існує константа $c > 0$ така, що нерівність $|\alpha - \frac{p}{q}| < \frac{c}{q^{2+\varepsilon}}$ не має розв'язків в цілих числах $p \in \mathbb{Z}$ і $q \in \mathbb{N}$.

а) Нехай для дійсного числа α для кожного $c > 0$ існує раціональне число $\frac{p}{q}$ ($\frac{p}{q} \neq \alpha$) таке, що

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^2 + \varepsilon},$$

де ε — дійсне число, $\varepsilon > 0$. Вивести з теореми Рота, що α — трансцендентне число.

б) Використовуючи а), довести трансцендентність числа $\alpha = \sum_{n=1}^{\infty} \frac{(-1)^n}{2^{3^n}}$.

11) Розв'язати конгруенції: а) $1710x \equiv 49 \pmod{997}$; б) $262x \equiv 100 \pmod{998}$; в) $997x \equiv 1661 \pmod{999}$.

12) Знайти всі розв'язки діофантових рівнянь: а) $482x - 577y = 1$; б) $2103x - 1249y = 5$; в) $3035x - 4010y = 77$.

13) Показати, що в уявних квадратичних полях $\mathbb{Q}(\sqrt{d})$, $d < 0$, група одиниць збігається з групою C_n коренів n -го степеня з одиницею, де n має значення

$$n = 6 \text{ для } d = -3,$$

$$n = 4 \text{ для } d = -1,$$

$n = 2$ в інших випадках.

(Вказівка. Використати теорему 5.3.6. Одиниці шукати у вигляді $\frac{u+v\sqrt{d}}{2}$.)

- 14) Показати, що кільця цілих елементів у квадратичних полях $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{10})$ не є факторіальними. Для цього перевірити, що в рівностях

$$\begin{aligned}2 \cdot 3 &= \sqrt{-6} \cdot (-\sqrt{-6}), \\3 \cdot 7 &= (4 + \sqrt{-5})(4 - \sqrt{-5}), \\2 \cdot 5 &= \sqrt{10} \cdot \sqrt{10}\end{aligned}$$

кожний множник є простим елементом у відповідному кільці цілих елементів і, що числа з правих частин не асоційовані з числами з лівих частин цих рівностей.

- 15) Якщо в кільці цілих квадратичного поля $\mathbb{Q}(\sqrt{d})$ для кожної пари елементів $\alpha \neq 0, \beta$ з $|N(\beta)| \geq |N(\alpha)|$ існує елемент γ такий, що

$$|N(\beta - \gamma\alpha)| < |N(\beta)|.$$

то це кільце факторіальне.

- 16) Довести, що кільця цілих елементів квадратичних полів $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ факторіальні.

- 17) Показати, що кільце цілих елементів квадратичного поля $\mathbb{Q}(\sqrt{5})$ є факторіальним, а кільце $\mathbb{Z}[\sqrt{5}]$ не факторіальне.

- 18) Обчислити основну одиницю наступних квадратичних полів: а) $\mathbb{Q}(\sqrt{11})$; б) $\mathbb{Q}(\sqrt{23})$; в) $\mathbb{Q}(\sqrt{41})$; г) $\mathbb{Q}(\sqrt{59})$.

- 19) Нехай α — редуковане число з $\mathbb{Q}(\sqrt{d})$, що має дискримінант \mathcal{D} , де

$$\mathcal{D} = \begin{cases} d, & d \equiv 1 \pmod{4}, \\ 4d, & d \equiv 2, 3 \pmod{4}, \end{cases}$$

k — період ланцюгового дробу для α , v — найбільший спільний дільник чисел Q_{k-1} , $P_{k-1} - Q_{k-2}$, P_{k-2} і $u = P_{k-1} + Q_{k-2}$. Тоді $\varepsilon = \frac{u+v\sqrt{\mathcal{D}}}{2}$ є одиницею, $\varepsilon > 1$, $N(\varepsilon) = (-1)^k$.

Вказівка. $\alpha = [a_0, a_1, \dots, a_{k-1}, \alpha] = \frac{P_{k-1}\alpha + P_{k-2}}{Q_{k-1}\alpha + Q_{k-2}}$. Отже, α є коренем квадратного рівняння

$$Q_{k-1}x^2 + (Q_{k-2} - P_{k-1})x - P_{k-2} = 0.$$

Якщо $Q_{k-1} = av$, $Q_{k-2} - P_{k-1} = bv$, $-P_{k-2} = cv$ і $u = P_{k-1} + Q_{k-2}$, то виразивши P_{k-1} , P_{k-2} , Q_{k-1} , Q_{k-2} через u і v , з рівності $P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2} = (-1)^k$ можна одержати $u^2 - \mathcal{D}v^2 = (-1)^k$.)

