МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
імені МИХАЙЛА ДРАГОМАНОВА

Наталія ВЕРПАТОВА

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ.
ОСНОВНІ ФАКТИ ТА АЛГОРИТМИ

(ДИДАКТИЧНІ МАТЕРІАЛИ
ДЛЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ)

КИЇВ – 2023

УДК 511.2 (075.8)

Наталія ВЕРПАТОВА. Алгебра і теорія чисел. Основні факти та алгоритми (дидактичні матеріали для самостійної роботи студентів). К.: УДУ імені Михайла Драгоманова, 2023. 130 с.

Рецензенти:
Анатолій ПЕТРАВЧУК, доктор фізико-математичних наук, професор, завідувач кафедри алгебри і комп'ютерної математики Київського національного університету імені Тараса Шевченка,
Катерина БОЖОНОК, кандидат фізико-математичних наук, доцент кафедри вищої математики Українського державного університету імені Михайла Драгоманова.

Рекомендовано Вченою радою
Українського державного університету імені Михайла Драгоманова
(*протокол* № 4 *від* 30 *листопада* 2023 *року*)

В посібнику представлено методи розв'язування основних задач курсу „Алгебра і теорія чисел" та теоретичний матеріал, необхідний для їх обґрунтування, наведено орієнтовний план практичних занять, завдання для контрольних робіт та перевірки знань.

Навчальний посібник розрахований на студентів закладів вищої освіти, які навчаються за спеціальностями „Інформатика", „Фізика", викладачів, вчителів закладів загальної середньої освіти з поглибленим вивченням математики.

1 ВІДНОШЕННЯ НА МНОЖИНАХ. ВІДНОШЕННЯ ЕКВІВАЛЕНТНОСТІ

Поняття множини – одне з основних понять сучасної математики. Як і кожне основне математичне поняття, воно не означується. Множину розуміємо як сукупність деяких об’єктів, об’єднаних за якою-небудь ознакою або за яким-небудь правилом. Рівнозначними терміну „множина” є терміни „сукупність”, „клас”, „система” та ін. (клас парних чисел, система векторів тощо).

Об’єкти, які утворюють дану множину, називають *елементами* цієї множини. Множини позначають великими латинськими буквами A, B, C, ..., X, Y, Z, а їх елементи – малими латинським буквами a, b, c, ..., x, y, z.

Якщо a є елементом множини M, то записують $a \in M$.

Множину вважають заданою, якщо про кожний об’єкт можна сказати, чи є він елементом цієї множини, чи ні. Множину можна визначити заданням характеристичної властивості її елементів, або переліком всіх її елементів. Те, що множина M складається з елементів a, b, c записують так:

$$M = \{ a, b, c \}.$$

Іноді може не існувати об’єктів, які мали б задану характеристичну властивість. Множину, яка не має жодного елемента, називають *порожньою множиною* і позначають символом $\varnothing$.

Означення. Множини A і B називають *рівними* (записують: $A = B$), якщо вони складаються з тих самих елементів, тобто якщо кожний елемент множини A є елементом множини B і, навпаки, кожний елемент множини B є елементом множини A.

Означення. Якщо кожний елемент множини A є елементом і множини B, то говорять, що A є *підмножиною* множини B, і записують $A \subseteq B$.

Твердження 1. *Дві множини рівні тоді і тільки тоді, коли кожна з них є підмножиною другої:*

$$A = B \iff (A \subseteq B \text{ і } B \subseteq A).$$

Означення. Якщо кожен елемент множини A є елементом множини B, але в множині B є принаймні один елемент, який не входить до A, то A називають *правильною* (або *власною*) підмножиною множини B і записують $A \subset B$.

Порожню множину і множину A називають *невласними* підмножинами множини A.

Операції над множинами

Нехай A і B – довільні множини.

Означення. *Об’єднанням множин* A і B називають множину S, яка складається з усіх елементів, що належать принаймні одній з цих множин (тобто або множині A, або множині B, або обом множинам), і записують $S = A \cup B$.

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

Означення. *Різницею множин* A і B називають множину T, яка складається з усіх тих елементів множини A, які не належать множині B, і записують $T = A \setminus B$.

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

Означення. *Перетином множин* A і B називають множину D, що складається з усіх елементів, які належать як множині A, так і множині B, і записують $D = A \cap B$.

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

Поняття об'єднання і перетину двох множин можна поширити на випадок будь-якої кількості множин.

Відношення на множинах

Означення. Нехай A і B – дві множини довільної природи, скінченні або нескінченні. Множину всіх впорядкованих пар (a, b), де $a \in A, b \in B$, називають *прямим* (або *декартовим*) *добутком* множин A і B, позначають $A \times B$:

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

Означення. *Бінарним відношенням* ρ, визначеним у множинах A, B, називають кожну непорожню підмножину прямого добутку $A \times B$, тобто

$$\rho \subseteq \{\ (a, b) \mid\ a \in A, b \in B\ \}.$$

Те, що елементи a і b перебувають у відношенні ρ, записують так:

$$(a, b) \in \rho \quad \text{або} \quad a\,\rho\,b\,.$$

Якщо $A = B$, то кажуть, що бінарне відношення ρ визначене у множині A, тобто $\rho \subseteq A \times A$.

Приклади бінарних відношень:
1) відношення паралельності $a \parallel b$ на множині A всіх прямих площини;
2) відношення перпендикулярності $a \perp b$ на множині A всіх прямих площини;
3) відношення рівності $a = b$ на множині $\mathbf{Z}$ всіх цілих чисел;
4) відношення менше $a < b$ на множині $\mathbf{Z}$ всіх цілих чисел.

***Властивості бінарних відношень*:**

Бінарне відношення ρ, визначене в множині A, називають

1) *рефлексивним*, якщо $\forall\ a \in A \quad a\,\rho\,a$, тобто $(a, a) \in \rho$;

2) *антирефлексивним*, якщо $\forall\ a \in A \quad a\,\overline{\rho}\,a$, тобто $(a, a) \notin \rho$;

3) *симетричним*, якщо $\forall\ a, b \in A \quad a\,\rho\,b \ \Rightarrow\ b\,\rho\,a$, тобто

$$(a, b) \in \rho \ \Rightarrow\ (b, a) \in \rho\,;$$

4) *асиметричним*, якщо $\forall\ a, b \in A \quad a\,\rho\, b \ \Rightarrow\ b\ \overline{\rho}\ a$, тобто

$$(a, b) \in \rho \ \Rightarrow\ (b, a) \notin \rho\,;$$

5) *антисиметричним*, якщо $\forall\ a, b \in A \quad (\ a\,\rho\, b \ \text{ і } \ b\,\rho\, a\ ) \ \Rightarrow\ a = b$, тобто

$$\begin{cases}(a,b)\in\rho\\(b,a)\in\rho\end{cases} \Rightarrow\quad a=b\,;$$

6) *транзитивним*, якщо $\forall\ a, b, c \in A \quad (\ a\,\rho\, b \ \text{ і } \ b\,\rho\, c\ ) \ \Rightarrow\ a\,\rho\, c$, тобто

$$\begin{cases}(a,b)\in\rho\\(b,c)\in\rho\end{cases} \Rightarrow\quad (a,c)\in\rho.$$

Означення. Бінарне відношення ρ, визначене на множині A, називають *відношенням порядку*, якщо воно антисиметричне і транзитивне. При цьому *відношенням строгого порядку*, якщо воно антирефлексивне, і *нестрогого порядку*, якщо воно рефлексивне.

Якщо на множині A визначене відношення порядку, то A називають *упорядкованою множиною*.

Означення. Бінарне відношення ρ, визначене в множинах A і B, називають *функціональним*, якщо

$$\forall\ \ a \in\ A \quad \exists!\ \ b \in\ B: \qquad (a, b) \in \rho\,.$$

Отже, бінарне функціональне відношення має такі властивості:

1) воно всюди визначене на множині A, тобто $D(\rho) = A$;

2) друга компонента пари (a, b) визначається однозначно.

Синонімами функціонального відношення вважаємо терміни: функція, відображення. В алгебрі замість слова “функція” вживають слово “операція”.

Відношення еквівалентності

Означення. Бінарне відношення ρ, визначене на множині A, називають *відношенням еквівалентності*, якщо воно є рефлексивним, симетричним і транзитивним.

Наприклад, відношеннями еквівалентності є відношення паралельності прямих, рівності та подібності геометричних фігур, рівності чисел і т.п.

Означення. Нехай ρ – відношення еквівалентності на множині A і a – деякий елемент множини A. Тоді множину елементів з A, які перебувають у відношенні ρ з елементом a, називають *класом еквівалентності* за відношенням ρ, породженим елементом a, і позначають a/ρ:

$$a/\rho = \{\ x \mid x \in A, \quad x\,\rho\, a\ \}\,.$$

Наприклад, ρ – відношення "мати однакову остачу від ділення на 3" на множині $\mathbf{Z}$ цілих чисел є відношенням еквівалентності. Тоді клас еквівалентності, породжений числом 2, складають всі числа, що мають вигляд $3k+2$, де $k \in \mathbf{Z}$:

$$2/\rho = \{\, 2+3k \mid k \in \mathbf{Z}\}.$$

Теорема 1.1. *Будь-які два класи еквівалентності за відношенням* ρ*, що мають, принаймні, один спільний елемент, збігаються.*

Наслідок 1. *Будь-які два різні класи еквівалентності за відношенням* ρ *не перетинаються.*

Наслідок 2. *Кожен елемент* $a \in A$ *міститься в одному і тільки в одному класі еквівалентності за відношенням* ρ.

Нехай a/ρ – довільно вибраний клас еквівалентності за відношенням ρ, c – будь-який елемент цього класу. Елемент c визначає клас еквівалентності c/ρ, але, за теоремою 1.1, $c/\rho = a/\rho$. Отже, *кожен клас еквівалентності* a/ρ *визначається будь-яким своїм елементом* c. Тому будь-який елемент даного класу еквівалентності називають *представником* цього класу.

Означення. Множину всіх класів еквівалентності множини A за відношенням ρ називають *фактор-множиною* множини A за еквівалентністю ρ і позначають A/ρ.

Означення. *Розбиттям* множини A називають сукупність S непорожніх підмножин X_i множини A, які попарно не перетинаються і об'єднання яких збігається з множиною A. Тобто

1) $\forall\ X_i \in \mathsf{S} \qquad X_i \neq \varnothing$,
2) $\forall\ X_i, X_j \in \mathsf{S} \qquad X_i \cap X_j = \varnothing \quad (i \neq j)$,
3) $\bigcup\limits_i X_i = A$.

Підмножини, з яких складається сукупність S, називають *суміжними класами*, або *класами розбиття* S.

Наприклад, множину цілих чисел $\mathbf{Z}$ можна розбити на два класи X_1 та X_2, де X_1 – множина парних цілих чисел, X_2 –множина непарних цілих чисел.:

$$\mathbf{Z} = \{2k\} \cup \{2k+1\}.$$

З означення розбиття випливає, що кожен елемент $a \in A$ міститься в одному і тільки одному класі розбиття.

Теорема 1.2. *Якщо ρ є відношенням еквівалентності на непорожній множині A, то множина класів еквівалентності за відношенням ρ є розбиттям множини A.*

Теорема 1.3. *Кожне розбиття $\mathbf{S}$ множини A визначає на A єдине відношення еквівалентності ρ, класи еквівалентності якого збігаються з підмножинами розбиття.*

Приклад 1.1. *Перевірити, які властивості має відношення "$\vdots$" подільності на множині $\mathbf{N}$ натуральних чисел.*

Нехай a, b – елементи деякої множини A. Вважають, що a *ділиться на* b *в множині* A (записують $a \vdots b$), якщо в множині A знайдеться такий елемент q, що виконується рівність $a = bq$.

Наприклад, в множині $2\mathbf{Z}$ всіх парних чисел $16 \vdots 2$, а $10 \not\vdots 2$.

1) На множині натуральних чисел відношення "$\vdots$" є рефлексивним, оскільки $\forall a \in \mathbf{N} \quad a \vdots a$, тому що $a = a \cdot 1, \; 1 \in \mathbf{N}$.

2) Якщо відношення є рефлексивним, то воно не може бути анти-рефлексивним.

3) Відношення "$\vdots$" не є симетричним, оскільки висловлення

$$\forall a, b \in \mathbf{N} \quad a \vdots b \;\Rightarrow\; b \vdots a$$

невірне. Наприклад, $6 \vdots 2$, але $2 \not\vdots 6$.

4) Проте це відношення не є і асиметричним, бо знайдуться такі натуральні числа a, b, для яких одночасно $a \vdots b$ і $b \vdots a$.

Це буде в тому випадку, коли $a = b$.

5) Отже відношення "$\vdots$" є антисиметричним, оскільки для нього виконується висловлення:

$$\forall a, b \in \mathbf{N} \quad (a \vdots b \text{ і } b \vdots a) \;\Rightarrow\; a = b.$$

6) Перевіримо, чи буде відношення "$\vdots$" транзитивним.

Нехай a, b, c – довільні натуральні числа, причому $a \vdots b$ і $b \vdots c$. Це означає, що число a можна представити у вигляді $a = b \cdot q$, де $q \in \mathbf{N}$. В той же час $b = c \cdot r, \; r \in \mathbf{N}$. Тоді

$$a = b \cdot q = (c \cdot r) \cdot q = c \cdot (r \cdot q) = c \cdot s,$$

де $s = r \cdot q \in \mathbf{N}$. Отже, $a \vdots c$.

Таким чином для відношення "$\vdots$" виконується висловлення:

$$\forall a, b, c \in \mathbf{N} \quad (a \vdots b \text{ і } b \vdots c) \;\Rightarrow\; a \vdots \text{c},$$

і відношення "$\vdots$" є транзитивним.

Отже, відношення подільності "$\vdots$" на множині $\mathbf{N}$ натуральних чисел є рефлексивним, антисиметричним і транзитивним. Це відношення є відношенням нестрогого порядку.

Приклад 1.2. Як зазначалося, відношення ρ – „мати однакову остачу від ділення на 3” – на множині цілих чисел $\mathbf{Z}$ є відношенням еквівалентності. *Побудувати фактор множину* Z/ρ .

Візьмемо довільний елемент з множини $\mathbf{Z}$, наприклад 0. Тоді за означенням класу еквівалентності

$$0/\rho = \{3k \mid k \in \mathbf{Z}\}.$$

Тобто в клас еквівалентності, породжений числом 0, ввійшли всі числа, кратні 3.

Візьмемо якийсь інший елемент з множини $\mathbf{Z}$. Зрозуміло, що брати елементи, які вже ввійшли до класу $0/\rho$ недоцільно, оскільки будемо знову отримувати той же клас $0/\rho$. Тому візьмемо, наприклад, 1:

$$1/\rho = \{3k+1 \mid k \in \mathbf{Z}\}.$$

Аналогічно, побудуємо клас

$$2/\rho = \{3k+2 \mid k \in \mathbf{Z}\}.$$

Бачимо, що об'єднання цих класів дасть всю множину $\mathbf{Z}$, тому процес побудови класів фактор-множини Z/ρ закінчився.

Тобто

$$Z/\rho = \left\{0/\rho,\ 1/\rho,\ 2/\rho\right\} = \{\ \{3k\},\ \{3k+1\},\ \{3k+2\}\ \}.$$

2 НАТУРАЛЬНІ ЧИСЛА. АКСІОМИ ПЕАНО. ПРИНЦИП МАТЕМАТИЧНОЇ ІНДУКЦІЇ

Натуральні числа використовують для двох головних цілей – для *лічби* і для *впорядкування.*

Найпростішими конкретними представниками цих чисел є ряди рисочок

$$|,\ ||,\ |||,\ ||||,\ \ldots$$

Перелічуючи (скінчену) множину об'єктів, ми кожному об'єкту ставимо у відповідність деяку рисочку, тобто встановлюємо взаємно однозначну відповідність між даною множиною і множиною рисочок. Впорядковуючи множину, ми нумеруємо всі її елементи у відповідності з послідовністю рисочок як перший, другий, третій і т.д. Основні властивості натуральних чисел можуть бути описані і вивчені з будь-якої з цих двох точок зору. Причому перша приводить до теорії *кардинальних* чисел в теорії множин (Г. Кантор), за якою натуральне число – це клас рівнопотужних множин, друга – до теорії *порядкових* чисел (Дж. Пеано).

Згідно другої, натуральні числа розглядають як об'єкти, які можна порівнювати за допомогою деякого відношення порядку. Найпростіше таке відношення – відношення „*a безпосередньо передує b*", або „*b безпосередньо слідує за a*". В інтерпретації рисочками це означає, що b можна отримати з a шляхом приєднання однієї рисочки. Будемо говорити „*b слідує за a*" і записувати

$$b = a'.$$

Очевидно, цим задали функцію (операцію), визначену на множині всіх натуральних чисел. Якими ж основними властивостями вона володіє?

Насамперед, існує натуральне число, яке позначимо 1, що не слідує ні за яким натуральним числом. По-друге, кожне натуральне число b, відмінне від 1, слідує за єдиним натуральним числом a, тобто якщо $b = a_1{}'$ і $b = a_2{}'$, то $a_1 = a_2$; іншими словами, функція безпосереднього слідування " $'$ " взаємно однозначна. Нарешті, легко бачити, що застосовуючи функцію " $'$ " достатню кількість разів, будь-яке натуральне число можна отримати з 1. В більш точних теоретико-множинних термінах останнє означає, що якщо множина A містить число 1 і разом з кожним x число x', то A містить всі натуральні числа.

Вперше чітко виділив систему основних понять: поняття натурального числа, поняття безпосереднього слідування одного числа за іншим в натуральному ряді, поняття початкового елемента натурального ряду (за який можна прийняти 0 або 1), і сформулював аксіоми, що пов`язують ці поняття італійський математик **Джузеппе Пеано** (1858 – 1932) в 1889 році.

Отже, *первинними термінами* теорії натуральних чисел є:

N – множина натуральних чисел, або *натуральний ряд*;

1 – *одиниця* – елемент множини **N**;

$'$ – *безпосереднє слідування* – унарна операція в **N**.

Ці поняття пов'язані між собою п'ятьма аксіомами, які можна розглядати як аксіоматичне означення системи натуральних чисел.

Аксіоми Пеано:

n₁) 1 є натуральним числом

$$1 \in \mathbf{N};$$

n₂) наступне за натуральним числом є число натуральне

$$\forall\, a \in \mathbf{N} \qquad a' \in \mathbf{N};$$

n₃) 1 не слідує ні за яким натуральним числом

$$\forall\, a \in \mathbf{N} \qquad a' \neq 1;$$

n₄) $\forall\, a, b \in \mathbf{N} \qquad a' = b' \;\Rightarrow\; a = b$;

n₅) **Аксіома індукції**.

Якщо деяка підмножина $M \subset \mathbf{N}$ має властивості:

а) $1 \in M$, б) $\forall\, a \quad a \in M \;\Rightarrow\; a' \in M$,

то $M = \mathbf{N}$.

Відношення порядку на множині N

Означення. Натуральне число a називають *меншим* за натуральне число b (і записують $a < b$), якщо існує таке натуральне число v, що виконується рівність:

$$b = a + v.$$

Число b в цьому випадку називають *більшим* за натуральне число a і записують $b > a$.

Якщо $\overline{a < b}$, то кажуть, що "число a *більше або дорівнює* b" або "число b *менше або дорівнює* a". Записують $a \geq b$ або $b \leq a$.

Твердження1. Відношення «менше» на множині натуральних чисел є антирефлексивним та транзитивним, тобто є відношенням строгого порядку.

Наступне твердження наводить властивості відношення «менше», які пов'язують його з відношенням «безпосереднього слідування» та одиницею.

Твердження 2. *Для довільних натуральних чисел* a, b *справедливі співвідношення*:

1) $1 \leq a$;

2) $a < b' \;\Leftrightarrow\; a \leq b$.

3) $b < b'$ *і не існує такого натурального числа* c, *для якого* $b < c < b'$.

Означення. Нехай A – непорожня підмножина множини натуральних чисел $\mathbf{N}$. Число $m \in A$ називають *найменшим елементом* або першим елементом множини A, якщо

$$\forall\, x \in A \quad m \le x,$$

$$(\text{або } \forall\, x \in A \quad x \ne m \;\Rightarrow\; m < x).$$

Теорема 2.1 (*Принцип найменшого числа*). *В кожній непорожній підмножині A множини натуральних чисел є найменший елемент.*

Метод математичної індукції

На аксіому індукції спирається плідний і широко вживаний метод доведення математичних тверджень, який називається *методом математичної індукції.*

Для обґрунтування цього методу наведемо ряд теорем.

Теорема 2.2 (*Принцип математичної індукції, основна форма*). *Якщо деяке твердження P, що залежить від натурального параметра n, правильне для числа 1 і якщо з припущення, що воно правильне для натурального числа k, випливає його правильність і для наступного числа k', то твердження P правильне для будь-якого натурального числа n.*

*Доведення***.** Позначимо через M множину тих натуральних чисел, для яких твердження P правильне.

$1 \in M$ за умовою.

Нехай $k \in M$, тоді за умовою теореми, $k' \in M$.

За аксіомою індукції, $M = \mathbf{N}$. Теорему доведено.

Отже, щоб довести справедливість якогось твердження для будь-якого натурального числа n методом математичної індукції потрібно: 1) довести, що це твердження справедливе для $n = 1$;
2) припустивши справедливість даного твердження для $n = k$, довести його справедливість для $n = k' = k + 1$;
3) зробити висновок про справедливість цього твердження для всіх натуральних чисел.

Теорема 2.3 (*Друга форма принципу математичної індукції*). *Якщо деяке твердження P, що залежить від натурального параметра n, правильне для числа 1 і якщо з припущення, що воно правильне для всіх натуральних чисел, менших ніж k, випливає його правильність і для числа k, то твердження P правильне для будь-якого натурального числа n.*

Доведення. Припустимо, що умови теореми здійснюються, але твердження P правильне не для всіх натуральних чисел. Нехай M – множина всіх тих натуральних чисел a, для кожного з яких твердження P неправильне. Внаслідок припущення, множина M – непорожня. Отже, за теоремою 2.1, в ній є найменше число r. Для числа r твердження P неправильне.

А для всіх натуральних чисел l, що задовольняють умову $l < r$, твердження P правильне. Але в такому разі, за умовою теореми, твердження P правильне і для числа r. Ми прийшли до суперечності. Отже, припущення про те, що твердження P правильне не для всіх натуральних чисел, невірне. Теорему доведено.

Теорема 2.4 (***Узагальнення основної форми принципу математичної індукції***)**.** *Якщо деяке твердження P, що залежить від натурального параметра n, правильне для певного натурального числа n_0 і якщо з припущення, що воно правильне для натурального числа $k \ge n_0$, випливає його правильність і для числа k', то твердження P правильне для будь-якого натурального числа $n \ge n_0$.*

Теорема 2.5 (***Узагальнення другої форми принципу математичної індукції***)**.** *Якщо деяке твердження P, що залежить від натурального параметра n, правильне для натурального числа n_0 і якщо з припущення, що воно правильне для всіх натуральних чисел l, які задовольняють умову $n_0 \le l < k$, випливає його правильність і для числа k, то твердження P правильне для будь-якого натурального числа $n \ge n_0$.*

Приклад 2.1. *Довести, що для довільного натурального n виконується твердження*

$$1^2 \cdot 2! + 2^2 \cdot 3! + \ldots + n^2 (n+1)! = (n-1)(n+2)! + 2.$$

1) При $n = 1$ твердження має вигляд:

$$1^2 \cdot 2! = 0! + 2,$$

і є справедливим.

2) Припустимо, що твердження справедливе при $n = k$, тобто

$$1^2 \cdot 2! + 2^2 \cdot 3! + \ldots + k^2 (k+1)! = (k-1)(k+2)! + 2.$$

Покажемо, що воно справедливе при $n = k + 1$:

$$\underbrace{1^2 \cdot 2! + 2^2 \cdot 3! + \ldots + k^2 (k+1)!} + (k+1)^2 (k+1+1)! = \text{(*за припущенням індукції*)}$$

$$= (k-1)(k+2)! + 2 + (k+1)^2 (k+2)! =$$

$$= (k - 1 + k^2 + 2k + 1) \cdot (k+2)! + 2 =$$

$$= (k^2 + 3k) \cdot (k+2)! + 2 =$$

$$= k\cdot(k+2)!\cdot(k+3)+2 =$$
$$= k\cdot(k+3)!+2 =$$
$$= \big((k+1)-1\big)\cdot\big((k+1)+2\big)!+2,$$

тобто твердження справедливе при $n = k + 1$.

За теоремою 2.2, твердження справедливе для всіх $n \in \mathbf{N}$.

Приклад 2.2. *Довести, що для довільного натурального n виконується твердження*

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}.$$

1) При $n = 1$ твердження має вигляд:

$$1-\frac{1}{2}=\frac{1}{1+1},$$

і є справедливим.

2) Припустимо, що твердження справедливе при $n = k$, тобто

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots-\frac{1}{2k}=\frac{1}{k+1}+\frac{1}{k+2}+\ldots+\frac{1}{2k}.$$

Покажемо, що воно справедливе при $n = k + 1$:

$$\underbrace{1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots-\frac{1}{2k}}+\frac{1}{2k+1}-\frac{1}{2(k+1)} = \text{(\textit{за припущенням індукції})}$$

$$=\frac{1}{k+1}+\frac{1}{k+2}+\ldots+\frac{1}{2k}+\frac{1}{2k+1}-\frac{1}{2(k+1)}=$$
$$=\frac{1}{k+2}+\ldots+\frac{1}{2k}+\frac{1}{2k+1}\underbrace{-\frac{1}{2(k+1)}+\frac{1}{k+1}}=$$
$$=\frac{1}{(k+1)+1}+\ldots+\frac{1}{2k}+\frac{1}{2k+1}+\frac{1}{2(k+1)},$$

тобто твердження справедливе при $n = k + 1$.

За теоремою 2.2, твердження справедливе для всіх $n \in \mathbf{N}$.

Приклад 2.3. *Довести, що* $\forall\ n \in \mathbf{N}$

$$\left(3^{3n+2}+2^{4n+1}\right)\ \vdots\ 11.$$

1) При $n = 1$ твердження має вигляд:

$$3^{3+2}+2^{4+1}=3^5+2^5=275\ \vdots\ 11,$$

і є справедливим.

2) Припустимо, що твердження справедливе при $n = k$, тобто

$$\left(3^{3k+2}+2^{4k+1}\right)\ \vdots\ 11.$$

Покажемо, що воно справедливе при $n = k + 1$:

$$3^{3(k+1)+2} + 2^{4(k+1)+1} = 3^{3k+2} \cdot 3^3 + 2^{4k+1} \cdot 2^4 =$$
$$= 27 \cdot \underbrace{\left(3^{3k+2} + 2^{4k+1}\right)}_{P(k)\ \vdots 11} - \underbrace{11 \cdot 2^{4k+1}}_{\vdots 11},$$

тобто $P(k+1) \vdots 11$.

За теоремою 2.2, твердження справедливе для всіх $n \in \mathbf{N}$.

Приклад 2.4. *Довести, що* $\forall\, n \in \mathbf{N},\ \ n > 4$ *виконується нерівність*

$$2^n > n^2.$$

1) При $n = 5$ твердження має вигляд:

$$2^5 > 5^2,$$

і є справедливим.

2) Припустимо, що твердження справедливе при $n = k$ $(k > 4)$, тобто

$$2^k > k^2. \tag{1}$$

Покажемо, що воно справедливе при $n = k + 1$, тобто доведемо, що

$$2^{k+1} > (k+1)^2. \tag{2}$$

Зауважимо, що суттєвим в цій задачі є те, що саме з нерівності (1) потрібно вивести нерівність (2), тому слід чітко дотримуватись цієї логіки.

$$2^k > k^2 \ \Rightarrow\ 2 \cdot 2^k > 2 \cdot k^2 \ \Rightarrow\ 2^{k+1} > 2k^2,$$

залишається довести, що $2k^2 > (k+1)^2$, це можна зробити двома способами:

а) розглянемо різницю

$$2k^2 - (k+1)^2 = 2k^2 - k^2 - 2k - 1 = k^2 - 2k - 1 = (\underbrace{k-1}_{>3})^2 - 2 > 0,$$

отже $2k^2 > (k+1)^2$;

б) оцінимо ліву частину нерівності

$$2k^2 = k^2 + k^2 + 2k + 1 - 2k - 1 = (k+1)^2 + k^2 - 2k - 1 =$$
$$= (k+1)^2 + (k-1)^2 - 2 > (k+1)^2,$$

оскільки $(\underbrace{k-1}_{>3})^2 - 2 > 0$ при $k > 4$.

Таким чином, $2^{k+1} > (k+1)^2$, тобто твердження справедливе при $n = k + 1$.

За теоремою 2.4, твердження справедливе для всіх $n \in \mathbf{N}$, $n > 4$.

3 КОМПЛЕКСНІ ЧИСЛА

Рівняння $x^2 + 1 = 0$ в множині дійсних чисел не має розв'язків. Один з коренів заданого рівняння позначають символом i. Тоді другий корінь цього рівняння позначається символом $-i$. Отже,

$$i^2 = (-i)^2 = -1.$$

Системою комплексних чисел називають множину $\boldsymbol{C}$, яка містить множину дійсних чисел та елемент i, квадрат якого дорівнює -1. Елементи цієї множини називають *комплексними числами.*

Алгебраїчна форма комплексного числа

Кожен елемент системи $\mathbf{C}$, тобто кожне комплексне число z можна записати у вигляді

$$z = a + bi, \tag{1}$$

де a, b – деякі дійсні числа, i – таке число, для якого $i^2 = -1$.

Запис (1) називають *алгебраїчною формою* комплексного числа z.

Число i називають *уявною одиницею*, число a називають *дійсною частиною* числа z, число bi – *уявною частиною* числа z, а число b – коефіцієнтом уявної частини числа z.

Два комплексні числа $a + bi$ і $c + di$ називають *рівними* , якщо рівні їх дійсні частини і коефіцієнти уявних частин, тобто коли $a = c$ і $b = d$.

Операції над комплексними числами, заданими в алгебраїчній формі:

$$z_1 + z_2 = (a + bi) + (c + di) = (a + c) + (b + d)\, i\,;$$
$$z_1 - z_2 = (a + bi) - (c + di) = (a - c) + (b - d)\, i\,;$$
$$z_1 \cdot z_2 = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)\, i\,,$$

тобто множення чисел z_1 та z_2 зводиться до множення суми на суму, при цьому враховуємо, що $i^2 = -1$;

$$\frac{z_1}{z_2} = \frac{a+bi}{c+di} = \frac{a+bi}{c+di}\cdot\frac{c-di}{c-di} = \frac{(a+bi)\cdot(c-di)}{c^2+d^2},$$

тобто, щоб поділити число z_1 на z_2, треба чисельник і знаменник помножити на число $c - di$.

Виконаємо ділення двох комплексних чисел:

$$\frac{2+3i}{4+5i} = \frac{(2+3i)\cdot(4-5i)}{(4+5i)\cdot(4-5i)} = \frac{(2\cdot 4+3\cdot 5)+(2\cdot(-5)+3\cdot 4)i}{4^2+5^2} = \frac{23+2i}{41} = \frac{23}{41}+\frac{2}{41}i\,.$$

Означення. Два комплексні числа $z = a + bi$ і $\bar{z} = a - bi$, що відрізняються одне від одного тільки знаком при уявній частині, називають *спряженими***.**

Властивості спряжених комплексних чисел:

1) $z+\bar{z}\in\mathbf{R}$; $\quad z\cdot\bar{z}\in\mathbf{R}$;

2) $\overline{z_1+z_2}=\bar{z}_1+\bar{z}_2$;

3) $\overline{z_1-z_2}=\bar{z}_1-\bar{z}_2$;

4) $\overline{z_1\cdot z_2}=\bar{z}_1\cdot\bar{z}_2$;

5) $\overline{\left(\dfrac{z_1}{z_2}\right)}=\dfrac{\bar{z}_1}{\bar{z}_2}$.

Геометрична інтерпретація комплексного числа

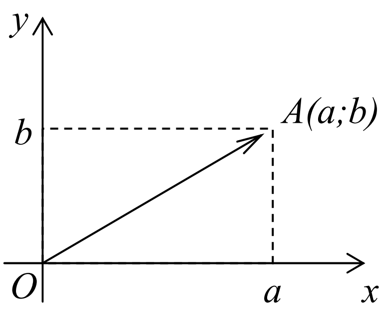
Візьмемо на площині прямокутну декартову систему координат xOy.

I. Комплексне число $z=a+bi$ зображають точкою $A\ (a,b)$.

Комплексне число 0 зображується точкою O площини, яку взято як початок відліку. Дійсні числа $z=a+0i$, і тільки вони, зображуються точками осі абсцис Ox, у зв'язку з чим цю вісь називають *дійсною віссю*. Суто уявні числа $z=0+bi$, і тільки вони, зображуються точками осі ординат Oy, тому цю вісь називають *уявною віссю*.

Площину, між точками якої і комплексними числами встановлено взаємно однозначну відповідність щойно описаним способом, називають *комплексною площиною*.

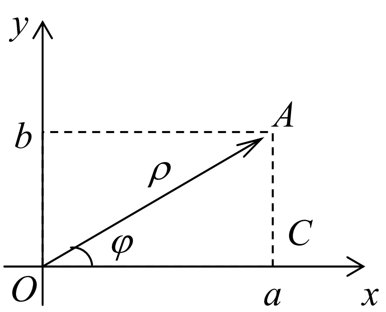
II. Довільному комплексному числу $z=a+bi$ поставимо у



відповідність напрямлений відрізок $\overrightarrow{OA}$ комплексної площини, початком якого є початок координат O, а кінцем – точка A з координатами (a,b). Вектор $\overrightarrow{OA}$ називають *радіус-вектором* точки A.

Тригонометрична форма комплексного числа

Розглянемо довільне відмінне від нуля комплексне число $z=a+bi$ і його радіус-вектор $\overrightarrow{OA}$ на площині.



Введемо позначення: ρ – довжина вектора $\overrightarrow{OA}$, φ – кут нахилу вектора $\overrightarrow{OA}$, тобто кут, який утворює вектор $\overrightarrow{OA}$ з додатним напрямом осі Ox.

З трикутника OAC: $\quad a=\rho\cdot\cos\varphi$, $\quad b=\rho\cdot\sin\varphi$.

Звідси,

$$z = a + bi = \rho\,(\cos\varphi + i\sin\varphi). \qquad (2)$$

Запис (2) називають *тригонометричною формою* комплексного числа z. Дійсне додатне число ρ називають *модулем* комплексного числа z і позначають $\rho = |z|$, а кут φ – *аргументом* числа z і позначають $\varphi = \arg z$.

З трикутника OAC маємо:

$$\rho = \sqrt{a^2 + b^2}, \qquad \begin{cases} \cos\varphi = \dfrac{a}{\rho}, \\ \sin\varphi = \dfrac{b}{\rho}. \end{cases} \qquad (3)$$

Зауважимо, що кут φ визначається неоднозначно, з точністю до доданків, кратних 2π, у зв'язку з періодичністю функцій $\cos x$ і $\sin x$. Інакше кажучи, поряд з зображенням (2) має місце і зображення:

$$z = a + bi = \rho\,[\cos(\varphi + 2\pi k) + i\sin(\varphi + 2\pi k)]. \qquad (4)$$

Таким чином,

рівність двох комплексних чисел, заданих у тригонометричній формі, означає, що модулі цих чисел рівні, а аргументи можуть відрізнятися на число, кратне 2π.

У більшості випадків, подаючи комплексне число в тригонометричній формі, аргумент φ беруть у межах $0 \le \varphi < 2\pi$ або $-\pi < \varphi \le \pi$.

Звернемо увагу, що для визначення φ використовуємо обидві рівності системи (3), бо значення тільки однієї тригонометричної функції не дає змоги визначити, в якій координатній чверті знаходиться шуканий кут. При переході від алгебраїчної форми комплексного числа до тригонометричної доцільно зображати дане число радіус-вектором на комплексній площині. Це полегшить знаходження значень аргументу.

Поняття модуля комплексного числа узагальнює поняття модуля (абсолютної величини) дійсного числа, дійсно

$$|-3| = |-3 + 0i| = \sqrt{(-3)^2 + 0^2} = \sqrt{9} = 3.$$

Операції над комплексними числами, заданими в тригонометричній формі:

$$z_1 \cdot z_2 = [\rho_1(\cos\varphi_1 + i\sin\varphi_1)] \cdot [\rho_2(\cos\varphi_2 + i\sin\varphi_2)] = \\ = \rho_1 \cdot \rho_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)); \qquad (5)$$

$$\frac{z_1}{z_2} = \frac{\rho_1(\cos\varphi_1 + i\sin\varphi_1)}{\rho_2(\cos\varphi_2 + i\sin\varphi_2)} = \frac{\rho_1}{\rho_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)); \qquad (6)$$

$$z^n = [\rho(\cos\varphi + i\sin\varphi)]^n = \rho^n(\cos n\varphi + i\sin n\varphi), \quad n \in \mathbf{Z}; \qquad (7)$$

Формулу (7) називають *формулою Муавра*.

$$\sqrt[n]{z}=\sqrt[n]{\rho(\cos\varphi+i\sin\varphi)}=\sqrt[n]{\rho}\left(\cos\frac{\varphi+2\pi k}{n}+i\sin\frac{\varphi+2\pi k}{n}\right), \qquad (8)$$

$$k=0,1,\ldots,n-1, \quad n\in\mathbf{N}.$$

Відмітимо, що *операція добування кореня n-го степеня в полі комплексних чисел завжди здійсненна*: *які б не були натуральне число* n *і комплексне число* z *, корінь* n*-го степеня з числа* z *існує*; *при* $z=0$ $\sqrt[n]{z}=0$, *а при* $z\neq 0$ $\sqrt[n]{z}$ *має* n *різних значень, що визначаються за формулою* (8).

Геометричний зміст $\sqrt[n]{z}$ (при $z\neq 0$):

Всі n значень $\omega_0, \omega_1, \ldots, \omega_{n-1}$ кореня n-го степеня з комплексного числа z , які дістаємо при $k=0, 1, \ldots, n-1$, мають один і той самий модуль $\sqrt[n]{|z|}$. Аргумент числа ω_0 дорівнює $\dfrac{\varphi}{n}$, а аргументи чисел $\omega_1, \omega_2, \ldots,$ ω_{n-1} дістаємо послідовним додаванням кута $\dfrac{2\pi}{n}$.

Отже, точки комплексної площини, якими зображуються числа $\omega_0, \omega_1,$ $\ldots, \omega_{n-1}$, є вершинами правильного n-кутника, вписаного в коло радіуса $\sqrt[n]{|z|}$ з центром у початку координат, причому одна з вершин зображує число ω_0 з аргументом $\dfrac{\varphi}{n}$, чим однозначно визначається положення всіх інших вершин.

Корені з одиниці

Число 1 в тригонометричній формі записується так:

$$1=\cos 0+i\sin 0\ .$$

Тому, за формулою (8),

$$\sqrt[n]{1}=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}, \qquad k=0,1,\ldots,n-1.$$

Значення $\sqrt[n]{1}$ позначатимемо відповідно символами $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$. Отже,

$$\varepsilon_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}, \qquad k=0,1,\ldots,n-1.$$

На комплексній площині корені n-го степеня з 1 зображуються вершинами правильного n-кутника, вписаного в коло одиничного радіуса з центром у початку координат, причому корінь $\varepsilon_0=1$ зображується вершиною, що лежить на дійсній додатній півосі.

Теорема 3.1. *Всі значення кореня n-го степеня з комплексного числа z можна дістати, помноживши одне з цих значень на кожен з коренів n-го степеня з* 1.

Якщо n – число складене, тобто має дільники, відмінні від 1 і самого себе, наприклад $n = pq$, то в множині всіх коренів n-го степеня з одиниці є корені, які є також коренями p-го і q-го степенів з одиниці.

Так серед коренів 6-го степеня з одиниці $\{\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5\}$ є значення коренів з одиниці степеня 2: $\{\varepsilon_0, \varepsilon_3\}$, і значення коренів з одиниці степеня 3: $\{\varepsilon_0, \varepsilon_2, \varepsilon_4\}$. Значення $\varepsilon_1, \varepsilon_5$ не є коренями з одиниці ніякого меншого, ніж 6, степеня.

Означення 1. Корінь n-го степеня з 1 називають *первісним*, якщо він не є коренем з 1 ніякого меншого степеня.

Означення 2. Значення кореня n-го степеня з 1 називають *первісним коренем*, якщо його різні цілі степені породжують всі значення кореня n-го степеня з 1.

Так, в попередньому прикладі

$$(\varepsilon_1)^1 = \varepsilon_1,\ \ (\varepsilon_1)^2 = \varepsilon_2,\ \ (\varepsilon_1)^3 = \varepsilon_3,\ \ (\varepsilon_1)^4 = \varepsilon_4,\ \ (\varepsilon_1)^5 = \varepsilon_5,\ \ (\varepsilon_1)^6 = \varepsilon_0 -$$

дістали всі значення кореня 6-го степеня з 1. Отже ε_1 є первісним коренем з одиниці 6-го степеня.

Проте

$$(\varepsilon_2)^1 = \varepsilon_2,\ \ (\varepsilon_2)^2 = \varepsilon_4,\ \ (\varepsilon_2)^3 = \varepsilon_0,$$

тобто ε_2 не є первісним коренем з одиниці 6-го степеня.

Теорема 3.2. *Корінь n-го степеня з одиниці* $\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ *є первісним тоді і тільки тоді, коли число k взаємно просте з числом n.*

Приклад 3.1. *Розв'язати рівняння* $z^2 + \bar{z} = 1$.

Використаємо алгебраїчну форму комплексного числа.

Нехай $z = x + yi$, де $x, y \in \mathbf{R}$. Тоді

$$(x + yi)^2 + (x - yi) = 1,$$
$$x^2 + 2xyi - y^2 + x - yi = 1,$$
$$(x^2 - y^2 + x) + (2xy - y)\, i = 1 + 0i.$$

За умовою рівності двох комплексних чисел, записаних в алгебраїчній формі, маємо:

$$\begin{cases} x^2 - y^2 + x = 1, \\ 2xy - y = 0. \end{cases}$$

Розв'яжемо цю систему рівнянь:

$$\begin{cases} x^2 - y^2 + x = 1, \\ (2x - 1)y = 0, \end{cases}$$

$$\left[\begin{array}{l}\begin{cases}x^2-y^2+x=1,\\ 2x-1=0,\end{cases}\\ \begin{cases}x^2-y^2+x=1,\\ y=0,\end{cases}\end{array}\right. \qquad \left[\begin{array}{l}\begin{cases}y^2=-\dfrac{1}{4},\\ x=\dfrac{1}{2},\end{cases}\\ \begin{cases}x^2+x-1=0,\\ y=0,\end{cases}\end{array}\right. \qquad \begin{cases}x=\dfrac{-1\pm\sqrt{5}}{2},\\ y=0.\end{cases}$$

Відповідь: $z_1=\dfrac{-1+\sqrt{5}}{2}+0i$, $z_2=\dfrac{-1-\sqrt{5}}{2}+0i$.

Приклад 3.2. *Обчислити* $\sqrt{5-12i}$.

Деякі квадратні корені з комплексного числа можна знаходити в алгебраїчній формі.

Нехай $\sqrt{5-12i}=x+yi$, де $x, y\in \mathbf{R}$. Тоді

$$5-12i=(x+yi)^2,$$

$$x^2+2xyi-y^2=5-12i,$$

$$(x^2-y^2)+2xyi=5-12i,$$

За умовою рівності двох комплексних чисел, записаних в алгебраїчній формі:

$$\begin{cases}x^2-y^2=5,\\ 2xy=-12.\end{cases}$$

З останньої рівності помічаємо, що дійсні числа x та y мають різні знаки. Очевидно, що розв'язками системи є:

$$\begin{cases}x=3,\\ y=-2\end{cases} \quad \text{або} \quad \begin{cases}x=-3,\\ y=2.\end{cases}$$

Таким чином $\sqrt{5-12i}=\pm(3-2i)$.

Приклад 3.3. *Розв'язати рівняння* $z^2-(5+5i)z+2+11i=0$.

Обчислимо дискримінант квадратного рівняння:

$$D=(5+5i)^2-4(2+11i)=-8+6i.$$

Знайдемо $\sqrt{-8+6i}$. Аналогічно тому, як це було зроблено в прикладі 3.2, матимемо

$$\sqrt{-8+6i}=\pm(1+3i).$$

За формулою коренів квадратного рівняння дістаємо

$$z_{1,2}=\frac{(5+5i)\pm(1+3i)}{2}.$$

Таким чином, $z_1=\dfrac{6+8i}{2}=3+4i$, $z_2=\dfrac{4+2i}{2}=2+i$.

Приклад 3.4. *Обчислити* $\sqrt[5]{\dfrac{(1+\sqrt{3}\,i)^2}{3-3i}}$.

1) Запишемо число $z_1 = 1+\sqrt{3}\,i$ в тригонометричній формі.

За формулами (3) маємо

$$\rho_1 = \sqrt{1^2 + (\sqrt{3})^2} = \sqrt{4} = 2\ ; \qquad \begin{cases} \cos\varphi_1 = \dfrac{1}{2}, \\ \sin\varphi_1 = \dfrac{\sqrt{3}}{2}, \end{cases}$$

звідси $\varphi_1 = \dfrac{\pi}{3}$.

Отже $z_1 = 1+\sqrt{3}\,i = 2\,(\cos\dfrac{\pi}{3} + i\sin\dfrac{\pi}{3})$.

2) Запишемо число $z_2 = 3 - 3i$ в тригонометричній формі.
Аналогічно,

$$\rho_2 = \sqrt{3^2 + 3^2} = \sqrt{18} = 3\sqrt{2}\ ; \qquad \begin{cases} \cos\varphi_2 = \dfrac{3}{3\sqrt{2}} = \dfrac{\sqrt{2}}{2}, \\ \sin\varphi_2 = -\dfrac{3}{3\sqrt{2}} = -\dfrac{\sqrt{2}}{2}, \end{cases}$$

з системи випливає, що $\varphi_2 = -\dfrac{\pi}{4}$.

Отже $z_2 = 3 - 3i = 3\sqrt{2}\left(\cos\left(-\dfrac{\pi}{4}\right) + i\sin\left(-\dfrac{\pi}{4}\right)\right)$.

3) Піднесемо чисельник до степеня. За формулою (7):

$$z_1^{\,2} = \left[2\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)\right]^2 = 2^2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right).$$

4) Виконаємо ділення. За формулою (6) маємо

$$\frac{z_1^{\,2}}{z_2} = \frac{2^2\left(\cos\dfrac{2\pi}{3} + i\sin\dfrac{2\pi}{3}\right)}{3\sqrt{2}\left(\cos\left(-\dfrac{\pi}{4}\right) + i\sin\left(-\dfrac{\pi}{4}\right)\right)} =$$

$$= \frac{2\sqrt{2}}{3}\left(\cos\left(\frac{2\pi}{3} - \left(-\frac{\pi}{4}\right)\right) + i\sin\left(\frac{2\pi}{3} - \left(-\frac{\pi}{4}\right)\right)\right) =$$

$$= \frac{2\sqrt{2}}{3}\left(\cos\frac{11\pi}{12} + i\sin\frac{11\pi}{12}\right).$$

5) Обчислимо значення кореня. За формулою (8):

$$\omega_k = \sqrt[5]{\frac{2\sqrt{2}}{3}\left(\cos\frac{11\pi}{12} + i\sin\frac{11\pi}{12}\right)} =$$

$$= \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{\frac{11\pi}{12} + 2\pi k}{5} + i\sin\frac{\frac{11\pi}{12} + 2\pi k}{5}\right), \quad k = 0,1,2,3,4.$$

При $k = 0$

$$\omega_0 = \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{11\pi}{60} + i\sin\frac{11\pi}{60}\right),$$

при $k = 1$

$$\omega_1 = \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{\frac{11\pi}{12} + 2\pi\cdot 1}{5} + i\sin\frac{\frac{11\pi}{12} + 2\pi\cdot 1}{5}\right) = \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{35\pi}{60} + i\sin\frac{35\pi}{60}\right),$$

далі

$$\omega_2 = \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{59\pi}{60} + i\sin\frac{59\pi}{60}\right),$$

$$\omega_3 = \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{83\pi}{60} + i\sin\frac{83\pi}{60}\right),$$

$$\omega_4 = \sqrt[5]{\frac{2\sqrt{2}}{3}}\left(\cos\frac{107\pi}{60} + i\sin\frac{107\pi}{60}\right).$$

Одержали п’ять різних значень кореня п’ятого степеня із заданого комплексного числа.

4 АЛГЕБРА МАТРИЦЬ

Прямокутною матрицею розмірності $m \times n$ називають таблицю чисел, що складається з m рядків і n стовпців.

Позначають $A = (a_{ij})_{m \times n}$, тобто $i = 1, \ldots, m$; $j = 1, \ldots, n$.

Матрицю $A = (a_{ij})$ розмірності $m \times n$ називають *рівною* матриці $B = (b_{ij})$ розмірності $p \times q$, якщо

1) $m = p$, $n = q$,
2) $a_{ij} = b_{ij}$, ($i = 1, \ldots, m$; $j = 1, \ldots, n$).

Операції над матрицями

Означення. Нехай дано дві матриці $A = (a_{ij})$, $B = (b_{ij})$ однакової розмірності $m \times n$. *Сумою* цих матриць називають матрицю $S = (a_{ij} + b_{ij})$ тієї самої розмірності.

Тобто додавання двох матриць однакової розмірності зводиться до додавання одноіменних елементів:

$$\begin{pmatrix} 2 & 3 & 5 \\ 1 & 7 & 4 \end{pmatrix} + \begin{pmatrix} -1 & 2 & 0 \\ 8 & 10 & 11 \end{pmatrix} = \begin{pmatrix} 2+(-1) & 3+2 & 5+0 \\ 1+8 & 7+10 & 4+11 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 5 \\ 9 & 17 & 15 \end{pmatrix}.$$

Означення. *Добутком* матриці $A = (a_{ij})$ розмірності $m \times n$ *на число* λ називають матрицю $D = (\lambda \cdot a_{ij})$ тієї самої розмірності.

Тобто множення матриці на число λ зводиться до множення всіх елементів цієї матриці на число λ:

$$3 \cdot \begin{pmatrix} -2 & 4 & 7 & 3 \\ 0 & 5 & -1 & 10 \\ 8 & 1 & 11 & 9 \end{pmatrix} = \begin{pmatrix} 3\cdot(-2) & 3\cdot 4 & 3\cdot 7 & 3\cdot 3 \\ 3\cdot 0 & 3\cdot 5 & 3\cdot(-1) & 3\cdot 10 \\ 3\cdot 8 & 3\cdot 1 & 3\cdot 11 & 3\cdot 9 \end{pmatrix} = \begin{pmatrix} -6 & 12 & 21 & 9 \\ 0 & 15 & -3 & 30 \\ 24 & 3 & 33 & 27 \end{pmatrix}.$$

Означення. Нехай дано матрицю $A = (a_{ij})$ розмірності $m \times n$ і матрицю $B = (b_{st})$ розмірності $n \times l$. *Добутком матриці* A *на матрицю* B називають матрицю $C = (c_{pq})$ розмірності $m \times l$, елементи якої визначають за правилом:

$$c_{pq} = a_{p1}b_{1q} + a_{p2}b_{2q} + \ldots + a_{pn}b_{nq}$$

($p = 1, \ldots, m$; $q = 1, \ldots, l$). Тобто елемент c_{pq}, який стоїть в p-му рядку і q-му стовпцеві матриці C, дорівнює сумі добутків елементів p-го рядка матриці A на відповідні елементи q-го стовпця матриці B.

$$\begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 10 & 5 \\ 9 & 11 \end{pmatrix} = \begin{pmatrix} 1\cdot 1+3\cdot 3+5\cdot 10+7\cdot 9 & 1\cdot 2+3\cdot 4+5\cdot 5+7\cdot 11 \\ 2\cdot 1+4\cdot 3+6\cdot 10+8\cdot 9 & 2\cdot 2+4\cdot 4+6\cdot 5+8\cdot 11 \\ 9\cdot 1+10\cdot 3+11\cdot 10+12\cdot 9 & 9\cdot 2+10\cdot 4+11\cdot 5+12\cdot 11 \end{pmatrix} = \begin{pmatrix} 123 & 116 \\ 146 & 138 \\ 257 & 245 \end{pmatrix}$$

Властивості операції додавання матриць:

1. *Комутативність.* Для довільних матриць $A = (a_{ij})$, $B = (b_{ij})$ однакової розмірності виконується рівність

$$A + B = B + A\ .$$

2. *Асоціативність.* Для довільних матриць $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ однакової розмірності виконується рівність

$$(A + B) + C = A + (B + C)\ .$$

3. У множині матриць даної розмірності є матриця Θ, яка має властивість

$$A + \Theta = \Theta + A = A$$

для будь-якої матриці A.

Такою є *нульова* матриця, всі елементи якої дорівнюють нулю.

4. У множині матриць даної розмірності для кожної матриці $A = (a_{ij})$ існує *протилежна* матриця, тобто така матриця B, що

$$A + B = B + A = \Theta.$$

Такою є матриця $B = (-\,a_{ij})$.

Властивості операції множення матриці на число:

1. *Асоціативність.* Для будь-якої матриці A і довільних чисел λ, μ виконується рівність

$$\lambda\,(\mu\,A) = (\lambda\,\mu)\,A\ .$$

2. *Дистрибутивність* відносно додавання матриць та додавання чисел. Для будь-яких матриць A, B і довільних чисел λ, μ виконуються рівності

$$\lambda\,(A + B) = \lambda A + \lambda B\ ,$$

$$(\lambda + \mu)\,A = \lambda A + \mu A\ .$$

Властивості операції множення матриць:

1. *Некомутативність.* Існують такі матриці, що

$$A \cdot B \neq B \cdot A\ .$$

2. *Асоціативність.* Для будь-яких матриць A, B, C відповідної розмірності виконується рівність

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

3. У множині квадратних матриць n-го порядку існує така матриця E, що

$$A \cdot E = E \cdot A = A$$

для довільної матриці A n-го порядку.

Такою є *одинична* матриця, елементи головної діагоналі якої дорівнюють одиниці, решта елементів – нулі.

4. *Дистрибутивність.* Для довільних матриць $A,\ B,\ C$ відповідної розмірності виконуються рівності

$$(A + B) \cdot C = A \cdot C + B \cdot C\,,$$
$$C \cdot (A + B) = C \cdot A + C \cdot B\,.$$

5. Для довільних матриць $A,\ B$ відповідної розмірності і довільного числа λ виконується рівність

$$(\lambda A) \cdot B = \lambda (A \cdot B) = A \cdot (\lambda B)\,.$$

Теорема 4.1. *Визначник добутку двох квадратних матриць* n*-го порядку дорівнює добутку визначників цих матриць*: $|\,A \cdot B\,| = |A| \cdot |B|$.

Обернена матриця

Означення. Матрицю A^{-1} називають *оберненою* до квадратної матриці A, якщо

$$A \cdot A^{-1} = A^{-1} \cdot A = E.$$

Матрицю A називають *невиродженою* (*неособливою*), якщо її визначник відмінний від нуля.

Терема 4.2. *Для того, щоб існувала матриця, обернена до матриці* A *, необхідно і достатньо, щоб матриця* A *була невиродженою.*

Теорема 4.3. *Для кожної квадратної неособливої матриці* A *існує єдина обернена матриця* A^{-1} .

Нехай матриця

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ a_{n1} & a_{n2} & \dots & a_{n\,n} \end{pmatrix} \qquad (1)$$

неособлива. Тоді оберненою до неї буде матриця

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \dots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{22}}{|A|} & \dots & \frac{A_{n2}}{|A|} \\ . & . & . & . \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \dots & \frac{A_{n\,n}}{|A|} \end{pmatrix}, \qquad (2)$$

в якій елементами i-го стовпця ($i = 1, ..., n$) є алгебраїчні доповнення елементів i-го рядка матриці A , поділені на визначник $|\,A\,|$.

Формула (2) дає *правило знаходження оберненої матриці* для заданої матриці A.

***Другий спосіб* знаходження оберненої матриці для матриці A :**

1. Скласти матрицю виду ($A \mid E$), де E – одинична матриця n-го порядку.

2. Виконуючи елементарні перетворення над рядками цієї матриці, добитися, щоб зліва від риски утворилась одинична матриця.

3. Тоді справа від риски утвориться шукана матриця A^{-1} :

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

Приклад 4.1. *Знайти матрицю, обернену до матриці*

$$A = \begin{pmatrix} 1 & 2 & -3 \\ -1 & 2 & 3 \\ 1 & -2 & 3 \end{pmatrix}.$$

Обчислимо визначник матриці :

$$|A| = \begin{vmatrix} 1 & 2 & -3 \\ -1 & 2 & 3 \\ 1 & -2 & 3 \end{vmatrix} = 24 .$$

$|A| \neq 0$, отже обернена до матриці A існує.