Список літератури

1. *Бухштаб А.А.* Теория чисел.- М.: Просвещение, 1966.
2. *Ван дер Варден Б.Л.* Алгебра. - М.: Наука, 1976.-623с.
3. *Виноградов И.М..* Основы теории чисел. - М.: Наука, 1972.
4. *Завало С.Т.* Курс алгебри. - К.: Вища школа, 1985.-500с.
5. *Калужнін Л.А., Вишенисъкий В.А., Шуб Ц.О.* Лінійні простори. - К.: Вища школа, 1971.-343с.
6. *Кострикін А.І.* Введение в алгебру. - М.: Наука, 1977.-495с.
7. *Кострикін А.І., Манин Ю.І.* Линейная алгебра и геометрия. - М.: Изд.-во Моск. ун-та, 1980.-319с.
8. *Курош А.Г.* Курс высшей алгебры. - М.: Наука, 1971.-431с.
9. *Мальцев А.А.* Основы линейной алгебры. - М.: Наука, 1975.-400с.
10. *Чарін В.С.* Лінійна алгебра. - К.: Техніка, 2004.-414с.
11. *Стренг Г.* Линейная алгебра и ее применения. - М.: Мир, 1980.-454с.
12. *Фаддеев Д.К.* Лекции по алгебре. - М.: Наука, 1984.-415с.

Зміст

\succ	2
Розділ 1. Основні алгебраїчні структури	7
1.1. Множини та відношення	7
1.1.1. Означення та приклади відношень (8). 1.1.2. Відношення еквівалентності (9). 1.1.3. Розбиття та відношення еквівалентності (11). 1.1.4. Функціональні відношення та відображення (13). 1.1.5. Добуток відображень (14). 1.1.6. Однічне та обернене відображення (16).	
1.2. Алгебраїчна операція	17
1.2.1. Означення та приклади алгебраїчних операцій (17). 1.2.2. Асоціативність. Напівгрупа та моноїд (18). 1.2.3. Обернений елемент. Група (20). 1.2.4. Підгрупа. Критерій підгрупи (24). 1.2.5. Циклічні підгрупи та групи (25). 1.2.6. Порядок елемента групи (26).	
1.3. Групи підстановок	27
1.3.1. Найпростіші властивості групи підстановок (27). 1.3.2. Цикли та орбіти (28). 1.3.3. Розклад підстановки в добуток циклів (29). 1.3.4. Розклад підстановки в добуток транспозицій (30). 1.3.5. Парні та непарні підстановки (31). 1.3.6. Розклад і парність підстановок (32).	
1.4. Гомоморфізми, суміжні класи та фактор-групи	33

1.4.1. Гомоморфізми півгруп та груп (33).	1.4.2. Суміжні класи (35).	1.4.3. Теорема Лагранжа (38).	1.4.4. Розбиття групи, узгоджені з операцією (38).	1.4.5. Фактор-група (40).
1.4.6. Теорема про гомоморфізми (42).				
1.5. Кільця та поля	43			
1.5.1. Означення та приклади кілець.	Наслідки з аксіом			
(43).	1.5.2. Підкільця та ідеали.	Суміжні класи за ідеалом		
(44).	1.5.3. Фактор-кільце (46).	1.5.4. Кільце $\mathbb{Z}/n\mathbb{Z}$ (47).		
1.5.5. Поле (49).	1.5.6. Гомоморфізми кілець та полів (50).			
1.6. Матриці	51			
1.6.1. Означення (51).	1.6.2. Лінійні операції над матрицями (52).			
1.6.3. Добуток матриць (53).	1.6.4. Одинична та транспонована матриці (56).	1.6.5. Кільце матриць (58).		
1.7. комплексні числа	58			
1.7.1. Поле комплексних чисел (58).	1.7.2. Алгебраїчна форма комплексних чисел (61).	1.7.3. Геометрична інтерпретація (62).	1.7.4. Модуль та аргумент (62).	1.7.5. Тригонометрична форма комплексного числа (65).
1.7.6. Формула Muавра (66).	1.7.7. Корені з комплексних чисел (67).	1.7.8. Корені з 1.	Група C_n (68).	1.7.9. Первісні корені з 1 (69).
1.8. Вправи	70			
Розділ 2. Системи лінійних рівнянь та визначники	75			
2.1. n -вимірний векторний простір	75			
2.1.1. Вектори та лінійні операції над ними (75).	2.1.2. Лінійна залежність (76).	2.1.3. Леми про лінійну залежність (78).		
2.1.4. Підпростори.	База підпростору (79).	2.1.5. Теореми про базу (81).		
2.2. Системи лінійних рівнянь	84			
2.2.1. Елементарні перетворення матриць (84).	2.2.2. Еквівалентні системи лінійних рівнянь (86).	2.2.3. Аналіз можливих випадків (89).	2.2.4. Лема Гаусса (90).	
2.3. Визначники	91			