Знайдемо її за формулою (2):

$$A_{11} = (-1)^{1+1}\begin{vmatrix} 2 & 3 \\ -2 & 3 \end{vmatrix} = 12, \qquad A_{21} = (-1)^{2+1}\begin{vmatrix} 2 & -3 \\ -2 & 3 \end{vmatrix} = 0,$$

$$A_{12} = (-1)^{1+2}\begin{vmatrix} -1 & 3 \\ 1 & 3 \end{vmatrix} = 6, \qquad A_{22} = (-1)^{2+2}\begin{vmatrix} 1 & -3 \\ 1 & 3 \end{vmatrix} = 6,$$

$$A_{13} = (-1)^{1+3}\begin{vmatrix} -1 & 2 \\ 1 & -2 \end{vmatrix} = 0, \qquad A_{23} = (-1)^{2+3}\begin{vmatrix} 1 & 2 \\ 1 & -2 \end{vmatrix} = 4,$$

$$A_{31} = (-1)^{3+1}\begin{vmatrix} 2 & -3 \\ 2 & 3 \end{vmatrix} = 12,$$

$$A_{32} = (-1)^{3+2}\begin{vmatrix} 1 & -3 \\ -1 & 3 \end{vmatrix} = 0,$$

$$A_{33} = (-1)^{3+3}\begin{vmatrix} 1 & 2 \\ -1 & 2 \end{vmatrix} = 4.$$

Запишемо обернену до матриці A :

$$A^{-1} = \frac{1}{24}\begin{pmatrix} 12 & 0 & 12 \\ 6 & 6 & 0 \\ 0 & 4 & 4 \end{pmatrix} = \frac{1}{12}\begin{pmatrix} 6 & 0 & 6 \\ 3 & 3 & 0 \\ 0 & 2 & 2 \end{pmatrix}.$$

Перевірити правильність знаходження оберненої матриці можна шляхом множення заданої і знайденої матриць: якщо добуток їх дорівнює одиничній матриці, то обернену матрицю знайдено правильно. Зробимо перевірку:

$$\begin{pmatrix} 1 & 2 & -3 \\ -1 & 2 & 3 \\ 1 & -2 & 3 \end{pmatrix} \cdot \frac{1}{12} \cdot \begin{pmatrix} 6 & 0 & 6 \\ 3 & 3 & 0 \\ 0 & 2 & 2 \end{pmatrix} = \frac{1}{12} \begin{pmatrix} 12 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E.$$

Приклад 4.2. *Знайти матрицю, обернену до матриці*

$$A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 5 & 6 \\ -1 & 2 & -7 \end{pmatrix}.$$

$|A| \neq 0$. Отже матриця A^{-1} існує. Скористаємось другим способом знаходження оберненої матриці. Складемо матрицю

$$(A|E) = \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 2 & 5 & 6 & 0 & 1 & 0 \\ -1 & 2 & -7 & 0 & 0 & 1 \end{array}\right) \quad \times(-2)+,\ + \quad \to$$

Перетворимо її (працюючи тільки з рядками):

$$\to \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & -1 & 2 & -2 & 1 & 0 \\ 0 & 5 & -5 & 1 & 0 & 1 \end{array}\right) \quad \times(-1) \quad \to$$

$$\to \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 2 & -1 & 0 \\ 0 & 5 & -5 & 1 & 0 & 1 \end{array}\right) \quad \times(-5)+ \quad \to \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 2 & -1 & 0 \\ 0 & 0 & 5 & -9 & 5 & 1 \end{array}\right) \quad \times 1/5 \quad \to$$

$$\to \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 2 & -1 & 0 \\ 0 & 0 & 1 & -9/5 & 1 & 1/5 \end{array}\right) \quad \times 2+,\ \times(-2)+ \quad \to$$

$$\to \left(\begin{array}{ccc|ccc} 1 & 3 & 0 & 23/5 & -2 & -2/5 \\ 0 & 1 & 0 & -8/5 & 1 & 2/5 \\ 0 & 0 & 1 & -9/5 & 1 & 1/5 \end{array}\right) \quad \times(-3)+ \quad \to \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 47/5 & -5 & -8/5 \\ 0 & 1 & 0 & -8/5 & 1 & 2/5 \\ 0 & 0 & 1 & -9/5 & 1 & 1/5 \end{array}\right).$$

Таким чином, оберненою до матриці A є матриця

$$A^{-1} = \frac{1}{5} \begin{pmatrix} 47 & -25 & -8 \\ -8 & 5 & 2 \\ -9 & 5 & 1 \end{pmatrix}.$$

5 ЕЛЕМЕНТИ ТЕОРІЇ ГРУП

Група. Підгрупа

Означення. Нехай M – довільна множина. Під *бінарною алгебраїчною операцією* $*$ в множині M розуміють закон, за яким будь-яким двом (різним чи однаковим) елементам a і b цієї множини, взятим у певному порядку, ставиться у відповідність єдиний елемент c цієї множини:

$$\forall\, a, b \in M \qquad \exists!\, c \in M: \qquad c = a * b.$$

Прикладами бінарних алгебраїчних операцій є додавання і множення чисел, матриць, многочленів; додавання векторів деякої площини і т.п. Але віднімання натуральних чисел, утворення скалярного добутку векторів не є бінарними алгебраїчними операціями.

Алгебраїчність операції $*$ ототожнюють з поняттям замкнености операції $*$ в даній множині.

Означення. Множину M, в якій введено одну або кілька алгебраїчних операцій, називають *алгебраїчною структурою* або *алгеброю*.

Наприклад, $(\mathbf{Z}, +)$, $(\mathbf{Q}, \cdot)$, $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$ і т. ін.

Означення. *Групою* називається непорожня множина G, в якій введено бінарну операцію $*$ і виконуються такі умови:

1) операція $*$ замкнена, тобто

$$\forall\, a, b \in G \qquad a * b \in G;$$

2) операція $*$ асоціативна, тобто

$$\forall\, a, b, c \in G \qquad (a * b) * c = a * (b * c);$$

3) в G існує *нейтральний елемент*, тобто такий елемент n, що

$$\forall\, a \in G \qquad a * n = n * a = a;$$

4) для кожного елемента $a \in G$ в множині G існує *симетричний елемент*, тобто такий елемент a', що

$$a * a' = a' * a = n.$$

Умови 1) – 4) називають *аксіомами групи*.

Зауважимо, що визначена в групі G бінарна операція $*$ не обов’язково повинна бути комутативною. Якщо ж вона комутативна, то групу G називають *комутативною*, або *абелевою*, за ім’ям норвезького математика Н.Абеля, який вивчав рівняння, теорія яких тісно пов’язана з теорією комутативних груп.

Групу називають *скінченною*, якщо множина її елементів скінченна; групу називають *нескінченною*, якщо множина її елементів нескінченна. Число елементів k скінченної групи G називають її *порядком* і записують

$$|G| = k.$$

В алгебрі бінарну операцію, визначену в множині, як правило, називають додаванням або множенням.

Якщо задану в групі G бінарну операцію називають множенням і користуються символікою, яка відповідає операції множення, то говорять, що в групі G прийнято *мультиплікативну* форму запису. Саму групу G називають мультиплікативною (з лат. *multiplico* – множити). В цьому випадку елемент $a \cdot b$ називають *добутком*, a і b – *множниками*, нейтральний елемент називають *одиничним* і позначають e, симетричний до a елемент називають *оберненим* і позначають a^{-1}.

Якщо ж задану в групі G бінарну операцію називають додаванням і вживають символіку, що відповідає операції додавання, то говорять, що в групі G прийнято *адитивну* форму запису. Саму групу називають адитивною (з лат. *additio* – додавати). Тоді елемент $a + b$ називають *сумою*, a і b – *доданками*, нейтральний елемент називають *нульовим* і позначають θ, симетричний до a елемент називають *протилежним* і позначають $-a$.

Приклади груп:

1) множина цілих чисел **Z** відносно додавання,

2) множина відмінних від нуля раціональних чисел $\mathbf{Q}^+$ відносно операції множення,

3) множина $\{1; -1\}$ відносно операції множення,

4) множина всіх невироджених матриць *n*-го порядку з дійсними елементами відносно операції множення і т.п.

Теорема 5.1. *Множина G всіх коренів n-го степеня з* 1 *є мультиплікативною абелевою групою.*

***Властивості груп*:**

1. *В кожній групі G існує, і притому тільки один, нейтральний відносно операції $*$ елемент.*

2. *В кожній групі G для будь-якого її елемента a існує єдиний симетричний йому елемент a'.*

3. *Для будь-яких елементів a, b групи G кожне з рівнянь $a * x = b$ і $y * a = b$ відносно невідомих x, y має в G єдиний розв'язок.*

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

Теорема 5.2 (*Критерій підгрупи*). *Для того, щоб підмножина H групи G була підгрупою цієї групи необхідно й достатньо, щоб підмножина H:*

1) *разом з будь-якими своїми елементами a і b містила і елемент* $a * b$;

2) *разом з будь-яким своїм елементом a містила і симетричний йому елемент a'.*

Наприклад, підмножина $2\mathbf{Z}$ парних цілих чисел є підгрупою адитивної групи $\mathbf{Z}$ цілих чисел.

Циклічна підгрупа. Порядок елемента

Підгрупу $\langle a \rangle = \{ a^k \mid k \in Z \}$, що складається з усіх цілих степенів деякого елемента a групи G, називають *циклічною підгрупою* групи G, *породженою елементом* a.

Якщо всі степені елемента a є різними елементами групи G, то a називають *елементом нескінченного порядку*, $\langle a \rangle$ – *нескінченною циклічною підгрупою*.

Найменший натуральний показник $n \in \mathrm{N}$, для якого $a^n = e$ називають *порядком елемента* a. Позначають

$$| a | = n.$$

Теорема 5.3. *Якщо* a *є елементом* n*-го порядку, то породжена ним циклічна підгрупа* $\langle a \rangle$ *складається з таких елементів*:

$$a^0 = e,\ a^1,\ a^2,\ a^3,\ \ldots,\ a^{n-1}.$$

Наслідок. *Якщо* a *– елемент скінченного порядку, то його порядок дорівнює порядку циклічної підгрупи* $\langle a \rangle$:

$$| a | = | \langle a \rangle |.$$

Групу G називають *циклічною*, якщо вона складається з степенів одного з своїх елементів g, тобто

$$G = \langle g \rangle.$$

Елемент g в цьому випадку називають *твірним елементом* групи G.

Адитивна група цілих чисел $\mathbf{Z}$ є циклічною з породжуючим елементом 1: $\mathbf{Z} = \langle 1 \rangle$;

мультиплікативна група K_n коренів n-го степеня з 1 є циклічною, породжуючим елементом якої є будь-який первісний корінь n-го степеня з 1:

$$K_n = \{ \sqrt[n]{1} \} = \langle \varepsilon_1 \rangle, \text{ де } \quad \varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Властивості циклічних груп:

1. *Кожна циклічна група є комутативною.*

2. *Кожна підгрупа циклічної групи є циклічною.*

Теорема 5.4 (*Лагранжа*). *В кожній скінченній групі порядок будь-якої підгрупи є дільником порядку групи.*

Наслідок 1. *Порядок кожного елемента* a *скінченної групи* G *є дільником порядку групи.*

Наслідок 2. *Кожна скінченна група G, порядок якої є просте число p, є циклічною групою.*

Так, в групі G з 12 елементів (тобто $|G| = 12$) не може бути підгруп та елементів 5-го порядку, оскільки 5 не є дільником числа 12.

Приклад 5.1. *Перевірити, чи утворює мультиплікативну групу множина всіх цілих степенів числа* 2.

Позначимо задану множину $G = \{ 2^k \mid k \in \mathbf{Z} \}$. Перевіримо виконання аксіом групи для множини G:

1) Покажемо, що операція множення замкнена в G.

Візьмемо довільні елементи a, b з множини G. Це означає, що $a = 2^{k_1}$, $b = 2^{k_2}$, де $k_1, k_2 \in \mathbf{Z}$. Розглянемо добуток $a \cdot b$:

$$a \cdot b = 2^{k_1} \cdot 2^{k_2} = 2^{k_1+k_2} = 2^{k_3}.$$

Бачимо, що $a \cdot b \in G$, оскільки k_3 є цілим числом. Тобто операція множення в G замкнена.

2) Покажемо, що операція множення в множині G асоціативна.

$\forall\, a, b, c \in G, \quad a = 2^{k_1},\ b = 2^{k_2},\ c = 2^{k_4}$.

$$(a \cdot b) \cdot c = (2^{k_1} \cdot 2^{k_2}) \cdot 2^{k_4} = 2^{k_1+k_2} \cdot 2^{k_4} = 2^{(k_1+k_2)+k_4} =$$
$$= 2^{k_1+(k_2+k_4)} = 2^{k_1} \cdot 2^{(k_2+k_4)} = 2^{k_1} \cdot (2^{k_2} \cdot 2^{k_4}) = a \cdot (b \cdot c),$$

оскільки для довільних цілих чисел k_1, k_2, k_4 виконується асоціативний закон додавання.

3) Одиничним елементом в множині G є: $e = 1 = 2^0$. Цей елемент належить G, оскільки степінь двійки – нуль – є цілим числом.

4) Знайдемо для довільного елемента $a \in G$ обернений елемент.

$a = 2^{k_1}$ ($k_1 \in \mathbf{Z}$). Очевидно, що $a^{-1} = 2^{-k_1}$, $-k_1 \in \mathbf{Z}$, отже $a^{-1} \in G$. Тобто і ця аксіома в G виконується.

Таким чином, множина G є мультиплікативною групою, причому циклічною з твірним елементом 2: $G = \langle 2 \rangle$.

Приклад 5.2. *Перевірити, чи утворює адитивну групу множина матриць 2-го порядку з цілими елементами виду* $\begin{pmatrix} a & 5b \\ c & a \end{pmatrix}$.

Позначимо задану множину $G = \left\{ \begin{pmatrix} a & 5b \\ c & a \end{pmatrix} \middle|\ a, b, c \in \mathbf{Z} \right\}$. Перевіримо для неї виконання аксіом групи:

1) Покажемо, що операція додавання замкнена в G.

Візьмемо довільні елементи $\alpha, \beta \in G$. Це означає, що

$$\alpha = \begin{pmatrix} a_1 & 5b_1 \\ c_1 & a_1 \end{pmatrix},\ \ \beta = \begin{pmatrix} a_2 & 5b_2 \\ c_2 & a_2 \end{pmatrix},\text{ де } a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbf{Z}.$$

Розглянемо суму

$$\alpha + \beta = \begin{pmatrix} a_1 & 5b_1 \\ c_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & 5b_2 \\ c_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & 5(b_1 + b_2) \\ c_1 + c_2 & a_1 + a_2 \end{pmatrix}.$$

Бачимо, що $\alpha + \beta \in G$, оскільки отримали матрицю того самого вигляду з цілими елементами. Тобто операція додавання в G замкнена.

2) Операція додавання для всіх квадратних матриць асоціативна, тому ї для матриць з множини G асоціативний закон додавання виконується.

3) Нульовим елементом в множині G є: $\theta = \begin{pmatrix} 0 & 5 \cdot 0 \\ 0 & 0 \end{pmatrix}$. Цей елемент належить G, оскільки $a = b = c = 0$ – ціле число.

4) Знайдемо для довільного елемента $\alpha \in G$ протилежний елемент. $\alpha = \begin{pmatrix} a_1 & 5b_1 \\ c_1 & a_1 \end{pmatrix}$ ($a_1, b_1, c_1 \in \mathbf{Z}$). Очевидно, що $-\alpha = \begin{pmatrix} -a_1 & 5(-b_1) \\ -c_1 & -a_1 \end{pmatrix} \in G$.

Отже, множина G є адитивною групою.

Приклад 5.3. *У мультиплікативній групі всіх неособливих матриць 2-го порядку знайти порядок елемента* $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$A^2 = A \cdot A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$A^3 = A^2 \cdot A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

$$A^4 = A^3 \cdot A = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E,$$

Отже, порядок елемента A: $\mathrm{P}(A) = 4$.

6 ГРУПИ ПІДСТАНОВОК

Множину n перших натуральних чисел, записаних у деякому певному порядку, називають *перестановкою* з n чисел. Перестановку з n чисел в загальному вигляді записують так:

$$(i_1, i_2, \ldots, i_n).$$

У цьому записі кожен із символів i_s ($s = 1, 2, ..., n$) означає одне з чисел $1, 2, ..., n$, причому жодне з цих чисел не зустрічається двічі.

Теорема 6.1. *Кількість різних перестановок, які можна утворити з n чисел, дорівнює* $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

Перестановку, в якій n перших натуральних чисел розташовані в порядку зростання, називатимемо *нормально впорядкованою*:

$$(1, 2, ..., n).$$

Інверсією називають таке розміщення двох чисел у перестановці, коли більше число стоїть ліворуч меншого.

Перестановку називають *парною*, якщо вона має парне число інверсій, і *непарною*, якщо число інверсій у ній непарне.

Наприклад, підрахуємо число інверсій в перестановці

$$(3, 1, 5, 4, 2).$$

Для “1” – 1, для “2” – 3, для “3” – 0, для “4” – 1, для “5” – 0. Загальне число інверсій дорівнює 5, отже перестановка є непарною.

Теорема 6.2. *Кількість парних перестановок з* n *чисел* ($n \geq 2$) *дорівнює кількості непарних, тобто* $\dfrac{n!}{2}$.

Транспозицією називають операцію переставлення місцями двох елементів перестановки при умові, що інші елементи залишаються на своїх місцях.

Теорема 6.3. *Одна транспозиція змінює парність перестановки*.

Відображення φ множини A на множину B називають *взаємно однозначним*, якщо для нього виконуються умови:

1) $\forall\, a \in A \quad \exists!\ b \in B: \quad \varphi(a) = b$,
2) $\forall\, b \in B \quad \exists\ a \in A: \quad \varphi(a) = b$,
3) $\forall\, a_1, a_2 \in A \quad a_1 \neq a_2 \;\Rightarrow\; \varphi(a_1) \neq \varphi(a_2)$.

Означення. Кожне взаємно однозначне відображення множини перших n натуральних чисел на себе називають *підстановкою n-го степеня* і записують:

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Наприклад, при $n = 5$

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

Будемо говорити, що в цьому випадку число 2 *переходить* в 1, число 5 переходить в 3, число 4 переходить в 4 (або *залишається на місці*), число 3 переходить в 2, 1 – в 5. Тобто ми задали відображення, яке кожному з натуральних чисел 1, 2, 3, 4, 5 ставить у відповідність одне з цих же натуральних чисел, причому двом різним числам ставляться у відповідність різні числа.

Таким чином, кожну підстановку n-го степеня складають дві перестановки з n чисел.

Числом інверсій підстановки називають суму числа інверсій в двох її перестановках. Якщо це число парне, то підстановку називають *парною*, якщо це число непарне, то – *непарною*.

Теорема 6.4. *Якщо в підстановці поміняти місцями два стовпчики, то підстановка не змінить своєї парності.*

Наслідок. *Якщо стовпчики підстановки перемістити так, щоб верхня перестановка була нормально впорядкованою, то парність підстановки не зміниться.*

Отже підстановки зручніше записувати так:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \beta_1 & \beta_2 & \beta_3 & \dots & \beta_n \end{pmatrix}.$$

Враховуючи цей факт, з теореми 1 випливає:

Теорема 6.5. *Кількість різних підстановок n-го степеня дорівнює* $n!$

Оскільки підстановка – це відображення, то можемо розглянути композицію двох таких відображень.

Означення. *Добутком* підстановки $A = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ на підстановку $B = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$ називають підстановку C, що є результатом послідовного виконання підстановок A та B, тобто

$$C = A \cdot B = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \cdot \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}.$$

Теорема 6.6. *Множина S_n всіх підстановок n-го степеня* $(n \geq 3)$ *є некомутативною групою відносно операції множення.*

Одиничним елементом цієї групи є: $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$ – *тотожня підстановка*.

Оберненою до підстановки $A = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ є підстановка $A^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$

Групу S_n називають *симетричною групою n-го степеня*, вона складається з $n!$ елементів.

Приклад 6.1. *Описати симетричну групу S_3.*

$n = 3$, $n! = 1 \cdot 2 \cdot 3 = 6$.

Елементи цієї групи позначимо:

$$a_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad a_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Знайдемо добутки цих елементів, результати зручно записати у таблицю (*таблицю Келі*):

•	a_0	a_1	a_2	a_3	a_4	a_5
a_0	a_0	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_0	a_5	a_4	a_3	a_2
a_2	a_2	a_4	a_0			
a_3	a_3					
a_4	a_4					
a_5	a_5					

Наприклад, $a_1 \cdot a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = a_0$,

$$a_1 \cdot a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a_5 \quad \text{і т д.}$$

З таблиці Келі скінченної групи можна встановити замкненість групової операції, її комутативність, знайти обернений до кожного елемента, визначити порядок кожного елемента.

Також з неї можна визначити всі підгрупи заданої групи.

Однією з них є підгрупа $A = \{a_0\}$.

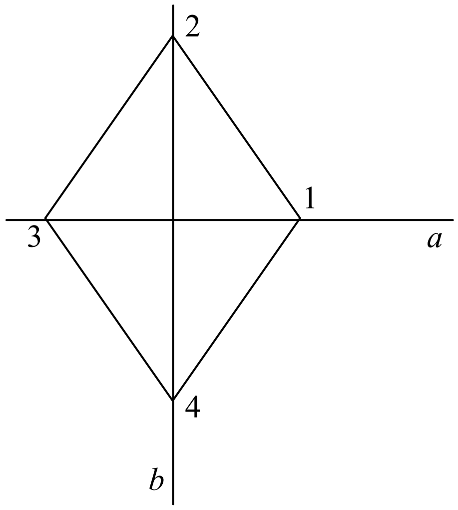
Знайдемо підгрупу B, яка містить елемент a_1. Ця підгрупа має містити і добуток $a_1 \cdot a_1 = e$. Отже $B = \{e, a_1\} = \langle a_1 \rangle$, $|a_1| = 2$.

Заповніть таблицю Келі та знайдіть всі підгрупи групи S_3.

Приклад 6.2. *Описати групу G самосуміщень ромба.*

Самосуміщенням фігури F називають таке перетворення (рух) в просторі або на площині, при якому F переходить в F.

Вершини ромба позначимо цифрами 1, 2, 3, 4.



Тоді елементи цієї групи (перетворення) описують підстановки:

тотожне перетворення $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$,

симетрія відносно діагоналі

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

симетрія відносно діагоналі

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

знайдемо добуток елементів a та b:

$$a \cdot b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ – поворот на } 180°,$$

таким чином, маємо ще один елемент групи, позначимо його c.

Побудуємо таблицю Келі для групи G:

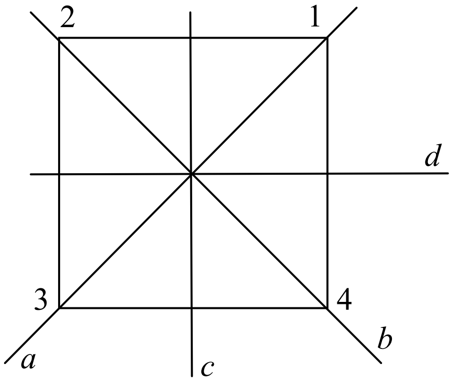
•	***e***	***a***	***b***	***c***
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

Бачимо, що інших елементів група G не містить. Отже група самосуміщень ромба складається з чотирьох елементів:

$$G = \{e, a, b, c\}.$$

Ця група є комутативною, нециклічною, всі елементи цієї групи, крім e, мають порядок 2.

Приклад 6.3. *Описати групу G самосуміщень квадрата.*
Вершини квадрата позначимо цифрами 1, 2, 3, 4.



Елементами групи G є:

тотожне перетворення $e=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$,

симетрія відносно діагоналі $a=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix}$,

симетрія відносно діагоналі $b=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix}$,

симетрія відносно серединного перпендикуляра $c=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$,

симетрія відносно серединного перпендикуляра $d=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}$,

поворот на 90° навколо центра квадрата $r_1=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}$,

поворот на 180° навколо центра квадрата $r_2=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}$,

поворот на 270° навколо центра квадрата $r_3=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$.

Побудуйте таблицю Келі та знайдіть всі підгрупи групи G.

Відмітимо, що група S_3 з прикладу 6.1 є групою самосуміщень правильного трикутника.

П р и к л а д и   г р у п

Нескінченні

Комутативні

- (**Z**, +) - адитивна група цілих чисел
- (**Q**, +) - адитивна група раціональних чисел
- (**R**, +) - адитивна група дійсних чисел
- (**C**, +) - адитивна група комплексних чисел
- (M, +) - адитивна група матриць n-го порядку з дійсними елементами
- (L, +) - адитивна група n-вимірних векторів з дійсними елементами

- (**Q** \ {**0**}, *) - мультиплікативна група ненульових рац. чисел
- (**R** \ {**0**}, *) - мультиплікативна група ненульових дійсних чисел
- (**C** \ {**0**}, *) - мультиплікативна група ненульових компл. чисел

Некомутативні

- (K, *) - мультиплікативна група невироджених матриць n-го порядку з дійсними елементами

Скінченні

Комутативні

Циклічні

- Група коренів n-го степеня з 1
- $G = \langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$
- Всі групи, порядок яких є простим числом

Нециклічні

- Група самосуміщень ромба порядку 4

Некомутативні

- Група самосуміщень прав. трикутника (симетрична група S_3) порядку 6
- Група самосуміщень квадрата порядку 8
- Група кватерніонів порядку 8

7 КІЛЬЦЕ. ПОЛЕ

Кільце. Підкільце

Означення. *Кільцем* називають непорожню множину K, в якій введено дві бінарні операції: додавання і множення, та виконуються такі умови:

1) – 5) множина K є комутативною групою відносно операції додавання;

6) операція множення замкнена, тобто

$$\forall\, a, b \in K \quad a \cdot b \in K;$$

7) операція множення асоціативна, тобто

$$\forall\, a, b, c \in K \quad (a \cdot b) \cdot c = a \cdot (b \cdot c);$$

8) операція множення дистрибутивна відносно додавання, тобто

$$\forall\, a, b, c \in K \qquad (a + b) \cdot c = a \cdot c + b \cdot c,$$
$$c \cdot (a + b) = c \cdot a + c \cdot b.$$

Умови 1) – 8) називають *аксіомами кільця*.

Якщо операція множення комутативна, то кільце називають *комутативним*.

Якщо кільце містить нейтральний елемент відносно операції множення, то його називають *кільцем з одиницею*.

Приклади кілець: ($\mathbf{Z}$, +, ·), (2$\mathbf{Z}$, +, ·), ($\mathbf{Q}$, +, ·), множина M_n матриць n-го порядку з дійсними елементами відносно операцій додавання і множення.

***Властивості кільця*:**

З того, що $(K, +)$ є комутативною групою, випливає, що для операції додавання в K справджуються властивості 1 – 3 груп. Тобто

1. *В кожному кільці існує, і притому тільки один, нульовий елемент* θ, який називають *нулем кільця*.

2. *В кожному кільці K для будь-якого його елемента a існує, і притому тільки один, протилежний йому елемент $-a$.*

3. *Для будь-яких елементів a, b кільця K рівняння $a + x = b$ має в K єдиний розв'язок.*

Розв’язок цього рівняння $x = b + (-a)$ називають різницею елементів b і a і позначають $b - a$. Таким чином, *різницею* двох елементів b, a називається такий елемент x, який в сумі з a дає b.

4. $\forall\, a, b, c \in K \qquad (a - b) \cdot c = a \cdot c - b \cdot c,$

$$c \cdot (a - b) = c \cdot a - c \cdot b.$$

5. $\forall\, a \in K \qquad a \cdot \theta = \theta \cdot a = \theta.$

6. $\forall\, a, b \in K \qquad (-a) \cdot b = -ab, \qquad a \cdot (-b) = -ab,$

$$(-a) \cdot (-b) = ab.$$

Однак не слід думати, що кожна властивість дій додавання і множення чисел зберігається для алгебраїчних операцій у будь-якому кільці.

Означення. Відмінні від нуля елементи a і b кільця K називають *дільниками нуля*, якщо їх добуток дорівнює нулю.

Наприклад, матриця $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ є нульовим елементом, або просто нулем в кільці M_2 матриць другого порядку з дійсними елементами. Матриці $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$ відмінні від нульової матриці, але

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

тобто ці матриці є дільниками нуля в кільці M_2.

Означення. Підмножину K_1 кільця K називають *підкільцем* цього кільця, якщо K_1 є кільцем відносно операцій додавання і множення, визначених в кільці K.

Теорема 7.1 (*Критерій підкільця*). *Для того, щоб непорожня підмножина K_1 кільця K була його підкільцем, необхідно й достатньо, щоб сума, різниця і добуток будь-яких двох елементів a і b підмножини K_1 належали до K_1.*

Наприклад, підмножина $2\mathbf{Z}$ парних цілих чисел є підкільцем кільця $\mathbf{Z}$ цілих чисел.

Область цілісності

З означення кільця не випливає існування або відсутність в даному кільці K одиниці e. Якщо в кільці K одиничний елемент існує, то тільки один.

Наприклад, кільце $2\mathbf{Z}$ парних цілих чисел є кільцем без одиниці.

Означення. Елементи a і b кільця K, які в добутку дають одиницю називають *дільниками одиниці:*

$$a \cdot b = e.$$

З цієї рівності випливає, що $b = a^{-1}$, $a = b^{-1}$. Тому *дільник одиниці – це елемент, для якого в кільці існує обернений елемент*.

Наприклад, в кільці цілих чисел $\mathbf{Z}$ дільниками одиниці є ± 1.
В кільці цілих гауссових чисел $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ дільниками одиниці є:

$$\pm 1, \pm i.$$

Теорема 7.2. Множина K^* всіх дільників одиниці кільця K є мультиплікативною групою.

Означення. Комутативне кільце з одиницею без дільників нуля називають *областю цілісності*.

Наприклад, числові кільця є областю цілісності.

Поле. Підполе

Означення. Комутативне кільце з одиницею, в якому для кожного відмінного від нуля елемента a існує обернений елемент a^{-1}, називають *полем*.

Отже, поле P є комутативною групою відносно операції додавання, а множина $P \setminus \{\theta\}$ є комутативною групою відносно множення.

Приклади полів: $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$.

***Властивості поля*:**

Оскільки кожне поле є комутативним кільцем, то всі наведені вище властивості кілець правильні також і для будь-якого поля. Розглянемо інші властивості поля:

1. *В кожному полі існує, і притому тільки один, одиничний елемент.*

2. *В кожному полі для будь-якого відмінного від нуля елемента a існує, і притому тільки один, обернений елемент a^{-1}.*

3. *Жодне поле P не містить дільників нуля.*

Означення. Підмножину P_1 поля P називають *підполем* цього поля, якщо вона сама є полем відносно алгебраїчних операцій, визначених у полі P. Поле P в цьому випадку називають *розширенням* поля P_1.

Наприклад, $\mathbf{Q}$ – підполе $\mathbf{R}$.

Теорема 7.3. *Множина комплексних чисел* $\mathbf{C}$ *з визначеними в ній операціями додавання і множення є полем.*

Теорема 7.4 (*Критерій підполя*). *Для того, щоб непорожня підмножина P_1 поля P була його підполем, необхідно й достатньо, щоб сума, різниця, добуток і частка (при умові, що вона існує) будь-яких двох елементів a і b підмножини P_1 належали до P_1.*

8 ІЗОМОРФІЗМ АЛГЕБРАЇЧНИХ СТРУКТУР

Абстрактне поняття групи (кільця, поля) дає змогу одночасно вивчати спільні властивості багатьох різних множин з введеними у них алгебраїчними операціями – всіх множин, що є групами (кільцями, полями) і глибше досліджувати природу алгебраїчних операцій, абстрагуючись від конкретних об'єктів їх застосування.

Наявність таких спільних властивостей не виключає того, що різні групи (кільця, поля) можуть істотно відрізнятися між собою своєю будовою, мати різні індивідуальні особливості. Так, наприклад, є скінченні групи і нескінченні; кільця без дільників нуля і кільця з дільниками нуля і т.п.

Проте це не означає, що кожну групу (кільце, поле) треба вивчати окремо. Уважно розглядаючи приклади конкретних алгебраїчних структур, можна помітити, що в деяких з них властивості цілком аналогічні.

Наприклад, розглянемо мультиплікативну групу G всіх цілих степенів числа 5:

$$\dots, 5^{-n}, 5^{-(n-1)}, \dots, 5^{-1}, 5^0 = 1, 5^1, \dots, 5^{n-1}, 5^n, \dots$$

і адитивну групу $\mathbf{Z}$ всіх цілих чисел:

$$\dots, -n, -(n-1), \dots, -1, 0, 1, \dots, n-1, n, \dots .$$

Порівняємо ці дві групи. Кожному елементу 5^n групи G поставимо у відповідність елемент n (його показник) із $\mathbf{Z}$. Цим, очевидно, буде задано взаємно однозначне відображення групи G на групу $\mathbf{Z}$, причому таке, що

$$5^k \cdot 5^l = 5^{k+l} \quad \to \quad k + l .$$

Звідси випливає, що будь-яке доведене нами твердження про множення елементів із G може бути перетворене у відповідне твердження про додавання елементів із $\mathbf{Z}$ і навпаки, треба тільки замінити 5^n на n, $5^k \cdot 5^l$ на $k + l$. Тому ці дві групи не можна вважати істотно різними.

Подібність двох конкретних алгебраїчних структур M і M_1 одного і того ж типу проявляється насамперед у можливості встановити взаємно однозначну відповідність між елементами множин M і M_1 . Крім цього повинна існувати взаємно однозначна відповідність і між алгебраїчними операціями, введеними в цих множинах.

Означення. Відображення φ множини A на множину B називають *взаємно однозначним*, якщо для нього виконуються умови:

1) $\forall\, a \in A \quad \exists!\ \ b \in B: \quad \varphi(a) = b$,

2) $\forall\, b \in B \quad \exists\ \ a \in A: \quad \varphi(a) = b$,

3) $\forall\, a_1, a_2 \in A \quad a_1 \neq a_2 \ \Rightarrow\ \varphi(a_1) \neq \varphi(a_2)$.

Означення. Нехай G і G_1 — групи з груповими операціями $*$ і $\circ$ відповідно. Групи G і G_1 називають *ізоморфними*, якщо між їх елементами можна встановити таке взаємно однозначне відображення φ , при якому

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) \qquad \forall\, a, b \in G.$$

Позначення для ізоморфних груп: $G \cong G_1$.

Відображення φ при цьому називають *ізоморфізмом* групи G на групу G_1.

Властивості ізоморфізму груп:

При будь-якому ізоморфізмі φ групи G на групу G_1:

1) *нейтральному елементу групи* G *відповідає нейтральний елемент групи* G_1;

2) *будь-якій парі взаємно симетричних елементів* g *і* $g`$ *групи* G *відповідає пара взаємно симетричних елементів групи* G_1.

Означення. Кільця (поля) K і K_1 називають *ізоморфними*, якщо між їх елементами можна встановити таке взаємно однозначне відображення φ, при якому

$$\varphi(a+b)=\varphi(a)+\varphi(b),$$
$$\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b) \qquad \forall\, a, b \in K.$$

***Властивості ізоморфізму кілець (полів)*:**

1. $\varphi(\theta)=\theta_1$, де $\theta_1 \in K_1$;

2. $\varphi(-a)=-\varphi(a)$;

3. $\varphi(e)=e_1$, де $e_1 \in K_1$;

4. $\varphi(a^{-1})=[\varphi(a)]^{-1}$.

Приклад 8.1. *Довести, що адитивна група* $3\mathbf{Z}$ *цілих чисел, кратних числу* 3 *ізоморфна мультиплікативній групі цілих степенів числа 7.*

Позначимо

$$G_1=\{\,3k \mid k \in \mathbf{Z}\,\},$$
$$G_2=\{\,7^m \mid m \in \mathbf{Z}\,\}.$$

Задамо відображення φ:

$$\varphi:\quad 3k \;\to\; 7^k,$$

тобто $\varphi(3k)=7^k \quad \forall\, k \in \mathbf{Z}$.

I. Покажемо, що відображення φ є взаємно однозначним, для цього перевіримо умови взаємно однозначного відображення:

1) $\forall\, a=3k \in G_1 \quad \exists!\; b=7^k \in G_2: \quad \varphi(a)=b,$

2) $\forall\, b=7^k \in G_2 \quad \exists\; a=3k \in G_1: \quad \varphi(a)=b,$

3) $\forall\, a_1, a_2 \in G_1 \quad a_1 \ne a_2 \;\Rightarrow\; 3k_1 \ne 3k_2 \;\Rightarrow\; k_1 \ne k_2 \;\Rightarrow$
$\Rightarrow\; 7^{k_1} \ne 7^{k_2} \;\Rightarrow\; \varphi(a_1) \ne \varphi(a_2).$

II. Покажемо, що відображення φ „зберігає операцію”:

$$\varphi(a_1+a_2)=\varphi(3k_1+3k_2)=\varphi(\,3(k_1+k_2)\,)=$$
$$=7^{k_1+k_2}=7^{k_1}\cdot 7^{k_2}=\varphi(a_1)\cdot\varphi(a_2).$$

Таким чином група $(G_1, +)$ ізоморфна групі $(G_2, \cdot)$.

9 ПОДІЛЬНІСТЬ В ОБЛАСТІ ЦІЛІСНОСТІ. ДІЛЕННЯ З ОСТАЧЕЮ

Операція ділення в кільці не завжди здійсненна.

Нехай K – комутативне кільце.

Вважають, що елемент $a \in K$ *ділиться* на елемент $b \in K$ (або елемент b *ділить* елемент a), якщо в кільці K існує такий елемент c, що

$$a = b \cdot c.$$

Записують $a \vdots b$ або $b \mid a$.

Елемент b називають *дільником* елемента a. Елемент a називають *кратним* елемента b.

В кільці цілих чисел $\mathbf{Z}$ $35 \vdots 5$, $34 \not\vdots 5$.

В кільці парних цілих чисел $2\mathbf{Z}$ $6 \not\vdots 2$, оскільки $6 = 2 \cdot 3$, але $3 \notin 2\mathbf{Z}$.

Якщо K – некомутативне кільце, то може бути, що $a = b \cdot c$, але $a \neq c \cdot b$. В цьому випадку b називають *лівостороннім дільником* елемента a і він не є правостороннім дільником елемента a.

Властивості подільності:

Нехай K – комутативне кільце.

1. $\forall\, a \in K \quad \theta \vdots a$.

2. $\forall\, a \in K \quad a \neq \theta \quad a \vdots a, \quad a \vdots e$ *в кільці K з одиницею e.*

3. *Відношення подільності є транзитивним, тобто*

$$\forall\, a, b, c \in K \quad a \vdots b \text{ і } b \vdots c \Rightarrow a \vdots c.$$

4. $\forall\, a, b, c \in K \quad a \vdots c$ і $b \vdots c \Rightarrow (a \pm b) \vdots c$.

Наслідок 1. *Якщо* $(a+b) \vdots c$ *і* $a \vdots c$, *то* $b \vdots c$.

Наслідок 2. *Якщо* $a \vdots c$, $b \not\vdots c$, *то* $(a+b) \not\vdots c$.

5. $\forall\, a, b, c \in K \quad a \vdots b \Rightarrow ac \vdots b$.

Асоційовані елементи

Нехай K – область цілісності (комутативне кільце з одиницею e без дільників нуля).

Означення. Елементи a, b області цілісності K називають *асоційованими*, якщо кожен з них є дільником іншого, тобто

$$a \vdots b \text{ і } b \vdots a.$$

Позначають $a \sim b$.

Якщо $a \sim b$, то $a \vdots b$ і $b \vdots a$, тобто $a = b \cdot q_1$, $b = a \cdot q_2$ $(q_1, q_2 \in K)$, звідси

$$a = b \cdot q_1 = (a \cdot q_2) \cdot q_1 = a \cdot (q_2 \cdot q_1),$$

і оскільки елемент a не може бути нулем кільця, то $q_2 \cdot q_1 = e$, тобто q_2, q_1 – дільники одиниці кільця K.

Теорема 9.1. *Елементи a, b області цілісності K тоді і тільки тоді є асоційованими, коли $a = b \cdot \varepsilon$, де ε – дільник одиниці кільця K.*

В кільці цілих чисел $\mathbf{Z}$ дільниками одиниці є ± 1, тому в цьому кільці елементи 5 та -5 є асоційованими.

В кільці цілих гауссових чисел $\mathbf{Z}[i]$ дільниками одиниці є: $\pm 1, \pm i$, отже

$$2,\ -2,\ 2i,\ -2i$$

асоційовані в ньому.

До властивостей подільності слід додати ще таку:

6. *Якщо елемент $a \in K$ ділиться на елемент $b \in K$, то a ділиться і на всі асоційовані до b елементи*:

$$\forall\, a, b \in K \quad a \,\vdots\, b \quad \Rightarrow \quad a \,\vdots\, b\varepsilon,$$

де ε – дільник одиниці.

Наслідок. *Всі елементи, асоційовані з елементом a, і всі дільники одиниці є дільниками елемента a.*

Їх називають *тривіальними дільниками елемента a.*

Ділення з остачею в кільці цілих чисел

Теорема 9.2. *Для будь-яких цілих чисел a, b $(b \neq 0)$ існують цілі числа q, r такі, що*

$$a = bq + r, \quad \text{де} \quad 0 \le r < |\, b \,|,$$

і пара таких чисел визначається однозначно.

Число q називають *неповною часткою*, число r називають *остачею* при діленні числа a на b.

Наслідок. *Ціле число a тоді й тільки тоді ділиться на ціле число b, коли остача від ділення a на b дорівнює нулю.*

Приклад 9.1. *Знайти неповну частку й остачу при діленні числа a на b*:

1) $a = -25$, $b = 3$

$$25 = 3 \cdot 8 + 1,$$
$$-25 = 3 \cdot (-8) - 1 + 3 - 3,$$
$$-25 = 3 \cdot (-9) + 2.$$

2) $a = 25$, $b = -3$

$$25 = 3 \cdot 8 + 1,$$
$$25 = (-3) \cdot (-8) + 1.$$

3) $a = -25$, $b = -3$

$$25 = 3 \cdot 8 + 1,$$
$$-25 = (-3) \cdot 8 - 1 + 3 - 3,$$
$$-25 = (-3) \cdot 9 + 2.$$

Приклад 9.2. *Довести, що з трьох послідовних цілих чисел одне і тільки одне ділиться на* 3.

Розглянемо три послідовних цілих числа:

$$a,\ a + 1,\ a + 2.$$

Оскільки $a \in \mathbf{Z}$, то можливий один з трьох випадків:

$$a = 3q\ \ (q \in \mathbf{Z}),\ \text{ або }\ a = 3q + 1,\ \text{ або }\ a = 3q + 2.$$

Якщо $a = 3q$, то $a \vdots 3$,

$$a + 1 = 3q + 1 \not\vdots 3,$$
$$a + 2 = 3q + 2 \not\vdots 3.$$

Якщо $a = 3q + 1$, то $a + 2 = 3q + 3 = 3(q + 1) \vdots 3$, при цьому

$$a = 3q + 1 \not\vdots 3,$$
$$a + 1 = 3q + 2 \not\vdots 3.$$

Якщо $a = 3q + 2$, то $a + 1 = 3q + 3 = 3(q + 1) \vdots 3$, при цьому

$$a = 3q + 2 \not\vdots 3,$$
$$a + 2 = 3q + 4 \not\vdots 3.$$

Аналогічно можна довести, що *з n послідовних цілих чисел одне і тільки одне ділиться на n.*

Приклад 9.3. *Довести, що добуток трьох послідовних цілих чисел ділиться на* 6.

Позначимо $A = a \cdot (a + 1) \cdot (a + 2)$.

За доведеним в прикладі 9.2, $A \vdots 2$, оскільки містить два послідовні цілі числа, аналогічно $A \vdots 3$, при цьому множники 2 та 3 не мають спільних дільників (крім 1), тому $A \vdots 6$.

Приклад 9.4. *Довести, що з двох сусідніх парних чисел* b та $b + 2$ *одне ділиться на 2, інше – на 4.*

Дійсно, в числах $b = 2k$ та $b + 2 = 2k + 2$ сам параметр k може бути парним або непарним, в першому випадку

$$b = 2k = 2(2m) \vdots 4,$$
$$b + 2 = 2k + 2 = 2(2m) + 2 = 4m + 2 \vdots 2,$$

в другому випадку

$$b = 2k = 2(2m + 1) \vdots 2,$$
$$b + 2 = 2k + 2 = 2(2m + 1) + 2 = 4m + 4 \vdots 4.$$

Приклад 9.5. *Довести, що добуток чотирьох послідовних цілих чисел ділиться на 24.*

Число $A = a \cdot (a + 1) \cdot (a + 2) \cdot (a + 3)$ містить принаймні два парних числа, причому вони є сусідніми парними числами. За доведеним в прикладі 9.4, один з цих множників ділиться на 2, інший на 4, тому число A ділиться на 8.

До того ж $A \,\vdots\, 3$, бо містить три послідовні цілі числа.

Отже $A \,\vdots\, 24$.

Приклад 9.6. *Довести, що для будь-якого цілого* n $\left(n^3 - n\right) \vdots\, 6$.

$$\left(n^3 - n\right) = n\left(n^2 - 1\right) = \underbrace{\underbrace{(n-1)n}_{\vdots 2}(n+1)}_{\vdots 3} \quad \vdots\, 6$$

Приклад 9.7. *Довести, що для будь-якого цілого* n $\left(n^5 - n\right) \vdots\, 30$.

$$\left(n^5 - n\right) = n\left(n^4 - 1\right) = n\left(n^2 - 1\right)\left(n^2 + 1\right) =$$

$$= (n-1)n(n+1)\left(n^2 + 1\right) =$$

$$= (n-1)n(n+1)\left(n^2 - 4 + 5\right) =$$

$$= \underbrace{\underbrace{\underbrace{(n-2)(n-1)}_{\vdots 2}n}_{\vdots 3}(n+1)(n+2)}_{\vdots 5} + 5\underbrace{\underbrace{(n-1)n}_{\vdots 2}(n+1)}_{\vdots 3} \quad \vdots\, 30$$

Зауважимо, що за умови, коли $n \in \mathbf{N}$ в прикладах типу 9.6 та 9.7 для доведення можна застосувати метод математичної індукції.

10 ОЗНАКИ ПОДІЛЬНОСТІ

Цифровий запис числа A – це певне представлення цього числа в системі числення з основою g ($g \in \mathbf{N}$):

$$A = a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + ... + a_2 \cdot g^2 + a_1 \cdot g + a_0.$$

Коефіцієнти a_0, a_1, a_2, ..., a_n називають *цифрами* (або *розрядними одиницями*) системи числення з основою g, очевидно, що

$$0 \le a_i \le g - 1, \quad a_n \ne 0.$$

Ми зазвичай користуємось десятковою системою числення, тобто $g = 10$, тоді кожне число подається у вигляді суми розрядних одиниць:

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0,$$

$$0 \le a_i \le 9, \quad a_n \ne 0.$$

при цьому a_0 – називають цифрою одиниць, a_1 – цифрою десятків, a_2 – цифрою сотен і т.д.

Наприклад, $2345 = 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 5$.

З'ясуємо, як не виконуючи ділення, а скориставшись лише цифровим записом числа в десятковій системі числення встановлювати деякі закономірності подільності заданого числа.

Ознака подільності на 2 (на 5, на 10)

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 =$$
$$= 10\left(a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + ... + a_2 \cdot 10 + a_1\right) + a_0 =$$
$$= 2 \cdot 5 \cdot K + a_0.$$

Число A ділиться на 2 (на 5, на 10) тоді і тільки тоді, коли число a_0 (остання цифра числа A) ділиться на 2 (на 5, на 10).

Ознака подільності на 4 (на 25, на 50)

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 =$$
$$= 100\left(a_n \cdot 10^{n-2} + a_{n-1} \cdot 10^{n-3} + ... a_3 \cdot 10 + a_2\right) + a_1 \cdot 10 + a_0 =$$
$$= 4 \cdot 25 \cdot K + a_1 \cdot 10 + a_0.$$

Число A ділиться на 4 (на 25, на 50) тоді і тільки тоді, коли число, записане останніми двома цифрами числа A, ділиться на 4 (на 25, на 50).

Ознака подільності на 8 (на 125)

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 =$$
$$= 1000\left(a_n \cdot 10^{n-3} + a_{n-1} \cdot 10^{n-4} + ... + a_3\right) + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 =$$
$$= 8 \cdot 125 \cdot K + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Число A *ділиться на 8 (на 125) тоді і тільки тоді, коли число, записане останніми трьома цифрами числа* A, *ділиться на 8 (на 125).*

Ознака подільності на 3 (на 9)

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 =$$
$$= a_n \cdot \left(9t+1\right) + \ldots + a_3 \cdot (999+1) + a_2 \cdot \left(99+1\right) + a_1 \cdot \left(9+1\right) + a_0 =$$
$$= 9 \cdot K + \left(a_n + \ldots + a_3 + a_2 + a_1 + a_0\right)$$

Число A *ділиться на 3 (на 9) тоді і тільки тоді, коли сума цифр цього числа ділиться на 3 (на 9).*

Ознака подільності на 11

$$A = a_n \cdot 10^n + \ldots + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 =$$
$$= a_n \cdot 10^n + \ldots + a_4 \cdot \left(9999+1\right) + a_3 \cdot (1001-1) + a_2 \cdot \left(99+1\right) + a_1 \cdot \left(11-1\right) + a_0 =$$
$$= 11 \cdot K + \left(a_0 + a_2 + a_4 + \ldots\right) - \left(a_1 + a_3 + a_5 + \ldots\right).$$

Число A *ділиться на 11 тоді і тільки тоді, коли різниця між сумою цифр цього числа, які стоять на непарних місцях, і сумою цифр, які стоять на парних місцях, ділиться на 11.*

Наприклад, для числа $A = 1642375$: $(5 + 3 + 4 + 1) - (7 + 2 + 6) = -2$, отже число A не ділиться на 11.

Приклад 10.1. *Знайти цифри* a, b *так, щоб число* $A = \overline{2001ab} \vdots 44$.

Оскільки $A \vdots 44 \;\Leftrightarrow\; \begin{cases} A \vdots 11 & \Rightarrow \left((b+1+0)-(a+0+2)\right) \vdots 11 \\ A \vdots 4 & \Rightarrow \left(a \cdot 10 + b\right) \vdots 4 \end{cases}$

Отже

$$\begin{cases} \left(b-a-1\right) \vdots 11, \\ \left(2a+b\right) \vdots 4. \end{cases}$$

Тобто

$$\begin{cases} b-a = 1+11k, & k \in \mathbf{Z}, \\ 2a+b = 4t, & t \in \mathbf{Z}. \end{cases}$$

Зауважимо, що a, b – цифри, отже $0 \le a \le 9$, $0 \le b \le 9$.
Звідси $-9 \le -a \le 0$, тому $-9 \le b-a \le 9$.
Таким чином, з першої умови системи випливає, що $b-a=1$.
З другої умови дістанемо $2a+b = 2a + \left(1+a\right) = 3a+1 \vdots 4$.
Враховуючи, що $0 \le a \le 9$, можливі випадки

$$a=1 \quad \text{або} \quad a=5.$$

Якщо $a=1$, то $b=1+a=2$. Якщо $a=5$, то $b=1+a=6$.

11 НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК. АЛГОРИТМ ЕВКЛІДА

Означення. Кільце K називають *евклідовим*, якщо:

1) K є областю цілісності (комутативним кільцем з одиницею, без дільників нуля);

2) існує відображення $\psi\colon\ K \setminus \{\theta\} \to \mathbf{N} \cup \{0\}$, при якому

3) $\forall\ a, b \in K \quad (b \neq \theta) \qquad \exists\ q, r \in K\colon \qquad a = bq + r$,

і якщо $r \neq \theta$, то $\psi\,(r) < \psi\,(b)$.

Тобто в евклідовому кільці можливе ділення з остачею.

Теорема 11.1. *Кільце цілих чисел* $\mathbf{Z}$ *є евклідовим кільцем.*

Нехай K – область цілісності.

Елемент c області цілісності K називають *спільним дільником* елементів $a, b \in K$, якщо кожен з цих елементів ділиться на c, тобто

$$a \,\vdots\, c \quad \text{і} \quad b \,\vdots\, c.$$

Означення. *Найбільшим спільним дільником* (НСД) елементів $a, b \in K$ називають такий спільний дільник d цих елементів, який ділиться на будь-який інший їх спільний дільник.

Позначають

$$d = \text{НСД}\,(a, b), \text{ або } \ d = (a, b).$$

З цього означення випливає, що НСД двох елементів області цілісності K визначається неоднозначно. *НСД двох елементів області цілісності K визначається з точністю до асоційованих* (*з точністю до множника* ε, *що є дільником одиниці кільця* K).

В кільці $\mathbf{Z}$ домовляються в ролі НСД (a, b) брати додатне число.

Наприклад, в кільці для чисел $a = 30$, $b = 75$ спільними дільниками є

$$\pm 1,\ \pm 3,\ \pm 5,\ \pm 15,$$

НСД (30, 75) = 15.

Нехай задано два цілих числа a та b.

За теоремою про ділення з остачею

$$a = bq_0 + r_0, \quad \text{де} \quad 0 < r_0 < |\,b\,|,$$

далі поділимо b на r_0 з остачею:

$$b = r_0\,q_1 + r_1, \quad \text{де} \quad 0 < r_1 < r_0,$$

$$r_0 = r_1\,q_2 + r_2, \quad \text{де} \quad 0 < r_2 < r_1,$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$r_{n-2} = r_{n-1}\,q_n + r_n, \quad \text{де} \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_n\,q_{n+1}, \quad \text{де} \quad r_{n+1} = 0.$$

Такий процес послідовного ділення називається *алгоритмом Евкліда* для чисел a та b.

Теорема 11.2. *Остання відмінна від нуля остача* r_n *при застосуванні до чисел* a *та* b *алгоритму Евкліда є найбільшим спільним дільником цих чисел*,

тобто НСД $(a, b) = r_n$.

Теорема 11.3 (*про існування і лінійне представлення НСД*). *Будь-які елементи* a, b $(b \neq \theta)$ *евклідового кільця* K *мають НСД, причому існують такі* $u, v \in K$, *що*

$$a \cdot u + b \cdot v = d \text{, де } d = \text{НСД } (a, b).$$

Наслідок. *Будь-які цілі числа* a, b $(b \neq \theta)$ *мають НСД.*

Взаємно прості елементи

Означення. Два елементи a, b області цілісності K називають *взаємно простими*, якщо їх найбільший спільний дільник дорівнює одиниці:

$$(a, b) = e.$$

Теорема 11.4 (*ознака взаємно простих елементів*). *Елементи* a, b евклідового *кільця* K *тоді і тільки тоді є взаємно простими, коли існують такі* $u, v \in K$, *що*

$$a \cdot u + b \cdot v = e.$$

Властивості взаємно простих елементів:

Нехай a, b, c – ненульові елементи евклідового кільця K.

1. *Якщо* $a \cdot b \vdots c$ *і* $(a, c) = e$, *то* $b \vdots c$.

2. *Якщо* $(a, b) = e$ *і* $(a, c) = e$, *то* $(a, bc) = e$.

3. *Якщо* $a \vdots b$ *і* $a \vdots c$, *причому* $(b, c) = e$, *то* $a \vdots b \cdot c$.

Найменше спільне кратне елементів кільця

Нехай K – область цілісності.

Елемент k області цілісності K називають *спільним кратним* елементів $a, b \in K$, якщо

$$k \vdots a \text{ і } k \vdots b.$$

Означення. *Найменшим спільним кратним* (НСК) елементів $a, b \in K$ називають таке спільне кратне цих елементів, яке ділить будь-яке інше їх спільне кратне.

Позначають

$$m = \text{НСК } (a, b), \text{ або } m = [a, b].$$

Теорема 11.5. *Якщо* $a \neq \theta,\ b \neq \theta$, *то*

$$\text{НСК}(a,b) = \frac{a \cdot b}{\text{НСД}(a,b)}.$$

Приклад 11.1. *Знайти найбільший спільний дільник та найменше спільне кратне чисел* -546 та 231.

Із зауваження до означення найбільшого спільного дільника чисел випливає, що

$$\text{НСД}\,(-a, b) = \text{НСД}\,(a, b),$$

тому можна перейти до додатних чисел.

Алгоритм Евкліда для чисел 546 та 231 зручніше записувати в стовпчик як при діленні кутом:

$$
\begin{array}{rrrrrrr}
 & & & & & -546 & \underline{\big|\,231\quad} \\
 & & & & & \underline{462} & 2 = q_0 \\
 & & & -231 & \big| & \underline{84} & = r_0 \\
 & & & \underline{168} & 2 = q_1 & & \\
 & -84 & \big| & \underline{63} & = r_1 & & \\
 & \underline{63} & 1 = q_2 & & & & \\
-63 \;\big| & \underline{21} & = r_2 & & & & \\
\underline{63} & 3 = q_3 & & & & & \\
0 = r_3 & & & & & &
\end{array}
$$

$r_3 = 0$, отже НСД $(-546, 231)$ = НСД $(546, 231) = r_2 = 21$.

$$\text{НСК}\,(-546, 231) = \text{НСК}\,(546, 231) = \frac{546 \cdot 231}{21} = 546 \cdot 11 = 6006.$$

Приклад 11.2. *Знайти лінійне представлення найбільшого спільного дільника чисел* -546 та 231.

З попередньої задачі відновимо алгоритм Евкліда для чисел 546 та 231:

$$546 = 231 \cdot 2 + 84,$$
$$231 = 84 \cdot 2 + 63,$$
$$84 = 63 \cdot 1 + 21,$$
$$63 = 21 \cdot 3 + 0.$$

Починаючи з передостанньої рівності будемо виражати остачі:

$$21 = 84 - 63 \cdot 1 =$$
$$= 84 - (231 - 84 \cdot 2) \cdot 1 = 84 \cdot 3 - 231 \cdot 1 =$$
$$= (546 - 231 \cdot 2) \cdot 3 - 231 \cdot 1 = 546 \cdot 3 + 231 \cdot (-7).$$

Отже, лінійне представлення найбільшого спільного дільника чисел 546 та 231 має вигляд:

$$546 \cdot 3 + 231 \cdot (-7) = 21,$$

тоді запишемо лінійне представлення найбільшого спільного дільника чисел $a = -546$ та $b = 231$:

$$(-546)\cdot(-3) + 231\cdot(-7) = 21.$$

Приклад 11.3. *Знайти такі цілі додатні числа* a та b *з умови, що*

$$\begin{cases} a + b = 144, \\ (a,b) = 24. \end{cases}$$

Оскільки $(a, b) = 24$, то

$$\begin{cases} a \,\vdots\, 24 \\ b \,\vdots\, 24 \end{cases} \Rightarrow \begin{cases} a = 24a_1 \\ b = 24b_1 \end{cases} \quad \text{причому } (a_1, b_1) = 1.$$

Тоді $a + b = 24\,a_1 + 24\,b_1 = 144$. Звідси

$$\begin{cases} a_1 + b_1 = 6, \\ (a_1, b_1) = 1. \end{cases}$$

З точністю до позначень доданків, можливий лише випадок

$$\begin{cases} a_1 = 1, \\ b_1 = 5. \end{cases}$$

Зверніть увагу, що випадки $\begin{cases} a_1 = 2, \\ b_1 = 4 \end{cases}$ та $\begin{cases} a_1 = 3, \\ b_1 = 3 \end{cases}$ неможливі в силу умови $(a_1, b_1) = 1$.