2.3.1. Аксіоматичне означення визначника (91).	2.3.2. Найпростіші властивості визначників (92).	2.3.3. Основна формула аксіоматичної теорії визначників (94).	2.3.4. Єдиність визначника (95).	2.3.5. Визначник транспонованої матриці та визначник добутку матриць (95).	2.3.6. Існування визначника n -го порядку (97).	2.3.7. Один практичний метод обчислення визначників (99).
2.4. Мінори, алгебраїчні доповнення	100					
2.4.1. Мінори та алгебраїчні доповнення (100).	2.4.2. Лема про добуток мінора на алгебраїчне доповнення (101).	2.4.3. Теорема Лапласа (102).	2.4.4. Розклад визначника за рядком (103).			
2.5. Застосування визначників	104					
2.5.1. Обернена матриця (104).	2.5.2. Теорема про ранг матриці (106).	2.5.3. Теорема Кронекера-Капеллі (108).	2.5.4. Формули Крамера (110).	2.5.5. Рангові та вільні невідомі системи лінійних рівнянь (111).	2.5.6. Фундаментальна система розв'язків (112).	
2.6. Вправи	114					
Розділ 3. Поліноми та евклідові кільця	119					
3.1. Кільця поліномів	119					
3.1.1. Означення. Операції над поліномами (119).	3.1.2. Поліноми як функції (121).	3.1.3. Ділення з остачею (124).				
3.1.4. Узагальнення на випадок поліномів над областями цілісності (126).	3.1.5. Теорема Безу та схема Горнера (126).					
3.2. Евклідові кільця	128					
3.2.1. Ділення в кільцях. Дільники одиниці та прості елементи (128).	3.2.2. Означення та приклади евклідових кілець (131).	3.2.3. Алгоритм Евкліда знаходження Н.С.Д. в евклідових кільцях (132).	3.2.4. Поняття про факторіальне кільце (134).	3.2.5. Факторіальність евклідових кілець (136).	3.2.6. Кільце цілих чисел \mathbb{Z} (138).	

3.3. Поліноми над факторіальними кільцями	139
3.3.1. Поле дробів (139). 3.3.2. Лема Гауса про примітивні поліноми (141). 3.3.3. Незвідні поліноми (142). 3.3.4. Факторіальність кілець поліномів (145).	
3.4. Корені поліномів	146
3.4.1. Похідна полінома та кратні корені (146). 3.4.2. Спільний множник двох поліномів. Результант (150). 3.4.3. Результант однорідних поліномів (152). 3.4.4. Основна теорема алгебри (153). 3.4.5. Формули Вієта (155).	
3.5. Вправи	156
Розділ 4. Класи лишків та їх застосування	163
4.1. Кільце $\mathbb{Z}/n\mathbb{Z}$	163
4.1.1. Означення кільця класів лишків. Скінченні поля (163). 4.1.2. Поле \mathbb{F}_p (165). 4.1.3. Мультиплікативна група скінченного поля (165). 4.1.4. функція Ойлера (167). 4.1.5. Теореми Ойлера та Ферма (169). 4.1.6. Теорема Вільсона (171). 4.1.7. Суми квадратів (171).	
4.2. Конгруенції	174
4.2.1. Конгруенції та діофантові рівняння (174). 4.2.2. Рівняння над полем $\mathbb{Z}/p\mathbb{Z}$ (конгруенції за $\text{mod } p$) (177). 4.2.3. Конгруенції за модулем p^n (180). 4.2.4. Конгруенції за модулем t (183). 4.2.5. Двочленні конгруенції за $\text{mod } p$ (185).	
4.3. Квадратичний закон взаємності	187
4.3.1. Символ Лежандра (187). 4.3.2. Лема Гауса (188). 4.3.3. Властивості символу Лежандра (189). 4.3.4. Закон взаємності (190). 4.3.5. Деякі застосування закону взаємності (193). 4.3.6. Шифри з відкритим ключем (197).	
4.4. Вправи	199

Розділ 5. Ланцюгові дроби та їх застосування	205
5.1. Ланцюгові дроби	205
5.1.1. Скінченні ланцюгові дроби (205). 5.1.2. Підхідні дроби ланцюгового дробу (207). 5.1.3. Означення нескінченних ланцюгових дробів (211). 5.1.4. Підхідні дроби нескінченних ланцюгових дробів (213). 5.1.5. Квадратичні ірраціональності ланцюгові дроби	та (218).
5.2. Діофантові наближення	226
5.2.1. Порядок наближення дійсних чисел раціональними (226). 5.2.2. Найкращі наближення та ланцюгові дроби (229). 5.2.3. Теорема Ліувілля (233). 5.2.4. Діофантові наближення та діофантові рівняння	та (237).
5.3. Застосування ланцюгових дробів	241
5.3.1. Розв'язування конгруенцій першого степеня (241). 5.3.2. Розв'язування діофантових рівнянь $aX+bY = c$ (242). 5.3.3. Кільце цілих чисел квадратичного поля (244). 5.3.4. Одиниці у квадратичних полях (248). 5.3.5. Обчислення основної одиниці	(253).
5.4. Вправи	256