Тому $a = 24$, $b = 120$, або навпаки.

12 ЛАНЦЮГОВІ ДРОБИ

Вираз виду

$$q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\dots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n+\dots}}}},$$

де q_0, q_1, q_2, ... – деякі цілі числа, називають *елементарним ланцюговим дробом.*

Числа q_0, q_1, q_2, ... називають *елементами* даного ланцюгового дробу, а правильні дроби $\frac{1}{q_1}$, $\frac{1}{q_2}$, ... – *ланками* ланцюгового дробу. Число ланок у ланцюговому дробі може бути як скінченним, так і нескінченним.

Розглянемо скінченний, або n-членний ланцюговий дріб

$$q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\dots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}, \qquad (1)$$

для зручності позначатимемо його символом $[q_0;\ q_1,\ q_2,\ \dots,\ q_n]$. Крім того, вважатимемо, що q_1, q_2, ..., q_n – натуральні числа, $q_n \neq 1$, а q_0 може бути будь-яким цілим числом.

Якщо в n-членному ланцюговому дробі (1) виконати всі дії, то одержимо раціональне число. Справедливе й обернене твердження:

Теорема 12.1. *Кожне раціональне число можна подати у вигляді деякого скінченного ланцюгового дробу і таке представлення єдине.*

Дійсно, нехай задано раціональне число $\frac{a}{b}$, тоді можна виділити його цілу частину, тобто

$$\frac{a}{b} = q_0+\frac{r_0}{b} = q_0+\cfrac{1}{\cfrac{b}{r_0}} = q_0+\cfrac{1}{q_1+\cfrac{r_1}{r_0}} = q_0+\cfrac{1}{q_1+\cfrac{1}{\cfrac{r_0}{r_1}}} = \dots$$

і так далі. Таким чином, числа q_0, q_1, q_2, ..., q_n – це неповні частки, що утворилися після застосування до чисел a і b алгоритму Евкліда.

Теорема 12.2. *Будь-якому дійсному ірраціональному числу відповідає єдиний нескінченний ланцюговий дріб, що має це число своїм значенням.* Навпаки, *будь-який нескінченний ланцюговий дріб визначає одне і тільки одне дійсне ірраціональне число.*

Підхідні дроби ланцюгового дробу

Означення. *Підхідним дробом* порядку s n-членного ланцюгового дробу (1) називається раціональний дріб $\frac{P_s}{Q_s}$, що представляється відрізком $[q_0\,; q_1\,, q_2\,, \ldots, q_s]$ ланцюгового дробу (1).

n-членний ланцюговий дріб має $n+1$ підхідних дробів:

$$\frac{P_0}{Q_0} = \frac{q_0}{1}\,,$$

$$\frac{P_1}{Q_1} = [q_0; q_1] = q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1}\,,$$

$$\frac{P_2}{Q_2} = [q_0; q_1, q_2] = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = q_0 + \frac{q_2}{q_1 q_2 + 1} =$$

$$= \frac{q_0(q_1 q_2 + 1) + q_2}{q_2 q_1 + 1} = \frac{q_2(q_0 q_1 + 1) + q_0}{q_2 q_1 + 1} = \frac{q_2 \cdot P_1 + P_0}{q_2 \cdot Q_1 + Q_0}\quad ,\ldots$$

Теорема 12.3 (*Правило утворення підхідних дробів*). *При* $s \geq 2$

$$P_s = q_s \cdot P_{s\text{-}1} + P_{s\text{-}2}\,,$$
$$Q_s = q_s \cdot Q_{s\text{-}1} + Q_{s\text{-}2}\,.$$

Ці формули зручно записати у таблицю:

s		0	1	2		n
q_s		$\boldsymbol{q_0}$	$\boldsymbol{q_1}$	$\boldsymbol{q_2}$	**…**	$\boldsymbol{q_n}$
P_s	1	$q_0 =$ $= P_0$	$q_1 \cdot P_0 + 1 =$ $= P_1$	$q_2 \cdot P_1 + P_0 =$ $= P_2$	…	$q_n \cdot P_{n\text{-}1} + P_{n\text{-}2} =$ $= P_n$
Q_s	0	1	$q_1 \cdot Q_0 + 0 =$ $= Q_1$	$q_2 \cdot Q_1 + Q_0 =$ $= Q_2$	…	$q_n \cdot Q_{n\text{-}1} + Q_{n\text{-}2} =$ $= Q_n$

Для раціонального числа $\frac{a}{b} = \frac{P_n}{Q_n}$.

***Властивості підхідних дробів*:**

1. *Кожний підхідний дріб нескоротний.*

2. *Підхідні дроби парного порядку даного ланцюгового дробу утворюють зростаючу, а підхідні дроби непарного порядку – спадну послідовність.*

3. *Кожен підхідний дріб парного порядку даного ланцюгового дробу завжди менший від будь-якого підхідного дробу непарного порядку цього ланцюгового дробу.*

Якщо $\frac{P}{Q} = [q_0\,;\, q_1\,,\, q_2\,,\, \ldots,\, q_n]$, то з властивостей підхідних дробів маємо:

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots \le \frac{P}{Q} = \frac{P_n}{Q_n} \le \ldots < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}\,.$$

Таким чином, підхідні дроби парного порядку є наближеними значеннями дробу $\frac{P}{Q}$ з недостачею, а непарного порядку – з надлишком.

Оцінка похибки наближення:

$$\left|\frac{a}{b} - \frac{P_k}{Q_k}\right| \le \frac{1}{Q_k^2}\,.$$

Для нескінченного ланцюгового дробу

$$[q_0\,;\, q_1\,,\, q_2\,,\, \ldots,\, q_n\,,\, \ldots] \qquad (2)$$

аналогічно визначається поняття підхідного дробу.

Підхідним дробом k–го порядку до нескінченного ланцюгового дробу (2) називають скінченний ланцюговий дріб $\frac{P_k}{Q_k} = [q_0\,;\, q_1\,,\, q_2\,,\, \ldots,\, q_k]$.

Кожен підхідний дріб до нескінченного ланцюгового дробу можна розглядати також як підхідний дріб до скінченного ланцюгового дробу. Тому підхідні дроби для нескінченних ланцюгових дробів мають такі ж самі властивості, що й для скінченних.

Лінійне діофантове рівняння

Діофантовим рівнянням називають рівняння від n змінних з цілими коефіцієнтами, розв'язок якого знаходять у цілих числах.

Розглянемо лінійне діофантове рівняння з двома невідомими

$$ax + by = c\,.$$

Теорема 12.4. *Загальним розв'язком у цілих числах лінійного діофантового рівняння з двома невідомими* $ax + by = c$, де $(a,b) = 1$, *є*

$$x = (-1)^{n-1} cQ_{n-1} + bt,$$
$$y = (-1)^{n} cP_{n-1} - at, \quad t \in \mathbf{Z},$$

P_{n-1}, Q_{n-1} – чисельник і знаменник передостаннього підхідного дробу розкладу числа $\frac{a}{b}$ у ланцюговий дріб.

Приклад 12.1. *Розкласти в ланцюговий дріб раціональне число* $-\frac{166}{217}$.

Виділимо цілу частину заданого дробу:

$$-\frac{166}{217} = -1 + \frac{51}{217} = -1 + \cfrac{1}{\cfrac{217}{51}}.$$

Далі можна алгоритм послідовного ділення (алгоритм Евкліда) для чисел 217 та 51 записати в стовпчик:

$$\begin{array}{r|l} \_217 & 51 \\ \underline{204} & 4 = q_1 \\ 13 & \end{array} \qquad \begin{array}{r|l} \_51 & 13 \\ \underline{39} & 3 = q_2 \\ 12 & \end{array} \qquad \begin{array}{r|l} \_13 & 12 \\ \underline{12} & 1 = q_3 \\ 1 & \end{array} \qquad \begin{array}{r|l} \_12 & 1 \\ \underline{12} & 12 = q_4 \\ 0 & \end{array}$$

Таким чином, $-\frac{166}{217} = [-1; 4, 3, 1, 12]$.

Приклад 12.2. *Розкласти в ланцюговий дріб ірраціональне число* $\sqrt{11}$.

Виділимо цілу частину цього числа, а дробову частину позначимо $\frac{1}{\alpha_1}$:

$$\sqrt{11} = 3 + \frac{1}{\alpha_1}.$$

Визначимо з цієї рівності α_1:

$$\alpha_1 = \frac{1}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{2} = 3 + \frac{1}{\alpha_2}.$$

Тобто з числа α_1 знов виділили цілу частину, а його дробову частину позначили $\frac{1}{\alpha_2}$. Тоді, з останньої рівності,

$$\alpha_2 = \frac{1}{\frac{\sqrt{11}+3}{2}-3} = \frac{2}{\sqrt{11}-3} = \frac{2(\sqrt{11}+3)}{2} = \sqrt{11}+3 = 6+\frac{1}{\alpha_3},$$

$$\alpha_3 = \frac{1}{\sqrt{11}-3} = \alpha_1$$

і далі процес виділення цілої частини буде періодично повторюватись, тобто матимемо:

$$\sqrt{11} = [3;\ 3,\ 6,\ 3,\ 6,\ \ldots] = [3;\ (3,\ 6)].$$

Виявляється, що *коли число* α *є квадратичною ірраціональністю, тобто є дійсним коренем деякого квадратного рівняння з цілими коефіцієнтами, то воно розкладається в періодичний ланцюговий дріб.*

І навпаки, *кожен періодичний ланцюговий дріб є розкладом деякої дійсної квадратичної ірраціональності.*

Приклад 12.3. *Знайти квадратичну ірраціональність* α, *якщо відомо, що* α *розкладається в періодичний ланцюговий дріб* [2; 1, (3, 1)].

$$\alpha = \left[2; 1, (3, 1)\right] = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\ldots}}}}}.$$

Позначимо $y = \left[(3,1)\right] = 3+\cfrac{1}{1+\left.\cfrac{1}{3+\cfrac{1}{1+\ldots}}\right\}=y}.$

Тоді

$$y = 3+\cfrac{1}{1+\cfrac{1}{y}},$$

звідки маємо

$$y^2-3y-3=0,$$

$$y_1 = 3+\sqrt{21}, \qquad y_2 = 3-\sqrt{21}.$$

Оскільки y – додатне число, то $y = 3+\sqrt{21}$.

Тепер обчислимо α:

$$\alpha = \quad 2+\cfrac{1}{1+\cfrac{1}{y}} \quad = \quad 2+\cfrac{1}{1+\cfrac{1}{3+\sqrt{21}}} \quad = \quad 2+\frac{3+\sqrt{21}}{4+\sqrt{21}} \quad = \quad \frac{11+3\sqrt{21}}{4+\sqrt{21}} \quad =$$

$$= \quad \frac{(11+3\sqrt{21})\,(4-\sqrt{21})}{4+\sqrt{21}} \quad = \quad \frac{19-\sqrt{21}}{5}\,.$$

Приклад 12.4. В прикладі 12.1 раціональне число $-\frac{166}{217}$ розкладено в ланцюговий дріб $-\frac{166}{217}$ = [– 1; 4, 3, 1, 12]. *Знайдемо підхідні дроби для нього*:

s		0	1	2	3	4
q_s		**– 1**	**4**	**3**	**1**	**12**
P_s	**1**	– 1	– 3	– 10	– 13	– 166
Q_s	**0**	1	4	13	17	217

$$\frac{P_0}{Q_0}=-\frac{1}{1},\quad \frac{P_1}{Q_1}=-\frac{3}{4},\quad \frac{P_2}{Q_2}=-\frac{10}{13},\quad \frac{P_3}{Q_3}=-\frac{13}{17},\quad \frac{P_4}{Q_4}=-\frac{166}{217}.$$

Приклад 12.5. *Знайти цілі розв'язки рівняння* $22x+17y=25$.

НСД (22, 17) = 1, застосуємо теорему 12.4. Розкладемо в ланцюговий дріб число $\frac{22}{17}$. Дістанемо $\frac{22}{17}$ = [1; 3, 2, 2].

Знайдемо підхідні дроби для цього ланцюгового дробу:

s		0	1	2	3
q_s		**1**	**3**	**2**	**2**
P_s	**1**	1	4	9	22
Q_s	**0**	1	3	7	17

$n = 3$, $\frac{P_2}{Q_2}=\frac{9}{7}$.

Отже

$$x=(-1)^2\,cQ_2+bt==25\cdot 7+17t=5+17(t+10)=5+17t_1,$$

$$y=(-1)^3\,cP_2-at=-25\cdot 9-22t=-5-22(t+10)=-5-22t_1,$$

$t_1\in\mathbf{Z}$.

13 ПРОСТІ ЕЛЕМЕНТИ КІЛЬЦЯ

Нехай K – область цілісності (комутативне кільце з одиницею e без дільників нуля), a – довільний елемент кільця K.

Раніше зазначалось, що елементи e, a, ε (дільники одиниці), $a\varepsilon$ (асоційовані до a) називають *тривіальними дільниками* елемента a.

Означення. Елемент a області цілісності K називають *простим*, якщо він не є дільником одиниці і не має нетривіальних дільників.

Означення. Елемент a області цілісності K називають *складеним*, якщо він має нетривіальні дільники.

Таким чином, складений елемент a можна подати у вигляді добутку

$$a = b \cdot c$$

двох нетривіальних дільників b та c.

В кільці цілих гауссових чисел $\mathbf{Z}[i]$ дільниками одиниці є: $\pm 1, \pm i$, в цьому кільці справедливою є рівність

$$2 = (1 + i)(1 - i),$$

таким чином число 2 не є простим в кільці $\mathbf{Z}[i]$.

***Властивості простих елементів*:**

Нехай K – евклідове кільце.

1. *Якщо елемент $p \in K$ простий, то і будь-який асоційований до нього елемент $p\varepsilon$ (ε – дільник одиниці) також є простим.*

2. *Нехай p – простий елемент кільця K, a – довільний елемент цього кільця,тоді $a \,\vdots\, p$ або $(a, p) = e$.*

3. *Якщо добуток ab елементів кільця K ділиться на простий елемент p цього кільця, то принаймні один з співмножників ділиться на p.*

Прості числа, їх властивості

Нехай $K = \mathbf{Z}$.

Означення. Відмінне від одиниці натуральне число a називають *простим*, якщо воно не має інших дільників, крім 1 та a.

Означення. Натуральне число a називають *складеним*, якщо воно має нетривіальні дільники.

Зауважимо, що число 1 не відносять ні до простих, ні до складених.

***Властивості простих чисел*:**

1. *Якщо число p є простим, то число $-p$ також є простим.*

2. *Нехай p – просте число, a – довільне ціле число, тоді $a \,\vdots\, p$ або $(a, p) = 1$.*

3. *Якщо добуток* ab *цілих чисел ділиться на просте число* p*, то принаймні один з співмножників ділиться на* p.

4. *Найменший відмінний від одиниці натуральний дільник натурального числа* a $(a>1)$ *є простим числом.*

5. *Найменший відмінний від одиниці натуральний дільник складеного натурального числа* a *не перевищує* $\sqrt{a}$.

Теорема 13.1 (*Евкліда*). *Множина простих чисел нескінченна.*

Доведення. Припустимо, що множина простих чисел скінченна:

$$p_1, p_2, \dots p_m,$$

то число $P = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$ не співпадає з жодним із них і не ділиться на жодне з них. Оскільки $P > 1$, то воно або є простим, або ділиться на деяке інше просте число q.

Теорема 13.2 (*Основна теорема арифметики*). *Кожне відмінне від одиниці натуральне число можна представити у вигляді добутку простих чисел. Таке представлення єдине з точністю до порядку слідування множників*:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k}, \qquad (1)$$

де p_i – прості числа, $\alpha_i \in \mathbf{N}$.

Запис (1) називають *канонічним розкладом числа* a на прості множники.

Означення. Кільце називають *факторіальним*, якщо в ньому кожен ненульовий та неодиничний елемент розкладається в добуток простих елементів. І таке представлення єдине з точністю до асоційованих множників та порядку слідування множників

Теорема 13.3. *Кожне евклідове кільце є факторіальним.*

Числові функції

Означення. В теорії чисел функцію називають *числовою*, якщо вона визначена для всіх натуральних значень аргументу:

$$f(n), \quad n \in \mathbf{N}.$$

$\tau(n)$ – функція, яка вказує *кількість натуральних дільників числа* n,

$\sigma(n)$ – функція, яка визначає *суму всіх натуральних дільників числа* n,

функція Ейлера $\varphi(n)$ – функція, що визначає для натурального числа n кількість невід'ємних чисел, які менші за n і взаємно прості з n.

Якщо канонічний розклад натурального числа n має вигляд

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k},$$

то

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1),$$

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1},$$

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Приклад 13.1. *Чи є число* 379 *простим*?

Якби число 379 було б складеним, то його найменший відмінний від одиниці натуральний дільник був би простим числом, що не перевищує $\sqrt{379} \approx 19{,}2$.

Випишемо всі прості числа, які не перевищують 19:

2, 3, 5, 7, 11, 13, 17, 19.

Перевіримо, чи ділиться 379 на них.

Ні. Отже 379 є простим числом.

Приклад 13.2 ***Решето Ератосфена.*** *Побудувати таблицю простих чисел, менших за деяке натуральне число* A.

Для цього випишемо всі натуральні числа від 2 до A:

2, 3, 4, 5, 6, 7, 8, 9, 10, …, A.

Викреслимо з них ті, які діляться на 2, крім самого числа 2; потім ті, які діляться на 3, крім самого числа 3; …; викреслимо всі числа, які діляться на p, для якого $p \le \sqrt{A}$.

Числа, які залишились невикресленими, є простими.

Таким же чином можна знаходити прості числа на будь-якому числовому проміжку.

Приклад 13.3. *Знайти значення числових функцій для числа* 12.

$$n = 12 = 2^2 \cdot 3.$$

Кількість натуральних дільників числа 12:

$$\tau\,(12) = (2+1)\cdot(1+1) = 6,$$

дільниками числа 12 є 1, 2, 3, 4, 6, 12, їх дійсно 6.

Сума натуральних дільників числа 12:

$$\sigma(12) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} = 28.$$

Значення функції Ейлера для числа 12, тобто кількість невід'ємних цілих чисел, які менші за 12 і з 12 взаємно прості:

$$\varphi(12) = 2^2 \cdot 3 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2^2 \cdot 3 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4,$$

такими числами є 1, 5, 7, 11, їх дійсно чотири.

14 КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД ОДНІЄЇ ЗМІННОЇ

Нехай K – область цілісності (комутативне кільце з одиницею без дільників нуля).

Многочленом від однієї змінної над областю цілісності K називають вираз виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0, \qquad (1)$$

де $n \in \mathbf{N}$, $a_i \in K$ $(i = 0, 1, 2, \ldots, n)$, $a_n \neq 0$.

Елементи a_i називають *коефіцієнтами* многочлена.

Запис (1) називають *канонічною формою многочлена.*

Доданок $a_k x^k$ $(k = 0, 1, 2, \ldots, n)$ канонічного представлення многочлена $f(x)$ називають *k-м членом* (членом k-го степеня), елемент a_k називають *k-м коефіцієнтом*, a_0 *вільним членом* многочлена $f(x)$.

Член n-го (найбільшого) степеня називають *старшим членом* многочлена $f(x)$, його коефіцієнт a_n – *старшим коефіцієнтом*, його степінь n – *степенем многочлена* $f(x)$ і позначають

$$\deg f = n.$$

Многочлен нульового степеня має вигляд $f(x) = a_0$ $(a_0 \in K,\ a_0 \neq 0)$, такі многочлени називають *константами*. Отже довільний ненульовий елемент області цілісності K можна розглядати як многочлен нульового степеня.

Многочлен, всі коефіцієнти якого дорівнюють нулю, називають *нульовим многочленом*. Такому многочлену не приписують ніякого степеня.

Отже, якщо $\deg f = n$, то $a_n \neq 0$.

Означення. Многочлени

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_2 x^2 + b_1 x + b_0$$

називають *рівними*, якщо

1) $\deg f = \deg g$,

2) $a_i = b_i$ $(i = 0, 1, 2, \ldots, n)$.

Означення. *Сумою* многочленів

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_2 x^2 + b_1 x + b_0$$

$(n > m)$ називають многочлен

$$s(x) = f(x) + g(x) = a_n x^n + \ldots + a_{m+1}x^{m+1} +$$
$$+ (a_m + b_m)x^m + \ldots + (a_2 + b_2)x^2 + (a_1 + b_1)x + (a_0 + b_0).$$

Наприклад, знайдемо суму многочленів
$f(x)=5x^5+3x^4-11x^3+x^2-4x+7$ та $g(x)=2x^3+9x^2-x+8$,

$$f(x)+g(x)=5x^5+3x^4-9x^3+10x^2-5x+15.$$

Означення. *Добутком* многочленів

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_2x^2+a_1x+a_0,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+...+b_2x^2+b_1x+b_0$$

$(n>m)$ називають многочлен

$$t(x)=f(x)\cdot g(x)=a_n\cdot b_mx^{n+m}+...+$$

$$+(a_kb_0+a_{k-1}b_1+a_{k-2}b_2+...a_1b_{k-1}+a_0b_k)x^k+...+$$

$$+(a_2b_0+a_1b_1+a_0b_2)x^2+(a_1b_0+a_0b_1)x+a_0\cdot b_0,$$

тобто многочлен, коефіцієнти якого обчислюють за правилом

$$c_k=a_kb_0+a_{k-1}b_1+a_{k-2}b_2+...a_1b_{k-1}+a_0b_k=\sum_{j=0}^{k}a_{k-j}b_j=\sum_{i+j=k}a_ib_j.$$

Наприклад, знайдемо добуток многочленів
$f(x)=5x^5+3x^4-11x^3+x^2-4x+7$ та
$g(x)=2x^3+9x^2-x+8$,

$$f(x)\cdot g(x)=5\cdot 2x^8+(5\cdot 9+3\cdot 2)x^7+(5\cdot(-1)+3\cdot 9+(-11)\cdot 2)x^6+$$

$$+(5\cdot 8+3\cdot(-1)+(-11)\cdot 9+1\cdot 2)x^5+(3\cdot 8+(-11)\cdot(-1)+1\cdot 9+(-4)\cdot 2)x^4+$$

$$+((-11)\cdot 8+1\cdot(-1)+(-4)\cdot 9+7\cdot 2)x^3+(1\cdot 8+(-4)\cdot(-1)+7\cdot 9)x^2+$$

$$+((-4)\cdot 8+7\cdot(-1))x+7\cdot 8=$$

$$=10x^8+51x^7-60x^5+36x^4-111x^3+75x^2-39x+56.$$

Теорема 14.1. $\deg(f+g)\le\max\{\deg f,\ \deg g\}$.

Теорема 14.2. $\deg(f\cdot g)=\deg f+\deg g$.

Теорема 14.3. *Сукупність* $K[x]$ *всіх многочленів від однієї змінної над областю цілісності* K *утворює комутативне кільце (але не поле).*

Теорема 14.4. *Якщо* K – *область цілісності, то і кільце многочленів* $K[x]$ *також є областю цілісності.*

Відношення подільності в кільці многочленів

Многочлен $f(x)\in K[x]$ *ділиться* на многочлен $\varphi(x)\in K[x]$, якщо існує такий многочлен $g(x)\in K[x]$, що

$$f(x)=\varphi(x)\cdot g(x).$$

Записують $f(x)\,\vdots\,\varphi(x)$.

Многочлен $\varphi(x)$ при цьому називають *дільником* многочлена $f(x)$.

В кільці многочленів $K[x]$ виконуються всі властивості подільності комутативного кільця (див. розділ **9**).

Оскільки $K \subset K[x]$, то $e = 1$ є одиницею в кільці многочленів $K[x]$.

Многочлени $\varepsilon_1(x),\ \varepsilon_2(x) \in K[x]$ називають *дільниками одиниці*, якщо

$$\varepsilon_1(x) \cdot \varepsilon_2(x) = 1.$$

Тоді $\deg(\varepsilon_1 \cdot \varepsilon_2) = \deg \varepsilon_1 + \deg \varepsilon_2 = 0$, звідси $\deg \varepsilon_1 = 0$ та $\deg \varepsilon_2 = 0$. Таким чином, *дільниками одиниці в кільці* $K[x]$ *є лише многочлени нульового степеня, тобто елементи області цілісності* K. Якщо $K = P$ – поле, то всі ненульові елементи поля P є дільниками одиниці в кільці $P[x]$.

Якщо $f(x) \vdots \varphi(x)$ і $\varphi(x) \vdots f(x)$, то многочлени $f(x)$ та $\varphi(x)$ називають *асоційованими*. Позначають $f(x) \sim \varphi(x)$.

В кільці $K[x]$ асоційованими є многочлени, що відрізняються один від одного на сталий множник $c \in K$:

$$f(x) \sim c \cdot f(x).$$

Якщо P – поле, то до властивостей подільності слід додати ще такі:

6. $\forall f(x) \in P[x],\ \forall c \in P\ (c \neq \theta) \quad f(x) \vdots c$.

7. $\forall f(x), \varphi(x) \in P[x],\ \forall c \in P\ (c \neq \theta)$

$$f(x) \vdots \varphi(x) \quad \Rightarrow \quad f(x) \vdots c \cdot \varphi(x).$$

Теорема 14.5 (*про ділення з остачею в кільці многочленів*). *Нехай* P – *поле. Для будь-яких многочленів* $f(x),\ \varphi(x) \in P[x]$ $(\varphi(x) \neq \theta)$ *існують такі многочлени* $q(x),\ r(x) \in P[x]$, *що*

$$f(x) = \varphi(x) \cdot q(x) + r(x)$$

і якщо $r(x) \neq \theta$, *то* $\deg r < \deg \varphi$.

Пара многочленів $q(x),\ r(x)$ *визначається однозначно.*

Многочлен $q(x)$ називають *неповною часткою*, $r(x)$ називають *остачею* при діленні многочлена $f(x)$ *на* $\varphi(x)$

Доведення. Нехай

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

$$\varphi(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_2 x^2 + b_1 x + b_0,$$

оскільки $\varphi(x) \neq \theta$, то $b_m \neq \theta$.

1) Якщо $f(x) = 0$, то $0 = \varphi(x) \cdot 0 + 0$, тобто $q(x) = 0,\ r(x) = 0$.

2) Якщо $n < m$, то $f(x) = \varphi(x) \cdot \underbrace{0}_{q(x)} + \underbrace{f(x)}_{r(x)}$.

3) Нехай $n \geq m$. Поділимо старший член многочлена $f(x)$ на старший член многочлена $\varphi(x)$, це можливо оскільки $b_m \neq \theta$, $\frac{a_n}{b_m} \in P$, матимемо допоміжний многочлен $\frac{a_n}{b_m} x^{n-m}$.

Помножимо цей допоміжний многочлен на $\varphi(x)$, тоді многочлен $\frac{a_n}{b_m} x^{n-m} \cdot \varphi(x)$ матиме старшим членом вираз $a_n x^n$, такий же як і многочлен $f(x)$. Після віднімання

$$f(x) - \frac{a_n}{b_m} x^{n-m} \cdot \varphi(x) = f_1(x)$$

отримаємо многочлен $f_1(x) \in P[x]$, $\deg f_1 = n_1 < n$ або $f_1(x) = 0$.

Нехай $f_1(x) \neq 0$, позначимо його старший коефіцієнт a_{n_1}:

$$f_1(x) = a_{n_1} x^{n_1} + a_{n_1 - 1} x^{n_1 - 1} + \ldots$$

Якщо $n_1 < m$, то процес припиняємо. Якщо $n_1 \geq m$, то аналогічно побудуємо допоміжний многочлен $\frac{a_{n_1}}{b_m} x^{n_1 - m}$, помножимо його на $\varphi(x)$ та після віднімання

$$f_1(x) - \frac{a_{n_1}}{b_m} x^{n_1 - m} \cdot \varphi(x) = f_2(x)$$

отримаємо многочлен $f_2(x) \in P[x]$, $\deg f_2 = n_2 < n_1$ або $f_2(x) = 0$ і т.д.

Оскільки степені многочленів $f(x)$, $f_1(x)$, $f_2(x)$, … утворюють спадну послідовність

$$n > n_1 > n_2 > \ldots,$$

то після скінченного числа кроків дістанемо многочлен $f_k(x)$:

$$f_{k-1}(x) - \frac{a_{n_{k-1}}}{b_m} x^{n_{k-1} - m} \cdot \varphi(x) = f_k(x),$$

який або дорівнює нулю, або має степінь $n_k < m$.

Тобто

$$f(x) - \frac{a_n}{b_m} x^{n-m} \cdot \varphi(x) = f_1(x),$$

$$f_1(x) - \frac{a_{n_1}}{b_m} x^{n_1 - m} \cdot \varphi(x) = f_2(x),$$

$$. \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad .$$

$$f_{k-1}(x) - \frac{a_{n_{k-1}}}{b_m} x^{n_{k-1}-m} \cdot \varphi(x) = f_k(x).$$

Додамо ці рівності, дістанемо

$$f(x) - \underbrace{\left(\frac{a_n}{b_m} x^{n-m} + \frac{a_{n_1}}{b_m} x^{n_1-m} + \ldots + \frac{a_{n_{k-1}}}{b_m} x^{n_{k-1}-m} \right)}_{q(x)} \cdot \varphi(x) = \underbrace{f_k(x)}_{r(x)},$$

тобто

$$f(x) = \varphi(x) \cdot q(x) + r(x)$$

при цьому $r(x) = \theta$ або $\deg r < \deg \varphi$.

Викладений метод відшукання многочленів $q(x)$, $r(x)$ для заданих $f(x)$ та $\varphi(x)$ називають *алгоритмом ділення з остачею*.

Наслідок. М*ногочлен* $f(x)$ *тоді й тільки тоді ділиться на многочлен* $\varphi(x)$*, коли остача від ділення* $f(x)$ *на* $\varphi(x)$ *дорівнює нулю*.

Теорема 14.6. *Кільце* многочленів $P[x]$ над полем P *є евклідовим кільцем*.

Виконаємо ділення з остачею многочлена $f(x) = 2x^5 + 4x^4 - 3x^3 + 5x^2 + x - 7$ на многочлен $\varphi(x) = 2x^2 - x + 3$.

$$\begin{array}{rl|l}
- & 2x^5 + 4x^4 - 3x^3 + 5x^2 + x - 7 & 2x^2 - x + 3 \\ \cline{3-3}
 & 2x^5 - x^4 + 3x^3 & \frac{2}{2}x^3 + \frac{5}{2}x^2 - \frac{7}{4}x - \frac{17}{8} \\ \cline{1-2}
- & 5x^4 - 6x^3 + 5x^2 + x - 7 & \\
 & 5x^4 - \frac{5}{2}x^3 + \frac{15}{2}x^2 & \\ \cline{1-2}
- & -\frac{7}{2}x^3 - \frac{5}{2}x^2 + x - 7 & \\
 & -\frac{7}{2}x^3 + \frac{7}{4}x^2 - \frac{21}{4}x & \\ \cline{1-2}
- & -\frac{17}{4}x^2 + \frac{25}{4}x - 7 & \\
 & -\frac{17}{4}x^2 + \frac{17}{8}x - \frac{51}{8} & \\ \cline{1-2}
 & \frac{33}{8}x - \frac{5}{8} &
\end{array}$$

Таким чином,

$$f(x) = \varphi(x) \cdot \underbrace{\left(x^3 + \frac{5}{2}x^2 - \frac{7}{4}x - \frac{17}{8} \right)}_{q(x)} + \underbrace{\frac{33}{8}x - \frac{5}{8}}_{r(x)}.$$

Теорема 14.7 (*Безу*). *Остача від ділення многочлена* $f(x)$ *на лінійний двочлен* $\varphi(x) = x - c$ *дорівнює значенню цього многочлена в точці* $x_0 = c$, *тобто*

$$f(c) = r.$$

Коренем многочлена $f(x) \in P[x]$ називають елемент $d \in T$ деякого розширення T поля P $(P \subset T)$, для якого $f(d) = 0$.

Теорема 14.8 (*Ознака кореня многочлена*). *Елемент* $d \in P$ *є коренем многочлена* $f(x) \in P[x]$ *тоді і тільки тоді, коли многочлен* $f(x)$ *ділиться на лінійний двочлен* $x - d$ *без остачі.*

Елемент $d \in P$ називають *k-кратним коренем многочлена* $f(x) \in P[x]$ якщо многочлен $f(x)$ ділиться на $(x-d)^k$ і не ділиться на $(x-d)^{k+1}$.

Тобто, якщо елемент d є k-кратним коренем многочлена $f(x)$, то

$$f(x) = (x-d)^k \cdot g(x), \quad \text{причому} \quad g(d) \neq 0.$$

Приклад 14.1. *Довести, що многочлен* $f(x) = (x+a)^n - x^n - a^n$ *ділиться на* $g(x) = x + a$ *при непарному* n *в кільці* $Z[x]$.

За теоремою Безу,

$$f(x) \vdots (x+a) \quad \Leftrightarrow \quad f(-a) = 0.$$

Тому потрібно обчислити значення $f(-a)$.

Приклад 14.2. *Довести, що многочлен* $f(x) = x^{1984} + x + 1$ *не ділиться на* $g(x) = x^2 - 1$ *в кільці* $Z[x]$.

Розкладемо многочлен $g(x)$ на лінійні множники

$$g(x) = (x-1)(x+1).$$

$$f(x) \vdots g(x) \quad \Leftrightarrow \quad \begin{cases} f(x) \vdots (x-1) & \Leftrightarrow \quad f(1) = 0 \\ f(x) \vdots (x+1) & \Leftrightarrow \quad f(-1) = 0 \end{cases}$$

Знаходимо $f(1) = 3 \neq 0$, отже многочлен $f(x)$ не ділиться на $(x-1)$, а отже не ділиться і на $(x-1)(x+1)$.

Зробимо висновок*: для того, щоб многочлен* $f(x)$ *ділився на* $g(x)$ *необхідно й достатньо, щоб всі корені многочлена* $g(x)$ *були коренями многочлена* $f(x)$.

Приклад 14.3. *Остача від ділення многочлена* $f(x)$ *на* $g_1(x) = x - 2$ *дорівнює* 1, *остача від ділення* $f(x)$ *на* $g_2(x) = x - 1$ *дорівнює* 2. *Знайти остачу від ділення* $f(x)$ *на* $g(x) = (x - 1)(x - 2)$.

За теоремою про ділення з остачею многочлена $f(x)$ на $g(x)$:

$$f(x) = (x - 1)(x - 2)\cdot q(x) + r(x),$$

де $\deg r < \deg g = 2$.

Отже $\deg r = 1$,тобто $r(x) = ax + b$. Звідси

$$f(x) = (x - 1)(x - 2)\cdot q(x) + ax + b.$$

Залишається знайти значення коефіцієнтів a, b.

За умовою, остача від ділення многочлена $f(x)$ на $g_1(x) = x - 2$ дорівнює 1, отже за теоремою Безу, значення $f(2) = 1$. А оскільки остача від ділення $f(x)$ на $g_2(x) = x - 1$ дорівнює 2, то $f(1) = 2$,тобто маємо систему рівностей

$$f(2) = 2a + b = 1,$$
$$f(1) = a + b = 2.$$

Звідси $a = -1$, $b = 3$, $r(x) = -x + 3$.

15 СХЕМА ГОРНЕРА. ПОХІДНА МНОГОЧЛЕНА

Ділення многочлена

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

на лінійний двочлен $\varphi(x) = x - c$ зручно виконувати за схемою Горнера:

	a_n	a_{n-1}	a_{n-2}	…	a_2	a_1	a_0
c	$a_n = b_{n-1}$	$c \cdot b_{n-1} + a_{n-1} = b_{n-2}$	$c \cdot b_{n-2} + a_{n-2} = b_{n-3}$	…	$c \cdot b_2 + a_2 = b_1$	$c \cdot b_1 + a_1 = b_0$	$c \cdot b_0 + a_0 = r$

Звідси

$$f(x) = (x-c) \cdot g(x) + r,$$

де $g(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_2 x^2 + b_1 x + b_0$.

В алгебрі поняття границі застосовне не в усякому полі, тому дамо таке визначення похідної многочлена. *Похідною* многочлена

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

з коефіцієнтами із поля P степеня n називають многочлен

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1 .$$

Вважають, що похідна від многочлена нульового степеня, а також від нуль-многочлена дорівнює нулю.

Таким чином, коефіцієнти похідної $f'(x)$ многочлена $f(x)$ належать тому самому полю, що і коефіцієнти самого многочлена і

$$\deg f' = n - 1 = \deg f - 1.$$

В алгебрі розглядають також похідні

$$f''(x),\ f'''(x),\ \ldots,\ f^{(k)}(x)$$

2-го, 3-го, …, k-го порядку.

Для многочленів залишаються справедливими правила диференціювання, відомі з курсу математичного аналізу.

Розклад многочлена $f(x)$ за степенями лінійного двочлена $(x-c)$

Поділимо многочлен $f(x)$ степеня n на лінійний двочлен $x - c$ з остачею:

$$f(x) = (x-c) \cdot g_1(x) + r_0,$$

$\deg g_1 = n - 1$. Нехай $n - 1 \neq 0$, тоді поділимо $g_1(x)$ на $(x - c)$ з остачею:

$$g_1(x) = (x-c) \cdot g_2(x) + r_1,$$

$\deg g_2 = n-2$. Нехай $n-2 \neq 0$, поділимо $g_2(x)$ на $(x-c)$ з остачею:

$$g_2(x) = (x-c)\cdot g_3(x) + r_2,$$

$$\cdots\cdots\cdots$$

$$g_{n-1}(x) = (x-c)\cdot g_n(x) + r_{n-1},$$

$\deg g_n = n-n = 0$, тому позначимо $g_n(x) = r_n$.

Отже

$$f(x) = (x-c)\cdot g_1(x) + r_0,$$
$$g_1(x) = (x-c)\cdot g_2(x) + r_1,$$
$$g_2(x) = (x-c)\cdot g_3(x) + r_2,$$
$$\cdots\cdots\cdots$$
$$g_{n-1}(x) = (x-c)\cdot r_n + r_{n-1}.$$

Помножимо першу з цих рівностей на 1, другу – на $(x-c)$, третю на $(x-c)^2$, …, останню – на $(x-c)^{n-1}$ і додамо їх. Позбувшись однакових доданків в правій і лівій частинах, дістанемо

$$f(x) = r_n(x-c)^n + r_{n-1}(x-c)^{n-1} + \ldots + r_2(x-c)^2 + r_1(x-c) + r_0 \ –$$

розклад многочлена $f(x)$ *за степенями лінійного двочлена* $(x-c)$.

Обчислення значення многочлена $f(x)$ та його похідних k-го порядку при $x_0 = c$

Нехай многочлен $f(x)$ за схемою Горнера розкладено за степенями лінійного двочлена $(x-c)$:

$$f(x) = r_n(x-c)^n + r_{n-1}(x-c)^{n-1} + \ldots + r_3(x-c)^3 + r_2(x-c)^2 + r_1(x-c) + r_0,$$

звідси при $x = c$ матимемо, що

$$f(c) = r_0.$$

Знайдемо першу похідну для многочлена $f(x)$:

$$f'(x) = n\cdot r_n(x-c)^{n-1} + (n-1)\cdot r_{n-1}(x-c)^{n-2} + \ldots + 3r_3(x-c)^2 + 2r_2(x-c) + r_1,$$

звідси при $x = c$ матимемо, що

$$f'(c) = r_1.$$

Знайдемо другу похідну для многочлена $f(x)$:

$$f''(x) = (n-1)n\cdot r_n(x-c)^{n-2} + \ldots + 2\cdot 3r_3(x-c) + 2r_2,$$

тоді при $x = c$ матимемо, що

$$f''(c) = 2!\cdot r_2.$$

Продовжуючи обчислювати похідні, дістанемо *формулу для обчислення значень похідних* k*-го порядку многочлена* $f(x)$ *при* $x_0 = c$:

$$\boxed{f^{(k)}(c) = k!\cdot r_k}$$

Приклад 15.1. *Знайти неповну частку та остачу при діленні многочлена*

$$f(x) = 2x^5 + 7x^4 - 5x^2 + 10x - 12$$

на $\varphi(x) = x + 3$.

Обчислимо коефіцієнти b_i неповної частки $g(x)$ та остачу r за схемою Горнера, тут $c = -3$:

	2	**7**	**0**	**– 5**	**10**	**– 12**
– 3	2	1	– 3	4	– 2	– 6 = *r*

Отже,

$$f(x) = (x+3)\cdot\left(2x^4 + 1x^3 - 3x^2 + 4x - 2\right) - 6.$$

Приклад 15.2. *Знайти значення многочлена*

$$f(x) = 2x^5 + 7x^4 - 5x^2 + 10x - 12$$

при $c = -3$.

Згідно з теоремою Безу, *остача від ділення многочлена* $f(x)$ *на лінійний двочлен* $\varphi(x) = x - c$ *дорівнює значенню цього многочлена в точці* $x_0 = c$, *тобто* $f(c) = r$.

Виконаємо ділення многочлена $f(x)$ на лінійний двочлен $\varphi(x) = x - c$ за схемою Горнера:

	2	**7**	**0**	**– 5**	**10**	**– 12**
– 3	2	1	– 3	4	– 2	– 6 = *r*

Отже,

$$f(-3) = -6.$$

Приклад 15.3. *Чи є число* $x_0 = 3$ *коренем многочлена*

$$f(x) = x^4 - 6x^3 + 10x^2 - 6x + 9?$$

Згідно з теоремою (ознака кореня многочлена), *елемент* $d \in P$ *є коренем многочлена* $f(x) \in P[x]$ *тоді і тільки тоді, коли многочлен* $f(x)$ *ділиться на лінійний двочлен* $x - d$ *без остачі.*

Виконаємо ділення многочлена $f(x)$ на $x - 3$ за схемою Горнера:

	1	**– 6**	**10**	**– 6**	**9**
3	1	– 3	1	– 3	0

Бачимо, що $f(3) = 0$, отже число $x_0 = 3$ є коренем многочлена $f(x)$.

Приклад 15.4. *Встановити кратність кореня* $x_0 = 3$ *многочлена*

$$f(x) = x^4 - 6x^3 + 10x^2 - 6x + 9.$$

Згідно з означенням, елемент $d \in P$ називають *k-кратним коренем многочлена* $f(x) \in P[x]$ якщо многочлен $f(x)$ ділиться на $(x-d)^k$ і не ділиться на $(x-d)^{k+1}$.

Виконаємо ділення многочлена $f(x)$ на $x-3$ за схемою Горнера:

	1	**– 6**	**10**	**– 6**	**9**	
3	1	– 3	1	– 3	0	$\Rightarrow f(x) \vdots (x-3)$
3	1	0	1	0		$\Rightarrow f(x) \vdots (x-3)^2$
3	1	3	$10 \neq 0$			$\Rightarrow f(x) \not\vdots (x-3)^3$

Отже, число $x_0 = 3$ є 2-кратним коренем многочлена $f(x)$ і

$$f(x) = (x-3)^2 \cdot (x^2 + 0x + 1).$$

Приклад 15.5. *Розкласти многочлен*

$$f(x) = 3x^5 - 7x^4 - x^3 + 5x^2 - 4x - 9$$

за степенями $(x-2)$ *та обчислити* $f'''(2)$.

Виконаємо послідовне ділення многочлена $f(x)$ на $x-2$ за схемою Горнера:

	3	**– 7**	**– 1**	**5**	**– 4**	**– 9**	
2	3	– 1	– 3	–1	– 6	– 21	$= r_0$
2	3	5	7	13	20	$= r_1$	
2	3	11	29	71	$= r_2$		
2	3	17	63	$= r_3$			
2	$3 = r_5$	23	$= r_4$				

Розклад многочлена $f(x)$ за степенями $(x-c)$:

$$f(x) = 3(x-2)^5 + 23(x-2)^4 + 63(x-2)^3 + 71(x-2)^2 + 20(x-2) - 21.$$

Для обчислення значення похідної k-порядку многочлена $f(x)$ в точці $x_0 = c$ використаємо формулу:

$$f^{(k)}(c) = k! \cdot r_k.$$

Для даної задачі $f'''(2) = 3! \cdot r_3 = 1 \cdot 2 \cdot 3 \cdot 63 = 378$.

16 НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК В КІЛЬЦІ МНОГОЧЛЕНІВ

Оскільки кільце $P[x]$ многочленів від однієї змінної над полем P є евклідовим кільцем, то для будь-яких двох многочленів цього кільця (з яких хоча б один відмінний від 0) існує НСД.

Сформулюйте означення НСД двох многочленів з кільця $P[x]$.

НСД двох елементів області цілісності K визначається неоднозначно, з точністю до асоційованих множників.

Кільце $P[x]$ є областю цілісності, асоційовані многочлени цього кільця відрізняються на сталий множник $c \in P$. Тому, в кільці $P[x]$ домовляються в ролі НСД $(f(x),\ \varphi(x))$ брати многочлен із старшим коефіцієнтом 1 (такий многочлен називають *нормованим*).

Наприклад, для многочленів $f(x) = (2x-4)^2 \cdot (x+5)$ та $\varphi(x) = (6x-12)\cdot(x^2+1)$

$$\text{НСД}\big(f(x), \varphi(x)\big) = x-2,$$

оскільки $f(x) = (2x-4)^2 \cdot (x+5) = 4\,(x-2)^2(x+5)$,

$\varphi(x) = (6x-12)\cdot(x^2+1) = 6\,(x-2)\cdot(x^2+1)$.

Оскільки кільце $P[x]$ (P– поле) є евклідовим кільцем, то в ньому справджується:

Теорема 16.1. *НСД двох ненульових многочленів* $f(x),\ \varphi(x)$ *з кільця* $P[x]$ *є остання, відмінна від нуля, остача при застосуванні до многочленів* $f(x),\ \varphi(x)$ *алгоритму Евкліда.*

Теорема 16.2 (*про лінійне представлення НСД многочленів*). *Нехай* P *– поле, для будь-яких двох многочленів* $f(x),\ \varphi(x) \in P[x]$ $(\varphi(x) \neq \theta)$ *ненульового степеня існують такі многочлени* $U(x),\ V(x) \in P\,[x]$, *що має місце співвідношення*:

$$f(x)\cdot U(x) + \varphi(x)\cdot V(x) = D(x),$$

де $D(x) = \text{НСД}(f, \varphi)$ *і многочлени* $U(x),\ V(x)$ *можна підібрати так, щоб*

$$\deg U < \deg \varphi,$$
$$\deg V < \deg f\,.$$

Означення. Многочлени $f(x),\ \varphi(x) \in P[x]$ (P – поле) називають *взаємно простими*, якщо $\text{НСД}(f, \varphi) = 1$, тобто є многочленом нульового степеня.

Пропонуємо самостійно сформулювати **теорему** (ознака взаємної простоти двох многочленів), **властивості** взаємно простих многочленів, **означення** НСК двох многочленів, та **теорему** про знаходження НСК двох многочленів.

17 ПРОСТІ ЕЛЕМЕНТИ КІЛЬЦЯ МНОГОЧЛЕНІВ

Прості елементи кільця многочленів $P[x]$, де P – поле, називають *незвідними многочленами*.

Означення. Многочлен $f(x) \in P[x]$ називають *звідним* над полем P, якщо його можна представити у вигляді добутку

$$f(x) = \varphi(x) \cdot g(x),$$

двох многочленів $\varphi(x), g(x) \in P[x]$ меншого степеня, тобто

$$\deg \varphi < \deg f, \quad \deg g < \deg f.$$

Якщо такого представлення не існує, то многочлен вважають незвідним над полем P. Зауважимо, що нуль-многочлен та многочлени нульового степеня не відносять ні до звідних, ні до незвідних.

Означення. Многочлен $p(x) \in P[x]$ ненульового степеня називають *незвідним* над полем P, якщо в будь-якому його представленні у вигляді

$$p(x) = \varphi(x) \cdot g(x),$$

$\varphi(x), g(x) \in P[x]$, один із множників є многочленом нульового степеня.

Наприклад, многочлен $f_1(x) = x^2 - 5x + 6 = (x-2) \cdot (x-3)$ є звідним над полем **Q**.
Многочлен $f_2(x) = x^2 - 2$ є незвідним над полем **Q**, але звідним над полем **R**.

Властивості подільності для многочленів:

Оскільки кільце многочленів $P[x]$ є евклідовим кільцем, то в ньому справджуються загальні властивості простих елементів.

Сформулюйте їх самостійно.

1.

2.

3.

4. *Якщо незвідний над полем P многочлен $p(x)$ ділиться на інший незвідний над цим полем многочлен $g(x)$, то ці многочлени збігаються з точністю до сталого множника.*

5. *Многочлен першого степеня незвідний над будь-яким полем.*

Теорема 17.1. К*ожен многочлен $f(x) \in P[x]$ ненульового степеня можна подати у вигляді добутку незвідних над полем P многочленів. Таке представлення єдине з точністю до асоційованих множників і порядку слідування множників.*

Нехай

$$f(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x) -$$

деякий довільно вибраний розклад многочлена $f(x)$ в добуток незвідних над P множників. Якщо з кожного многочлена $q_i(x)$ $(i = 1,\ 2,\ \ldots,\ s)$ винести за дужки його старший коефіцієнт, то дістанемо розклад

$$f(x) = a \cdot p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_s(x),$$

в якому всі множники $p_i(x)$ – нормовані незвідні над P многочлени, об'єднуючи однакові співмножники операцією піднесення до натурального степеня, дістанемо

$$f(x) = p_1^{\,l_1}(x) \cdot p_2^{\,l_2}(x) \cdot \ldots \cdot p_n^{\,l_n}(x). \qquad (1)$$

Вираз (1) називають *канонічним розкладом* многочлена $f(x)$ з кільця $P[x]$ *на незвідні над* P *(нормовані) множники.*

Такий розклад для многочлена $f(x)$ визначається однозначно.

Незвідний многочлен $p(x)$ називається k*-кратним множником* многочлена $f(x)$, якщо

$$f(x) \vdots p^k(x) \quad \text{і} \quad f(x) \not\vdots\, p^{k+1}(x),$$

тобто в розкладі (1) множник $p(x)$ зустрічається k разів.

Якщо $k = 1$, то $p(x)$ називають *простим* (однократним) множником для $f(x)$.

Теорема 17.2. *Для того, щоб многочлен* $f(x)$ *не мав кратних множників необхідно й достатньо, щоб він був взаємно простий із своєю похідною* $f'(x)$.

Теорема 17.3 (*Ознака кратного кореня многочлена*). *Для того, щоб елемент* $c \in P$ *був коренем кратності* k *многочлена* $f(x) \in P[x]$ *необхідно й достатньо, щоб*

$$f(c) = f'(c) = f''(c) = \ldots = f^{(k-1)}(c) = 0, \text{ а } \quad f^{(k)}(c) \neq 0.$$

18 КОРЕНІ МНОГОЧЛЕНА. ФОРМУЛИ ВІЄТА ДЛЯ АЛГЕБРАЇЧНОГО РІВНЯННЯ *n*-ГО СТЕПЕНЯ.

Означення. Елемент d поля P називають *коренем многочлена* $f(x) \in P[x]$, якщо $f(d)=0$.

Теорема (*Ознака кореня многочлена*). *Елемент $d \in P$ є коренем многочлена $f(x) \in P[x]$ тоді і тільки тоді, коли многочлен $f(x)$ ділиться на лінійний двочлен $x-d$.*

Означення. Елемент $d \in P$ називають *k-кратним коренем многочлена* $f(x) \in P[x]$ якщо многочлен $f(x)$ ділиться на $(x-d)^k$ і не ділиться на $(x-d)^{k+1}$.

Корені кратності 1 називають *простими*, двократні та трикратні корені іноді називають *подвійними* та *потрійними* відповідно.

Якщо $f(x)$ – нуль-многочлен, то довільний елемент d поля P є його коренем, причому кратність цього кореня неможливо визначити, оскільки $0 \,\vdots\, (x-d)^m \quad \forall\, m \in \mathbf{N}$.

Якщо $f(x) \neq 0$, $d \in P$ – його корінь, то кратність цього кореня

$$k \leq \deg f\,.$$

Домовимось далі, підраховуючи кількість коренів многочлена $f(x)$ в полі P, кожен k-кратний корінь $d \in P$ лічити k разів, тобто вважати, що $f(x)$ має в полі P k коренів, які дорівнюють d.

Теорема 18.1 (*Про найбільшу можливу кількість коренів многочлена*). *Многочлен $f(x) \in P[x]$ степеня $n \geq 1$ може мати в полі P не більше, ніж n коренів.*

Наслідок. *Якщо многочлен $f(x) \in P[x]$ степеня n має в полі P $n+1$ різних коренів, то $f(x)$ є нуль-многочленом.*

Залишається питання, а чи існує поле, в якому існує хоча б один з коренів будь-якого многочлена ненульового степеня.

Наприклад, многочлен $f(x)=x^2-3$ над полем $\mathbf{Q}$ не має раціональних коренів; многочлен $g(x)=x^2+1$ над полем $\mathbf{R}$ не має дійсних коренів.

Але кожен з цих многочленів має корені у деякому розширенні розглядуваного поля: $f(x)$ має корені в $\mathbf{R}$, $g(x)$ має корені в $\mathbf{C}$.

Означення. *Коренем многочлена* $f(x) \in P[x]$ називають елемент d будь-якого розширення T поля P такий, що $f(d)=0$.

Теорема 18.2 (*Кронекера*). *Якщо* $f(x)$ *– довільний многочлен над полем* P *степеня* $n \geq 1$*, то існує поле* T*, що містить* P*, тобто розширення поля* P*, в якому многочлен* $f(x)$ *має хоча б один корінь*

Наслідок 1. *Для будь-якого многочлена* $f(x) \in P[x]$ *степеня* $n \geq 1$ *існує таке розширення* L *поля* P*, в якому многочлен* $f(x)$ *розкладається на лінійні множники.*

Означення. Поле L, в якому многочлен $f(x)$ розкладається на лінійні множники, називають *полем розкладу* цього многочлена.

Отже, для будь-якого многочлена $f(x) \in P[x]$ ненульового степеня існує поле розкладу L, яке є розширенням поля P.

Звичайно, може бути, що $L = P$.

Наприклад, многочлен $f(x) = x^4 - 2$ є незвідним над полем **Q**.

Над полем $\mathbf{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\right\}$:

$$f(x) = \left(x^2 - \sqrt{2}\right)\left(x^2 + \sqrt{2}\right).$$

Над полем **R**:

$$f(x) = \left(x - \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x^2 + \sqrt{2}\right).$$

Над полем **C**:

$$f(x) = \left(x - \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x - \sqrt[4]{2}\, i\right)\left(x + \sqrt[2]{2}\, i\right).$$

Наслідок 2. *Многочлен* $f(x) \in P[x]$ *n-го степеня має у полі розкладу* n *коренів.*

Оскільки многочлен $f(x) \in P[x]$ n-го степеня в жодному розширенні поля P не може мати більше, ніж n, коренів, то можна сказати, що *поле розкладу многочлена містить усі його корені*.

Означення. Поле P називають *алгебраїчно замкненим*, якщо воно є полем розкладу для будь-якого многочлена $f(x) \in P[x]$ ненульового степеня.

Іншими словами, P *є алгебраїчно замкненим полем, якщо усі корені будь-якого многочлена* $f(x) \in P[x]$ *належать цьому самому полю*.

Поле **C** комплексних чисел є єдиним числовим полем, що має цю властивість.

Формули Вієта

Нехай задано многочлен

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_3 x^3 + a_2 x^2 + a_1 x + a_0,$$

$f(x) \in P[x]$ і $x_1, x_2, \ldots, x_n$ – його корені, які належать до деякого розширення T поля P ($P \subset T$).

Тоді справедливі формули (*формули Вієта*):

$$x_1 + x_2 + ... + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n},$$

$$x_1 x_2 + x_1 x_3 + x_1 x_4 .. + x_{n-1} x_n = \frac{a_{n-2}}{a_n},$$

$$x_1 x_2 x_3 + x_1 x_2 x_4 + ... + x_{n-2} x_{n-1} x_n = -\frac{a_{n-3}}{a_n},$$

. . . .

$$x_1 x_2 x_3 ... x_n = (-1)^n \frac{a_0}{a_n}.$$

Для розв’язання задач корисними будуть такі формули:

$$x_1^{\ 2} + x_2^{\ 2} = (x_1 + x_2)^2 - 2\, x_1 x_2;$$

$$x_1^{\ 3} + x_2^{\ 3} = (x_1 + x_2)^3 - 3 x_1^{\ 2} x_2 - 3 x_1 x_2^{\ 2} = (x_1 + x_2)^3 - 3\,(x_1 + x_2) x_1 x_2;$$

$$x_1^{\ 4} + x_2^{\ 4} = \left(x_1^{\ 2} + x_2^{\ 2}\right)^2 - 2\, x_1^{\ 2} x_2^{\ 2} = \left((x_1 + x_2)^2 - 2\, x_1 x_2\right)^2 - 2(x_1 x_2)^2;$$

$$x_1^{\ 2} + x_2^{\ 2} + x_3^{\ 2} = (x_1 + x_2 + x_3)^2 - 2\,(x_1 x_2 + x_1 x_3 + x_2 x_3);$$

$$x_1^{\ 3} + x_2^{\ 3} + x_3^{\ 3} = (x_1 + x_2 + x_3)^3 - 3\,(x_1 + x_2 + x_3)\cdot(x_1 x_2 + x_1 x_3 + x_2 x_3) + 3 x_1 x_2 x_3$$

.

Приклад 18.1. *Розв’язати рівняння*

$$x^4 - 4x^3 + 3x^2 + 8x - 10 = 0,$$

якщо відомо, що два його корені відрізняються один від одного лише знаком.

Нехай x_1, x_2, x_3, x_4 – корені заданого рівняння, тоді для них справедливі формули Вієта:

$$x_1 + x_2 + x_3 + x_4 = -(-4) = 4,$$

$$x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 = 3,$$

$$x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 = -8,$$

$$x_1 x_2 x_3 x_4 = -10,$$

до того ж, за умовою задачі $x_1 = -x_2$.

Отже матимемо

$$\begin{cases} x_3 + x_4 = 4, \\ -(x_2)^2 + x_3 x_4 = 3, \\ -(x_2)^2 x_3 - (x_2)^2 x_4 = -8, \\ -(x_2)^2 x_3 x_4 = -10. \end{cases}$$

Розв’яжемо цю систему

$$\begin{cases} x_3 + x_4 = 4, \\ -(x_2)^2 + x_3x_4 = 3, \\ -(x_2)^2(x_3 + x_4) = -8, \\ -(x_2)^2 x_3x_4 = -10. \end{cases} \Rightarrow \begin{cases} x_3 + x_4 = 4, \\ -(x_2)^2 + x_3x_4 = 3, \\ (x_2)^2 = 2, \\ -(x_2)^2 x_3x_4 = -10. \end{cases} \Rightarrow \begin{cases} x_3 + x_4 = 4, \\ x_3x_4 = 5, \\ (x_2)^2 = 2. \end{cases}$$

Звідси, числа x_3 та x_4 є коренями рівняння

$$t^2 - 4t + 5 = 0.$$

$$D = 16 - 20 = -4, \quad \sqrt{-4} = \pm 2i,$$

$$t_1 = 2 + i, \quad t_2 = 2 - i.$$

Таким чином, коренями заданого рівняння є числа

$$\sqrt{2}, \quad -\sqrt{2}, \quad 2+i, \quad 2-i.$$

Приклад 18.2. *Знайти суму кубів коренів рівняння*

$$x^3 + 2x^2 + x - 3 = 0.$$

Нехай x_1, x_2, x_3 – корені заданого рівняння, тоді за формулами Вієта:

$$x_1 + x_2 + x_3 = -2,$$

$$x_1x_2 + x_1x_3 + x_2x_3 = 1,$$

$$x_1x_2x_3 = 3.$$

З відомого співвідношення

$$x_1^3 + x_2^3 + x_3^3 = (x_1 + x_2 + x_3)^3 - 3(x_1 + x_2 + x_3)\cdot(x_1x_2 + x_1x_3 + x_2x_3) + 3x_1x_2x_3 =$$

$$= (-2)^3 - 3\cdot(-2)\cdot 1 + 3\cdot 3 = 7.$$

Приклад 18.3. *Скласти кубічне рівняння, коренями якого є квадрати коренів рівняння* $x^3 - 2x^2 + x - 12 = 0$.

Нехай x_1, x_2, x_3 – корені заданого рівняння, тоді за формулами Вієта:

$$x_1 + x_2 + x_3 = 2,$$

$$x_1x_2 + x_1x_3 + x_2x_3 = 1,$$

$$x_1x_2x_3 = 12.$$

Корені шуканого рівняння позначимо y_1, y_2, y_3. За умовою задачі $y_1 = x_1^2, \quad y_2 = x_2^2, \quad y_3 = x_3^2$.

Складемо для них формули Вієта:

$$y_1 + y_2 + y_3 = x_1^2 + x_2^2 + x_3^2 =$$

$$= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = 2^2 - 2\cdot 1 = 2,$$

$$y_1y_2 + y_1y_3 + y_2y_3 = x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 =$$

$$= (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2) =$$

$$= (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2x_1x_2x_3\cdot(x_1 + x_2 + x_3) = 1^2 - 2\cdot 12\cdot 2 = -47,$$

$$y_1y_2y_3 = x_1^2x_2^2x_3^2 = (x_1x_2x_3)^2 = 12^2 = 144.$$

Таким чином, y_1, y_2, y_3 є коренями рівняння $y^3 - 2y^2 - 47y - 144 = 0$.

Приклад 18.4. *Розв'язати систему рівнянь*:

$$\begin{cases} x^3 + y^3 = 35, \\ x + y = 5. \end{cases}$$

Маємо *симетричну* систему рівнянь (систему, яка не зміниться внаслідок довільної перестановки змінних) з двома невідомими. Для розв'язання таких систем вводять нові змінні:

$$u = x + y,$$

$$v = x \cdot y.$$

Тоді система набуває вигляду:

$$\begin{cases} u^3 - 3uv = 35, \\ u = 5. \end{cases} \Rightarrow \begin{cases} v = 6, \\ u = 5. \end{cases}$$

Отже, x, y є коренями рівняння $t^2 - ut + v = 0$ (*зауважимо*, що таке рівняння має дійсні корені за умови, що $u^2 - 4v \geq 0$).

$t^2 - 5t + 6 = 0$, корені цього рівняння $t_1 = 2$, $t_2 = 3$. Всі розв'язки системи дістаємо перестановкою цих чисел.

Розв'язками системи є набори (2, 3), (3, 2).

Приклад 18.5. *Розв'язати систему рівнянь*:

$$\begin{cases} x + y + z = 1, \\ x^2 + y^2 + z^2 = 9, \\ x^3 + y^3 + z^3 = 1. \end{cases}$$

Ця система також є симетричною. Введемо нові змінні:

$$u = x + y + z,$$

$$v = xy + xz + yz,$$

$$w = xyz.$$

Тоді система набуває вигляду:

$$\begin{cases} u = 1, \\ u^2 - 2v = 9, \\ u^3 - 3uv + 3w = 1. \end{cases} \Rightarrow \begin{cases} u = 1, \\ v = -4, \\ w = -4. \end{cases}$$

Отже, x, y, z є коренями рівняння $t^3 - ut^2 + vt - w = 0$.

$$t^3 - t^2 - 4t + 4 = 0,$$

$$t^2(t-1) - 4(t-1) = 0,$$

$$(t-2)(t+2)(t-1) = 0,$$

корені цього рівняння $t_1 = 2$, $t_2 = -2$, $t_3 = 1$.

Всі розв'язки системи дістаємо перестановкою цих чисел.

Відповідь: (2, –2, 1), (2, 1, –2), (–2, 2, 1), (–2, 1, 2), (1, 2, –2), (1, –2, 2).

19 МНОГОЧЛЕНИ ВІД *n* ЗМІННИХ СИМЕТРИЧНІ МНОГОЧЛЕНИ

Розглянемо многочлен від n невідомих

$$f(x_1, x_2, ..., x_n),$$

його можна подати у вигляді скінченної суми

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{m} a_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}, \qquad (1)$$

Вираз виду $ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ в (1) називають *одночленом*, або членом многочлена $f(x_1, x_2, ..., x_n)$, $a \in K$ називають *коефіцієнтом* одночлена, $k_i \in \mathbf{N} \cup \{0\}$.

Означення. Два одночлени

$$\alpha = a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \quad \text{та} \quad \beta = b x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$$

називають *рівними*, якщо $a = b$, $k_i = t_i$ (i = 0, 1, 2, …, n).

Два одночлени $\alpha = ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$, $\beta = bx_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ називають *подібними*, якщо $a \neq b$, $k_i = t_i$ (i = 0, 1, 2, …, n).

При записі многочлена у формі (1) будемо вважати, що серед членів многочлена немає подібних. Таку форму многочлена називають *канонічною*.

Означення. Два многочлени від n змінних називають *рівними*, якщо їх канонічні форми складаються з одних і тих самих членів.

Степенем одночлена $\alpha = ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ називають число

$$s = k_1 + k_2 + \ldots + k_n.$$

Найбільший серед степенів членів многочлена $f(x_1, x_2, ..., x_n)$ називають *степенем цього многочлена*, позначають

$$\deg f = m.$$

Член з найбільшим степенем називають *старшим членом* многочлена $f(x_1, x_2, ..., x_n)$. Зрозуміло, що у многочлена $f(x_1, x_2, ..., x_n)$ може бути декілька старших членів.

Нуль-многочлену $\theta(x_1, x_2, ..., x_n)$, всі коефіцієнти якого дорівнюють нулю, не приписують степеня.

Многочлени нульового степеня – це ненульові елементи кільця K.

Якщо всі члени многочлена $f(x_1, x_2, ..., x_n)$ мають один і той самий степінь l, то многочлен називають *однорідним многочленом*, або формою степеня l.

Звідси зокрема випливає, що однорідний многочлен не містить вільного члена.

Очевидно, що будь-який многочлен $f(x_1, x_2, ..., x_n)$ можна подати як суму скінченного числа однорідних многочленів різних степенів.

Над многочленами від n змінних можна виконувати операції додавання (воно зводиться до додавання подібних членів) та множення (воно зводиться до почленного множення).

Різні способи упорядкування многочленів

Многочлени від n змінних можна впорядкувати такими способами:

1) *за степенями одночленів,*

тобто многочлен $f(x_1, x_2, ..., x_n)$ подається у вигляді суми однорідних многочленів

$$f = \varphi_{l_1} + \ldots + \varphi_{l_s}.$$

2) *за степенями однієї змінної,*

тобто многочлен $f(x_1, x_2, ..., x_n)$ подається як многочлен від однієї змінної, коефіцієнти в якому – многочлени від $n-1$ решти змінних.

3) *лексико-графічним способом*,

при якому застосовується принцип розташування слів у словнику, а саме серед двох одночленів

$$\alpha = a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

$$\beta = b x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$$

α називають *вищим* за β, якщо $k_1 = t_1,\ k_2 = t_2,\ \ldots,\ k_i > t_i$.

При цьому впорядкуванні одночлен, який вище за всі інші, називають *вищим членом многочлена* $f(x_1, x_2, ..., x_n)$ і в записі многочлена його ставлять першим.

Наприклад, многочлен

$$f(x_1, x_2, x_3) = x_1^3 x_2^2 + x_1^4 x_3^2 + x_1^2 x_2^3 x_3^3 + x_2^3 x_3^2 + x_1^4 x_2^1 + x_1^3 x_2^2 x_3^1$$

впорядкуємо за степенями одночленів:

$$f(x_1, x_2, x_3) = x_1^2 x_2^3 x_3^3 + \left(x_1^4 x_3^2 + x_1^3 x_2^2 x_3^1\right) + \left(x_1^3 x_2^2 + x_2^3 x_3^2 + x_1^4 x_2^1\right);$$

впорядкуємо за степенями змінної x_3:

$$f(x_1, x_2, x_3) = \left(x_1^2 x_2^3\right) x_3^3 + \left(x_1^4 + x_2^3\right) x_3^2 + \left(x_1^3 x_2^2\right) x_3^1 + \left(x_1^4 x_2^1 + x_1^3 x_2^2\right);$$

впорядкуємо заданий многочлен лексико-графічно:

$$f(x_1, x_2, x_3) = x_1^4 x_2^1 + x_1^4 x_3^2 + x_1^3 x_2^2 x_3^1 + x_1^3 x_2^2 + x_1^2 x_2^3 x_3^3 + x_2^3 x_3^2.$$

Теорема 19.1. *Вищий член добутку двох многочленів дорівнює добутку вищих членів цих многочленів (при лексико-графічному впорядкуванні).*

Многочлен $f(x_1, x_2, \ldots, x_n)$ від n змінних називають *симетричним*, якщо він не змінюється внаслідок довільної перестановки змінних.

Наприклад, $f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3$, $f(x, y) = x^2 y + y^2 x$ є симетричним.

***Властивості симетричних многочленів*:**

1. *Сума, різниця і добуток симетричних многочленів є симетричним многочленом.*

2. *Якщо симетричний многочлен містить член, в який невідоме x_i входить з показником k, то він містить і член, утворений внаслідок довільної транспозиції змінних $x_i \leftrightarrow x_j$, тобто член, в який невідоме x_j входить в тому ж степені k.*

3. *Якщо $A x_1^{l_1} x_2^{l_2} x_3^{l_3} \ldots x_n^{l_n}$ – вищий член симетричного многочлена, то*

$$l_1 \geq l_2 \geq l_3 \geq \ldots \geq l_n .$$

Чи можна доповнити многочлен $f(x_1, x_2, x_3) = x_1^3 x_2^2 + \ldots$ найменшим числом нових членів, щоб він став симетричним?

Заданий многочлен є многочленом від трьох змінних, за властивістю 2, він повинен містити всі одночлени, які містять одну змінну в степені 3, а іншу – в степені 2 (степінь третьої змінної в цих одночленах дорівнює нулю), тобто

$$f(x_1, x_2, x_3) = x_1^3 x_2^2 + x_1^3 x_3^2 + x_2^3 x_1^2 + x_2^3 x_3^2 + x_3^3 x_1^2 + x_3^3 x_2^2 .$$

Такі симетричні многочлени називають *моногенними*, вони складаються з одночленів одного виду, або *орбітою* $O(x_1^3 x_2^2)$ одночлена $x_1^3 x_2^2$, тобто

$$f(x_1, x_2, x_3) = O(x_1^3 x_2^2).$$

Елементарними симетричними многочленами від n змінних називають многочлени

$$\sigma_1 = x_1 + x_2 + \ldots + x_{n-1} + x_n ,$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 .. + x_{n-1} x_n ,$$

$$\sigma_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + \ldots + x_{n-2} x_{n-1} x_n ,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n = x_1 x_2 x_3 \ldots x_n .$$

Теорема 19.2 (*основна теорема теорії симетричних многочленів*). *Будь-який симетричний многочлен $f(x_1, x_2, \ldots, x_n)$ від n змінних над полем P можна подати у вигляді многочлена $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ від елементарних симетричних многочленів $\sigma_1, \sigma_2, \ldots, \sigma_n$ цих змінних, коефіцієнти якого належать тому самому полю P. Таке представлення єдине.*

Приклад 19.1. Виразити через елементарні симетричні многочлени многочлен

$$f(x_1,x_2,x_3)=x_1^5x_2x_3+x_2^5x_1x_3+x_3^5x_1x_2+2x_1x_2x_3.$$

Наступний алгоритм застосовується до однорідних симетричних многочленів. *Однорідним* називають многочлен, всі члени якого мають один й той самий степінь s.

Подамо заданий многочлен у вигляді суми однорідних многочленів:

$$f(x_1,x_2,x_3)=\left(x_1^5x_2x_3+x_2^5x_1x_3+x_3^5x_1x_2\right)+\left(x_1x_2x_3\right)=f_1+f_2.$$

Застосуємо алгоритм до кожного з них.

$$f_1(x_1,x_2,x_3)=x_1^5x_2x_3+x_2^5x_1x_3+x_3^5x_1x_2 \qquad (2)$$

Випишемо вищий член многочлена f_1:

$$x_1^5x_2^1x_3^1. \qquad (3)$$

За вищим членом многочлена f_1 складемо допоміжний многочлен від елементарних симетричних многочленів

$$x_1^5x_2^1x_3^1 \quad \to \quad \sigma_1^{5-1}\sigma_2^{1-1}\sigma_3^1.$$

Правило утворення допоміжного многочлена

$$\boxed{Ax_1^{k_1}x_2^{k_2}x_3^{k_3}\ldots x_n^{k_n} \quad \to \quad A\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\sigma_3^{k_3-k_4}\ldots\sigma_{n-1}^{k_{n-1}-k_n}\sigma^{k_n}}$$

Складемо систему вищих членів многочленів, які можуть утворитися після віднімання від многочлена f_1 таких допоміжних многочленів (вони не можуть бути вище за (3), вони всі мають бути степеня однорідності 7, оскільки допоміжний многочлен, як і многочлен f_1 є однорідним степеня 7, і для них виконується властивість 3 симетричних многочленів):

$Bx_1^4x_2^3x_3^0$

$Cx_1^4x_2^2x_3^1$

$Dx_1^3x_2^3x_3^1$

$Ex_1^3x_2^2x_3^2$

Система показників $l_1,l_2,l_3,\ldots,l_n$

степенів в цих вищих членах повинна мати такі властивості:

1) $\forall i \quad l_i\le k_1$;

2) $l_1+l_2+l_3+\ldots+l_n=s$, де $s=\deg f_1$;

3) $l_1\ge l_2\ge l_3\ge\ldots\ge l_n$

За кожним з цих вищих членів знов складемо допоміжний многочлен від елементарних симетричних многочленів:

$$\begin{array}{rcl} x_1^{5} x_2^{1} x_3^{1} & \to & \sigma_1^{5-1}\sigma_2^{1-1}\sigma_3^{1} \\ B\,x_1^{4} x_2^{3} x_3^{0} & \to & B\sigma_1^{4-3}\sigma_2^{3-0}\sigma_3^{0} \\ C\,x_1^{4} x_2^{2} x_3^{1} & \to & C\sigma_1^{4-2}\sigma_2^{2-1}\sigma_3^{1} \\ D\,x_1^{3} x_2^{3} x_3^{1} & \to & D\sigma_1^{3-3}\sigma_2^{3-1}\sigma_3^{1} \\ E\,x_1^{3} x_2^{2} x_3^{2} & \to & E\sigma_1^{3-2}\sigma_2^{2-2}\sigma_3^{2} \end{array}$$

Тоді f_1 є сумою всіх цих допоміжних многочленів:

$$f_1(x_1, x_2, x_3) = \sigma_1^{4}\sigma_3^{1} + B\sigma_1^{1}\sigma_2^{3} + C\sigma_1^{2}\sigma_2^{1}\sigma_3^{1} + D\sigma_2^{2}\sigma_3^{1} + E\sigma_1^{1}\sigma_3^{2}, \qquad (4)$$

де

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + x_3, \\ \sigma_2 &= x_1x_2 + x_1x_3 + x_2x_3, \qquad (5) \\ \sigma_3 &= x_1x_2x_3. \end{aligned}$$

Залишається знайти коефіцієнти B, C, D, E.

Для цього змінним x_1, x_2, x_3 надамо довільних значень (значення σ_1, σ_2, σ_3 знайдемо за (5), значення многочлена $f_1(x_1, x_2, x_3)$ визначимо з (2) та (4)):

x_1	x_2	x_3	σ_1	σ_2	σ_3	$f_1(x_1, x_2, \ldots, x_n)$	
0	1	1	2	1	0	$0 = 2B$	$B = 0$
2	–1	–1	0	–3	2	$36 = 18D$	$D = 2$
1	1	1	3	3	1	$3 = 81 + 27C + 18 + 3E$	
1	1	2	4	5	2	$36 = 512 + 160C + 100 + 16E$	

$$\begin{cases} 9C + E = -32, \\ 10C + E = -36. \end{cases}$$

$C = -4$, $E = 4$.

Таким чином,

$$f_1(x_1, x_2, x_3) = \sigma_1^{4}\sigma_3 - 4\sigma_1^{2}\sigma_2\sigma_3 + 2\sigma_2^{2}\sigma_3 + 4\sigma_1\sigma_3^{2}.$$

$$f_2(x_1, x_2, x_3) = 2\sigma_3.$$

$$f(x_1, x_2, x_3) = f_1 + f_2 = \sigma_1^{4}\sigma_3 - 4\sigma_1^{2}\sigma_2\sigma_3 + 2\sigma_2^{2}\sigma_3 + 4\sigma_1\sigma_3^{2} + 2\sigma_3.$$

20 МНОГОЧЛЕНИ ВІД ОДНІЄЇ ЗМІННОЇ НАД ПОЛЕМ C та R

Многочлени з числовими коефіцієнтами до середини XIX ст. були основним предметом вивчення алгебри. Тому, теорема, яку розглянемо в цьому розділі, зберегла свою історичну назву „Основна теорема алгебри”.

Важливими характеристиками многочлена є наявність, кількість та розміщення його коренів, отже суттєво над яким полем розглядаємо многочлен.

Лема (*про модуль старшого члена многочлена*). *Нехай*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \in \mathbf{C}\,[x],\;\; n \geq 1,$$

тоді для довільного дійсного $k > 0$ *існує дійсне додатне* l, *що* $\forall \,|\, x \,|\, \geq l$ *має місце співвідношення*

$$|\; a_n x^n \;| \;>\; k \,|\; a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \;|. \qquad (1)$$

Таким дійсним додатним числом є

$$1 + \frac{k\,A}{|\; a_n \;|} = l\,.$$

Наслідок 1. *Якщо* $\alpha \in \mathbf{C}$ *є коренем многочлена* $f(x) \in \mathbf{C}[x]$ *степеня* $n \geq 1$, *то* $|\alpha| < l$, *де*

$$l = 1 + \frac{A}{|\; a_n \;|} \qquad (k = 1).$$

Тобто всі комплексні корені многочлена $f(x)$ *знаходяться на комплексній площині всередині кола радіуса* l *з центром в точці* O.

Наслідок 2. *Нехай многочлен* $f(x)$ *ненульового степеня має дійсні коефіцієнти, тоді при досить великих значеннях* $|x|$ *знак многочлена співпадає із знаком його старшого члена.*

Наслідок 3. *Многочлен* $f(x)$ *з дійсними коефіцієнтами непарного степеня має принаймні один дійсний корінь.*

Теорема 20.1. (*Гаусса*, „*Основна теорема алгебри*”). *Кожен многочлен* $f(x)$ *степеня* $n \geq 1$ *з числовими коефіцієнтами має принаймні один комплексний корінь.*

Наслідки з теореми Гаусса для многочленів з комплексними коефіцієнтами

Наслідок 1. *Незвідними над полем* $\mathbf{C}$ *є лише многочлени першого степеня.*

Наслідок 2. *Кожен многочлен* $f(x) \in \mathbf{C}[x]$ *степеня* $n \geq 1$ *розкладається над полем* $\mathbf{C}$ *в добуток лінійних множників і таке представлення єдине з точністю до порядку запису множників і асоційованих:*

$$f(x) = (a_1 x + b_1) \cdot (a_2 x + b_2) \cdot \ldots \cdot (a_n x + b_n) =$$
$$= a_1 \cdot a_2 \cdot \ldots \cdot a_n (x + \frac{b_1}{a_1}) \cdot (x + \frac{b_2}{a_2}) \cdot \ldots \cdot (x + \frac{b_n}{a_n}) =$$
$$= A\,(x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n) \text{ –}$$

канонічний розклад многочлена над полем $\mathbf{C}$, α_i – його корені, A – старший коефіцієнт.

З розкладу многочлена $f(x)$ випливає, що жодне комплексне число, відмінне від чисел α_i, не може бути коренем цього многочлена. Тобто

Твердження 1. *Многочлен n-го степеня має в полі* $\mathbf{C}$ *точно n коренів.*

Всі $\alpha_i \in \mathbf{C}$, тобто полем розкладу будь-якого многочлена $f(x) \in \mathbf{C}[x]$ є поле $\mathbf{C}$. Звідси

Твердження 2. *Поле* $\mathbf{C}$ *є алгебраїчно замкненим.*

Наслідки з теореми Гаусса для многочленів з дійсними коефіцієнтами

Наслідок 3. *Якщо комплексне число* z *є коренем многочлена* $f(x) \in \mathbf{R}[x]$ *кратності k, то число* $\overline{z}$, *спряжене з* z, *також є коренем* $f(x)$ *тієї ж кратності.*

Тобто многочлен $f(x)$ ділиться на многочлен

$$\varphi(x) = \left(x - z\right) \cdot \left(x - \overline{z}\right) = x^2 - \underbrace{\left(z + \overline{z}\right)}_{\in \mathbf{R}} x + \underbrace{z \cdot \overline{z}}_{\in \mathbf{R}},$$

який має дійсні коефіцієнти.

Наслідок 4. *Незвідними над полем* $\mathbf{R}$ *можуть бути лише многочлени першого та другого степенів.*

Наслідок 5. *Кожен многочлен* $f(x) \in \mathbf{R}[x]$ *степеня* $n \geq 1$ *розкладається над полем* $\mathbf{R}$ *в добуток лінійних множників та множників другого степеня* (*лінійним множникам відповідають дійсні корені, множникам 2-го степеня – комплексні корені*) *і таке представлення єдине з точністю до порядку запису множників і асоційованих.*

Тобто

$$f(x) = (a_1 x + b_1) \cdot \ldots \cdot (a_m x + b_m) \cdot \left(c_1 x^2 + d_1 x + k_1\right) \cdot \ldots \cdot \left(c_t x^2 + d_t x + k_t\right) =$$
$$= A\,(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) \cdot \left(x^2 + u_1 x + v_1\right) \cdot \ldots \cdot \left(x^2 + u_t x + v_t\right) \text{ –}$$

канонічний розклад многочлена над полем $\mathbf{R}$.

Приклад 20.1. *Знайти на комплексній площині коло, в якому знаходяться всі комплексні корені рівняння*

$$x^{1982} - 4x^{24} + 4x^3 - 7x^2 + 1 = 0.$$

Згідно з наслідком 1 до Леми про модуль старшого члена: *Якщо* $\alpha \in \mathbf{C}$ *є коренем многочлена* $f(x) \in \mathbf{C}[x]$ *степеня* $n \geq 1$, *то* $|\alpha| < l$, *де*

$$l = 1 + \frac{A}{|a_n|}$$

$(k = 1)$, $A = \max\{|a_{n-1}|, \ldots, |a_2|, |a_1|, |a_0|\}$.

Тобто всі комплексні корені многочлена

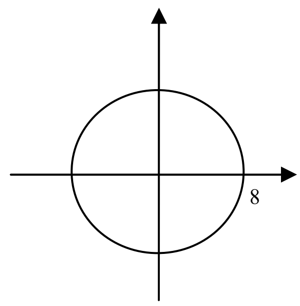
$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

знаходяться на комплексній площині всередині кола радіуса l з центром в точці *O*. А всі дійсні корені многочлена $f(x)$ знаходяться на осі Ox, тобто в інтервалі $(-l, l)$.

Знайдемо число l.

$A = \max\{|a_{24}|, \ldots, |a_3|, |a_2|, |a_0|\} = 7$,

$|a_{1982}| = 1$,



отже $l = 1 + \frac{7}{1} = 8$ – всі комплексні корені многочлена містяться всередині кола радіуса 8.

Приклад 20.2. *Чи може число* $3 - 4i$ *бути коренем многочлена*

$$f(z) = 2i z^5 + 3z^4 - (1+i)z^2 + (2-3i)z - 4i\ ?$$

Знов спираємось на наслідок 1 до Леми про модуль старшого члена. Знайдемо модулі всіх коефіцієнтів (пригадайте, як обчислити модуль комплексного числа), вибрати A, знайти l =3.

Знайдемо $|3-4i| = \sqrt{3^2+4^2} = 5$, задане число не міститься в колі радіуса 3, отже воно не може бути коренем заданого многочлена.

Приклад 20.3. *Чи має многочлен* $f(x) = 2x^3 - 3x^2 + 4x - 1$ *корінь в проміжку* [4, 10]?

Для заданого многочлена $l = 3$. Дійсні корені цього многочлена містяться на дійсній осі, тобто в інтервалі (– 3, 3), тому коренів з проміжку [4, 10] бути не може.

Приклад 20.4. *Довести, що многочлен* $f(x)=6x^5-4x^3+2x^2+3x-1$ *при всіх* $x \geq 2$ *набуває тільки додатних значень.*

Згідно з наслідком 2 до Леми про модуль старшого члена: *Якщо многочлен* $f(x)$ *ненульового степеня має дійсні коефіцієнти, то при досить великих значеннях* $|x|$ *знак многочлена співпадає із знаком його старшого члена.*

Знаходимо $l=\frac{5}{3}$, межі дійсних коренів заданого многочлена $\left(-\frac{5}{3},\frac{5}{3}\right)$.

Отже при $x \geq 2$ знак $f(x)$ співпадає із знаком старшого члена. Візьмемо $x=3$, тоді старший член $6 \cdot 3^5$ – він додатний.

Приклад 20.5. *Розв'язати рівняння*

$$x^4+x^3-x^2-10x-12=0,$$

якщо $x_1=-1+i\sqrt{3}$.

Згідно з наслідком 3 до „Основної теореми алгебри": *Якщо комплексне число* z *є коренем многочлена* $f(x)\in \mathbf{R}[x]$ *кратності* k, *то число* $\overline{z}$, *спряжене з* z, *також є коренем* $f(x)$ *тієї ж кратності.*

Звернемо увагу, що у лівій частині – многочлен з дійсними коефіцієнтами $f(x)\in \mathbf{R}[x]$, його корінь x_1 є комплексним, отже заданий многочлен має своїм коренем і спряжене до x_1. Тобто знаємо ще один корінь $x_2=\overline{x_1}=-1-i\sqrt{3}$, тоді

$$f(x) \,\vdots\, (x-x_1)(x-x_2),$$

$$(x-x_1)(x-x_2)=(x+1-i\sqrt{3})(x+1+i\sqrt{3})=(x+1)^2+3=x^2+2x+4.$$

Поділимо стовпчиком $f(x)$ на x^2+2x+4, отримаємо

$$f(x)=(x^2+2x+4)(x^2-x-3),$$

після цього знайдемо x_3, x_4.

Приклад 20.6. *Знайти многочлен найменшого степеня, в якого число* i *є подвійним коренем, а* $1-i$ *– простим.*

В умові не сказано, з якого поля коефіцієнти многочлена, тому слід розглянути два випадки:

1) якщо $f(x)\in \mathbf{C}[x]$, то $f(x)=(x-i)^2(x-1+i)$;

2) якщо $f(x)\in \mathbf{R}[x]$, то $-i$ також є подвійним коренем, а $1+i$ – простим, тому

$$f(x)=(x-i)^2(x+i)^2(x-1+i)(x-1-i)=(x^2+1)^2(x^2-2x+2).$$

21 РОЗВ'ЯЗУВАННЯ АЛГЕБРАЇЧНИХ РІВНЯНЬ 3-ГО СТЕПЕНЯ (ФОРМУЛИ КАРДАНО)

Нехай задано рівняння

$$x^3 + ax^2 + bx + c = 0. \tag{1}$$

Підстановка $x = y - \frac{a}{3}$ зведе його до виду

$$y^3 + py + q = 0. \tag{2}$$

Розв'язок цього рівняння шукають у вигляді: $y = u + v$, де на u та v накладають додаткову умову:

$$u \cdot v = -\frac{p}{3}. \tag{3}$$

Дискримінантом кубічного рівняння називають число

$$D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3.$$

Тоді $u = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}$.

Знайдемо одне із значень цього кореня, позначимо його u_0.

Після цього можемо знайти v_0 (з додаткової умови (3)):

$$v_0 = -\frac{p}{3u_0}.$$

Тепер запишемо корені рівняння (2) за *формулами Кардано*:

$$\begin{aligned} y_0 &= u_0 + v_0, \\ y_1 &= -\frac{1}{2}(u_0 + v_0) + \frac{\sqrt{3}}{2} i\,(u_0 - v_0), \\ y_2 &= -\frac{1}{2}(u_0 + v_0) - \frac{\sqrt{3}}{2} i\,(u_0 - v_0). \end{aligned} \tag{4}$$

Для знаходження коренів рівняння (1) повернемось до змінної x:

$$x_0 = y_0 - \frac{a}{3}, \qquad x_1 = y_1 - \frac{a}{3}, \qquad x_2 = y_2 - \frac{a}{3}.$$

Теорема 21.1. *Якщо кубічне рівняння* $y^3 + py + q = 0$ *з дійсними коефіцієнтами має дискримінант D, який*

1) $D > 0$, *то таке рівняння має один дійсний корінь і два комплексні спряжені корені;*

2) $D = 0$, *то всі корені такого рівняння дійсні,причому два з них рівні між собою;*

3) $D < 0$, *то таке рівняння має три різні дійсні корені.*

Приклад 21.1. *Розв'язати рівняння*

$$x^3 + 9x^2 + 18x + 28 = 0.$$

Для виключення доданка, що містить x^2, застосуємо підстановку

$$x = y - 3:$$

$$(y-3)^3 + 9(y-3)^2 + 18(y-3) + 28 = 0,$$

$$y^3 - 9y + 28 = 0.$$

Тут $p = -9$, $q = 28$. Тоді

$$D = 14^2 + (-3)^3 = 169, \quad \sqrt{D} = 13.$$

Утворимо формулу для обчислення u:

$$u = \sqrt[3]{-14+13} = \sqrt[3]{-1},$$

одним із значень цього кореня є $u_0 = -1$.

Із співвідношення (3) знайдемо $v_0 = -\dfrac{-9}{3\cdot(-1)} = -3$.

За формулами (4):

$$y_0 = -1 - 3 = -4,$$

$$y_1 = -\frac{1}{2}(-4) + \frac{\sqrt{3}}{2} i \cdot 2 = 2 + \sqrt{3}\, i,$$

$$y_2 = -\frac{1}{2}(-4) - \frac{\sqrt{3}}{2} i \cdot 2 = 2 - \sqrt{3}\, i.$$

Повертаючись до змінної x, дістанемо

$$x_0 = y_0 - 3 = -4 - 3 = -7,$$

$$x_1 = y_1 - 3 = 2 + \sqrt{3}\, i - 3 = -1 + \sqrt{3}\, i,$$

$$x_2 = y_2 - 3 = 2 - \sqrt{3}\, i - 3 = -1 - \sqrt{3}\, i.$$

Приклад 21.2. *Розв'язати рівняння*

$$x^3 - 6x + 4 = 0.$$

Доданка, що містить x^2, в цьому рівнянні немає, тобто одразу маємо рівняння виду (2), в якому $p = -6$, $q = 4$.

Знаходимо $D = 2^2 + (-2)^3 = -4$, $\sqrt{D} = 2i$.

Утворимо формулу для обчислення u:

$$u = \sqrt[3]{-2+2i}.$$

Для обчислення кубічного кореня запишемо число $-2+2i$ в тригонометричній формі

$$-2+2i = 2\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right),$$

за формулою добування кореня n-го степеня з комплексного числа:

$$\sqrt[3]{-2+2i} = \sqrt[3]{2\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)} =$$

$$= \sqrt{2}\left(\cos\frac{\frac{3\pi}{4}+2\pi k}{3} + i\sin\frac{\frac{3\pi}{4}+2\pi k}{3}\right), \quad k = 0, 1, 2.$$

Одним із значень цього кореня (при $k=0$) є

$$u_0 = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 1+i.$$

Із співвідношення (3) знайдемо

$$v_0 = -\frac{-6}{3\cdot(1+i)} = \frac{2}{1+i} = \frac{2(1-i)}{2} = 1-i.$$

За формулами (4):

$$x_0 = (1+i)+(1-i) = 2,$$

$$x_1 = -\frac{1}{2}\cdot 2 + \frac{\sqrt{3}}{2}i\cdot 2\,i = -1-\sqrt{3},$$

$$x_2 = -\frac{1}{2}\cdot 2 - \frac{\sqrt{3}}{2}i\cdot 2\,i = -1+\sqrt{3}.$$

22 РОЗВ'ЯЗУВАННЯ АЛГЕБРАЇЧНИХ РІВНЯНЬ 4-ГО СТЕПЕНЯ (МЕТОД ФЕРРАРІ)

Розв'язати рівняння

$$x^4 + ax^3 + bx^2 + cx + d = 0. \qquad (1)$$

Залишимо в лівій частині перші два доданки, решту доданків перенесемо в праву частину

$$x^4 + ax^3 = -bx^2 - cx - d,$$

виділимо повний квадрат в лівій частині рівняння (для цього додамо до обох частин рівняння доданок $\frac{a^2}{4}x^2$):

$$\left(x^2 + \frac{a}{2}x\right)^2 = \frac{a^2}{4}x^2 - bx^2 - cx - d.$$

Внесемо в дужку допоміжне невідоме t, або для зручності обчислень $\frac{t}{2}$ (тобто до обох частин рівняння додамо вираз $t\left(x^2 + \frac{a}{2}x\right) + \frac{t^2}{4}$):

$$\left(\underbrace{x^2 + \frac{a}{2}x} + \frac{t}{2}\right)^2 = \frac{a^2}{4}x^2 - bx^2 - cx - d + t\left(x^2 + \frac{a}{2}x\right) + \frac{t^2}{4},$$

спростимо

$$\left(x^2 + \frac{a}{2}x + \frac{t}{2}\right)^2 = \left(\frac{a^2}{4} - b + t\right)x^2 + \left(\frac{at}{2} - c\right)x + \left(\frac{t^2}{4} - d\right). \qquad (2)$$

Підберемо t так, щоб праву частину рівняння можна було подати у вигляді повного квадрату, тобто у вигляді $(Ax + B)^2$, для цього дискримінант правої частини має дорівнювати нулю:

$$\left(\frac{at}{2} - c\right)^2 - 4\left(\frac{a^2}{4} - b + t\right)\cdot\left(\frac{t^2}{4} - d\right) = 0, \qquad (3)$$

рівняння (3) називають *кубічною резольвентою* рівняння (1).

Знайшовши один з коренів t_0 кубічної резольвенти (3), підставимо його в (2), дістанемо

$$\left(x^2 + \frac{a}{2}x + \frac{t_0}{2}\right)^2 = (Ax + B)^2.$$

Звідси

$$\left(x^2+\frac{a}{2}x+\frac{t_0}{2}\right)^2-(Ax+B)^2=0,$$

$$\left(x^2+\frac{a}{2}x+\frac{t_0}{2}-Ax-B\right)\left(x^2+\frac{a}{2}x+\frac{t_0}{2}+Ax+B\right)=0.$$

Далі задача зводиться до розв'язання двох квадратних рівнянь.

Приклад 22.1. *Розв'язати рівняння*

$$x^4-2x^3+2x^2+4x-8=0.$$

$x^4-2x^3=-2x^2-4x+8,$

$\left(x^2-x\right)^2=x^2-2x^2-4x+8,$

$\left(x^2-x+t\right)^2=-x^2-4x+8+2\left(x^2-x\right)\cdot t+t^2,$

$\left(x^2-x+t\right)^2=(2t-1)x^2-(4+2t)x+t^2+8,$

$D=(4+2t)^2-4(2t-1)\left(t^2+8\right)=0,$

$-8t^3+8t^2-48t+48=0,$

$t^3-t^2+6t-6=0,$

$t_0=1,$

$\left(x^2-x+1\right)^2=x^2-6x+9,$

$\left(x^2-x+1\right)^2=(x-3)^2,$

$\left(x^2-x+1\right)^2-(x-3)^2=0,$

$\left(x^2-x+1-(x-3)\right)\cdot\left(x^2-x+1+x-3\right)=0,$

$\left(x^2-2x+4\right)\cdot\left(x^2-2\right)=0.$

$x^2-2x+4=0,$

$D=4-16=-12,\quad \sqrt{-12}=\pm 2\sqrt{3}i,$

$x_1=\dfrac{2+2\sqrt{3}i}{2}=1+\sqrt{3}i,$

$x_2=\dfrac{2-2\sqrt{3}i}{2}=1-\sqrt{3}i.$

$x^2-2=0,$

$x_3=\sqrt{2},$

$x_4=-\sqrt{2}.$

Приклад 22.2. *Розкласти многочлен*

$$f(x)=x^4-2x^3+2x^2+4x-8.$$

на незвідні множники над полем: а) **Q**, б) **R**, в) **C**.

Розв'яжемо рівняння

$$x^4-2x^3+2x^2+4x-8=0,$$

застосуємо метод Феррарі (див. Приклад 21.1, дістанемо

$$\left(x^2-2x+4\right)\cdot\left(x^2-2\right)=0.$$

а) оскільки перший множник не має дійсних коренів (для нього $D<0$), а коренями другого множника є ірраціональні числа, то розкладом многочлена $f(x)$ на незвідні над полем **Q** множники є:

$$f(x)=\left(x^2-2x+4\right)\cdot\left(x^2-2\right).$$

б) оскільки перший множник не має дійсних коренів (для нього $D<0$), та знайшовши корені другого множника, отримаємо розклад многочлена $f(x)$ на незвідні над полем **R** множники:

$$f(x)=\left(x^2-2x+4\right)\cdot\left(x-\sqrt{2}\right)\cdot\left(x+\sqrt{2}\right).$$

в) знайдемо всі корені многочлена $f(x)$:

$x^2-2x+4=0,$ $\qquad$ $x^2-2=0,$

$x_1=\dfrac{2+2\sqrt{3}i}{2}=1+\sqrt{3}i,$ $\qquad$ $x_3=\sqrt{2},$

$x_2=\dfrac{2-2\sqrt{3}i}{2}=1-\sqrt{3}i,$ $\qquad$ $x_4=-\sqrt{2}.$

Тоді розклад многочлена $f(x)$ на незвідні над полем **C** множники такий:

$$f(x)=\left(x-1-\sqrt{3}i\right)\cdot\left(x-1+\sqrt{3}i\right)\cdot\left(x-\sqrt{2}\right)\cdot\left(x+\sqrt{2}\right).$$

Приклад 22.3. *Розв'язати рівняння*

$$x^4-3x^3+x^2+4x-6=0.$$

$$x^4-3x^3=-x^2-4x+6,$$

$$\left(x^2-\frac{3}{2}x\right)^2=\frac{9}{4}x^2-x^2-4x+6,$$

$$\left(x^2-\frac{3}{2}x+t\right)^2=\frac{5}{4}x^2-4x+6+2\left(x^2-\frac{3}{2}x\right)\cdot t+t^2,$$

$$\left(x^2-\frac{3}{2}x+t\right)^2=\left(2t+\frac{5}{4}\right)x^2-(4+3t)x+t^2+6,$$

$$D=(4+3t)^2-4\left(2t+\frac{5}{4}\right)\left(t^2+6\right)=0,$$

$$8t^3-4t^2+24t+14=0,$$

$$a=2t,$$

$$(2t)^3-(2t)^2+12\cdot(2t)+14=0,$$

$$a^3 - a^2 + 12a + 14 = 0,$$
$$a_0 = -1,$$
$$t_0 = -\frac{1}{2},$$
$$\left(x^2 - \frac{3}{2}x - \frac{1}{2}\right)^2 = \frac{1}{4}x^2 - \frac{5}{2}x + \frac{25}{4},$$
$$\left(x^2 - \frac{3}{2}x - \frac{1}{2}\right)^2 = \left(\frac{1}{2}x - \frac{5}{2}\right)^2,$$
$$\left(x^2 - \frac{3}{2}x - \frac{1}{2}\right)^2 - \left(\frac{1}{2}x - \frac{5}{2}\right)^2 = 0,$$
$$\left(x^2 - 2x + 2\right)\cdot\left(x^2 - x - 3\right) = 0.$$
$$x_1 = \frac{2+2i}{2} = 1 + i, \qquad x_3 = \frac{1+\sqrt{13}}{2},$$
$$x_2 = \frac{2-2i}{2} = 1 - i, \qquad x_4 = \frac{1-\sqrt{13}}{2}.$$

Приклад 22.4. *Розкласти многочлен*

$$f(x) = x^4 - 3x^3 + x^2 + 4x - 6.$$

на незвідні множники над полем: а) **Q**, б) **R**, в) **C**.

Розв'яжемо рівняння

$$x^4 - 3x^3 + x^2 + 4x - 6 = 0,$$

застосуємо метод Феррарі (див. Приклад 21.3), дістанемо

$$\left(x^2 - 2x + 2\right)\cdot\left(x^2 - x - 3\right) = 0.$$

а) розклад многочлена $f(x)$ на незвідні над полем **Q** множники:

$$f(x) = \left(x^2 - 2x + 2\right)\cdot\left(x^2 - x - 3\right).$$

б) розклад многочлена $f(x)$ на незвідні над полем **R** множники:

$$f(x) = \left(x^2 - 2x + 2\right)\cdot\left(x - \frac{1+\sqrt{13}}{2}\right)\cdot\left(x - \frac{1-\sqrt{13}}{2}\right).$$

в) розклад многочлена $f(x)$ на незвідні над полем **C** множники:

$$f(x) = \left(x - 1 - i\right)\cdot\left(x - 1 + i\right)\cdot\left(x - \frac{1+\sqrt{13}}{2}\right)\cdot\left(x + \frac{1-\sqrt{13}}{2}\right).$$

23 РАЦІОНАЛЬНІ КОРЕНІ МНОГОЧЛЕНА

Твердження 1. *Всі дійсні корені многочлена*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0,$$

$f(x) \in \mathbf{C}[x]$ *степеня* $n \geq 1$ *містяться в інтервалі* $(-\alpha, \alpha)$, *де*

$$\alpha = 1 + \frac{A}{|a_n|}, \qquad \left(A = \max\left\{ |a_{n-1}|, |a_{n-2}|, \ldots, |a_0| \right\} \right).$$

Теорема 23.1. (*необхідна умова*) *Якщо нескоротний дріб* $\dfrac{l}{m}$ *є коренем многочлена*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0$$

з цілими коефіцієнтами, то l *є дільником вільного члена* a_0, m *– дільником старшого члена* a_n.

Теорема 23.2. (*необхідна умова*) *Якщо нескоротний дріб* $\dfrac{l}{m}$ *є коренем многочлена* $f(x) \in \mathbf{Z}[x]$, *то для будь-якого цілого* k *вираз* $\dfrac{f(k)}{l - km}$ *є цілим числом*.

Приклад 23.1. Знайти раціональні корені многочлена

$$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6.$$

Знайдемо межі дійсних коренів многочлена:

$$\alpha = 1 + \frac{19}{24} = \frac{43}{24} \approx 1.8,$$

дійсні корені многочлена містяться в інтервалі (– 1.8; 1.8).

Відповідно до теореми 1, встановимо можливих претендентів на корені многочлена $f(x)$:

l: $\pm 1, \pm 2, \pm 3, \pm 6$,

m: $1, 2, 3, 4, 6, 8, 12, 24$,

$\dfrac{l}{m}$: $\pm 1, \pm 2, \pm 3, \pm 6, \pm\dfrac{1}{2}, \pm\dfrac{3}{2}, \pm\dfrac{1}{3}, \pm\dfrac{2}{3}, \pm\dfrac{1}{4}, \pm\dfrac{3}{4}, \pm\dfrac{1}{6}, \pm\dfrac{1}{8}, \pm\dfrac{3}{8}, \pm\dfrac{1}{12}, \pm\dfrac{1}{24}$.

$\pm 2, \pm 3, \pm 6$ одразу вилучимо з претендентів, оскільки вони містяться поза інтервалом (– 1.8; 1.8). Отже

$\dfrac{l}{m}$: $\pm 1, \pm\dfrac{1}{2}, \pm\dfrac{3}{2}, \pm\dfrac{1}{3}, \pm\dfrac{2}{3}, \pm\dfrac{1}{4}, \pm\dfrac{3}{4}, \pm\dfrac{1}{6}, \pm\dfrac{1}{8}, \pm\dfrac{3}{8}, \pm\dfrac{1}{12}, \pm\dfrac{1}{24}$.

До претендентів, що залишилися, застосуємо теорему 23.2.

Нехай $k=1$, обчислимо $f(1) = 15$ (відмітимо, що 1 не є коренем $f(x)$), складемо вираз $\frac{f(k)}{l-km} = \frac{f(1)}{l-m} = \frac{15}{l-m}$, перевіримо, для яких $\frac{l}{m}$ він є цілим числом:

$\frac{1}{2}$: $\frac{15}{1-2} \in \mathbf{Z}$,	$-\frac{1}{2}$: $\frac{15}{-1-2} \in \mathbf{Z}$,
$\frac{3}{2}$: $\frac{15}{3-2} \in \mathbf{Z}$,	$-\frac{3}{2}$: $\frac{15}{-3-2} \in \mathbf{Z}$,
$\frac{1}{3}$: $\frac{15}{1-3} \notin \mathbf{Z}$,	$-\frac{1}{3}$: $\frac{15}{-1-3} \notin \mathbf{Z}$,
$\frac{2}{3}$: $\frac{15}{2-3} \in \mathbf{Z}$,	$-\frac{2}{3}$: $\frac{15}{-2-3} \in \mathbf{Z}$,
$\frac{1}{4}$: $\frac{15}{1-4} \in \mathbf{Z}$,	$-\frac{1}{4}$: $\frac{15}{-1-4} \in \mathbf{Z}$,
$\frac{3}{4}$: $\frac{15}{3-4} \in \mathbf{Z}$,	$-\frac{3}{4}$: $\frac{15}{-3-4} \notin \mathbf{Z}$,
$\frac{1}{6}$: $\frac{15}{1-6} \in \mathbf{Z}$,	$-\frac{1}{6}$: $\frac{15}{-1-6} \notin \mathbf{Z}$,
$\frac{1}{8}$: $\frac{15}{1-8} \notin \mathbf{Z}$,	$-\frac{1}{8}$: $\frac{15}{-1-8} \notin \mathbf{Z}$,
$\frac{3}{8}$: $\frac{15}{3-8} \in \mathbf{Z}$,	$-\frac{3}{8}$: $\frac{15}{-3-8} \notin \mathbf{Z}$,
$\frac{1}{12}$: $\frac{15}{1-12} \notin \mathbf{Z}$,	$-\frac{1}{12}$: $\frac{15}{-1-12} \notin \mathbf{Z}$,
$\frac{1}{24}$: $\frac{15}{1-24} \notin \mathbf{Z}$,	$-\frac{1}{24}$: $\frac{15}{-1-24} \notin \mathbf{Z}$.

Залишились

$$\frac{l}{m}: \ -1, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{2}{3}, \pm\frac{1}{4}, \ \frac{3}{4}, \ \frac{1}{6}, \ \frac{3}{8}.$$

Ще раз застосуємо теорему 23.2. Візьмемо будь-яке інше ціле k, наприклад $k = -1$, обчислимо $f(-1) = -21$ (відмітимо, що -1 не є коренем $f(x)$), складемо вираз $\frac{f(k)}{l-km} = \frac{f(1)}{l+m} = \frac{21}{l+m}$, перевіримо, для яких $\frac{l}{m}$ він є цілим числом:

$\frac{1}{2}$: $\frac{21}{1+2} \in \mathbf{Z}$,	$-\frac{1}{2}$: $\frac{21}{-1+2} \in \mathbf{Z}$,
$\frac{3}{2}$: $\frac{21}{3+2} \notin \mathbf{Z}$,	$-\frac{3}{2}$: $\frac{21}{-3+2} \in \mathbf{Z}$,
$\frac{2}{3}$: $\frac{21}{2+3} \notin \mathbf{Z}$,	$-\frac{2}{3}$: $\frac{21}{-2+3} \in \mathbf{Z}$,

$$\frac{1}{4}: \quad \frac{21}{1+4} \notin \mathbf{Z}, \qquad\qquad -\frac{1}{4}: \quad \frac{21}{-1+4} \in \mathbf{Z},$$

$$\frac{3}{4}: \quad \frac{21}{3+4} \in \mathbf{Z}, \qquad\qquad \frac{1}{6}: \quad \frac{21}{1+6} \in \mathbf{Z},$$

$$\frac{3}{8}: \quad \frac{21}{3+8} \notin \mathbf{Z}.$$

Тепер залишились

$$\frac{l}{m}: \quad \pm\frac{1}{2},\ -\frac{3}{2},\ -\frac{2}{3},\ -\frac{1}{4},\ \frac{3}{4},\ \frac{1}{6}.$$

Ці числа можна перевірити вже безпосередньо за схемою Горнера:

	24	**10**	**– 1**	**– 19**	**– 5**	**6**	
$1/2$	24	22	10	–14	–12	0	перевіримо, чи не є $\frac{1}{2}$ кратним коренем
$1/2$	24	34	27	$-1/2$	$\neq 0$		
$-1/2$	24	10	5	$-33/2$	$\neq 0$		
$-3/2$	24	–14	31	$-121/2$	$\neq 0$		
$-2/3$	24	6	6	–18	0		перевіримо, чи не є $-\frac{2}{3}$ кратним коренем
$-2/3$	24	–10	$38/3$	$\neq 0$			
$-1/4$	24	0	6	$\neq 0$			
$3/4$	24	24	24	0			перевіримо, чи не є $\frac{3}{4}$ кратним коренем
$3/4$	24	42	$\neq 0$				
$1/6$	24	28	$\neq 0$				

Отже, раціональними коренями многочлена $f(x)$ є

$$x_1 = \frac{1}{2}, \quad x_2 = -\frac{2}{3}, \quad x_3 = \frac{3}{4},$$

і можна розкласти многочлен $f(x)$ на незвідні над полем **Q** множники

$$f(x) = \left(x - \frac{1}{2}\right)\cdot\left(x + \frac{2}{3}\right)\cdot\left(x - \frac{3}{4}\right)\left(24x^2 + 24x + 24\right),$$

або

$$f(x) = (2x-1)\cdot(3x+2)\cdot(4x-3)\left(x^2 + x + 1\right).$$

Практичне заняття № 1

ГРУПИ. ПІДГРУПИ ГРУПИ. ГРУПИ ПІДСТАНОВОК

Основні поняття. *Група, підгрупа, циклічна група, порядок елемента, порядок групи, підстановка, група підстановок.*

Основні формули і теореми. *Критерій підгруп. Теорема Лагранжа та наслідки з неї.*

Результати навчання. Знати зміст основних понять, формул та теорем. **Вміти** визначати, чи є дана множина із заданою на ній операцією групою, чи є підмножина групи підгрупою даної групи. Знаходити порядок елемента групи.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Що називають *бінарною алгебраїчною операцією*? Наведіть приклади бінарних операцій, які є алгебраїчними, які не є алгебраїчними.
2. В якому випадку бінарну операцію називають *комутативною*? *асоціативною*? Наведіть приклад бінарної операції, яка є асоціативною, але некомутативною. Наведіть приклади неасоціативних операцій.
3. Що називають *нейтральним елементом* для бінарної алгебраїчної операції?
4. Який елемент називають *симетричним* для заданого?
5. Які способи знаходження оберненої матриці вам відомі?
6. Що називають *підстановкою* n-го степеня? Як виконати множення двох підстановок?
7. Де на комплексній площині розташовані корені 8-го степеня з 1?
8. Яку алгебраїчну структуру називають *групою*?
9. Виконання яких умов достатньо, щоб підмножина групи сама була групою?
10. Чим відрізняються поняття «*порядок елемента*» та «*порядок групи*»? В якому випадку ці два поняття визначаються одним числом?

План практичного заняття

1. Алгебраїчні операції, закони операцій. Група
   [10] — 26.1 (а, д), 9.7, 26.2 (б)
2. Групи підстановок. Таблиця Келі
   [10] — 26.5
3. Підгрупи групи. Циклічні групи. Теорема Лагранжа
   [10] — 26.18, 26.6, 26.7, 26.8, 26.17
4. Порядок елемента
   [10] — 26.25 (г,д)

   Додаткові завдання:
   [10] — 19.5, 19.6.

Домашнє завдання: [10] – 26.2, 26.3, 26.11, 26.12, 26,19, 26.26, побудувати таблицю Келі для групи самосуміщень квадрата

Практичне заняття № 2

КІЛЬЦЕ. ВІДНОШЕННЯ ПОДІЛЬНОСТІ

Основні поняття. *Кільце, підкільце, поле, підполе, область цілісності, відношення подільності елементів кільця, асоційовані елементи.*

Основні формули і теореми. *Властивості кілець. Критерій підкільця. Властивості подільності.*

Результати навчання. Знати зміст основних понять, формул та теорем. **Вміти** визначати, чи є дана множина кільцем, полем, чи є підмножина кільця підкільцем даного кільця. Встановлювати, чи є два елементи кільця асоційованими.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Яку алгебраїчну структуру називають *кільцем*? *полем*?
2. Виконання яких умов достатньо, щоб підмножина кільця сама була кільцем?
3. Які елементи кільця називають *дільниками одиниці*? *дільниками нуля*? Чи може елемент кільця бути одночасно дільником нуля і дільником одиниці?
4. За яких умов вважають, що один елемент кільця *ділиться* на інший? Наведіть приклади елементів, які перебувають у відношенні подільності в одному кільці і не перебувають у такому відношенні в іншому кільці.
5. Які елементи кільця називають *асоційованими*? Наведіть два способи встановлення, чи є елементи асоційованими.
6. Чи існують кільця, в яких неможливо означити поняття асоційованих елементів?

План практичного заняття

1. Кільце
   [11] — 7.1 (л, з), 7.4 (з), 7.5 (д)
   [10] — 9.4, 9.5
2. Подільність елементів кільця
   [11] — 7.8 (в)
3. Асоційовані елементи кільця
   [11] — 7.16 (г)

Домашнє завдання: [11] – 7.5 (в, є, к), 7.16 (д, е)

Практичне заняття № 3

ДІЛЕННЯ З ОСТАЧЕЮ В КІЛЬЦІ ЦІЛИХ ЧИСЕЛ

Основні поняття. *Неповна частка, остача. Евклідове кільце.*

Основні формули і теореми. *Властивості подільності. Теорема про ділення з остачею в кільці цілих чисел. Ознаки подільності.*

Результати навчання. Знати зміст основних понять, формул та теорем. **Вміти** визначати неповну частку та остачу при діленні будь-яких цілих чисел, застосовувати властивості подільності та ознаки подільності для доведення арифметичних задач.

Підготовку до практичного заняття слід розпочати з відповідей на питання:
1. Чи до будь-яких цілих чисел можна застосувати теорему про ділення з остачею?
2. Як визначити *неповну частку* та *остачу* для цілих чисел з різними знаками? для двох від'ємних цілих чисел?
3. Що називають *евклідовим кільцем*? які евклідові кільця вам відомі?
4. Перелічіть властивості подільності елементів кільця.
5. Як застосовують метод математичної індукції для доведення задач на подільність?
6. Сформулюйте ознаки подільності натурального числа на 4, на 8, на 9, на 11.

План практичного заняття
1. Теорема про ділення з остачею в кільці **Z**
   [11] — 1.1 (в, д, ж, г, е, є), 1.2 (а), 1.3 (а)
2. Подільність в кільці **Z**
   [11] — 1.5 (а, г), 1.6 (б, в), 1.10 (а, б)
3. Ознаки подільності натуральних чисел
   [11] — 19.4 (г, а), 19.5 (е, г, є)

Домашнє завдання: [11] – 1.2 (в, е), 1.3 (в, г, е), 1.8, 1.10, 1.12, 19.5 (а, в, ж)

Практичні заняття № 4, 5

НСД ЦІЛИХ ЧИСЕЛ

Основні поняття. *Найбільший спільний дільник елементів кільця, взаємно прості елементи кільця, найменше спільне кратне елементів кільця.*

Основні формули і теореми. *Алгоритм Евкліда. Лінійне представлення НСД елементів евклідового кільця. Ознака взаємно простих елементів. властивості взаємно простих елементів. Зв'язок між НСД та НСК двох елементів.*

Результати навчання. Знати зміст основних понять, формул та теорем. **Вміти** знаходити НСД цілих чисел за алгоритмом Евкліда та його лінійне представлення, застосовувати ознаку та властивості взаємно простих чисел.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Який елемент називають *спільним дільником* двох елементів кільця?
2. Що називають *найбільшим спільним дільником* двох елементів кільця?
3. Чи однозначно визначається НСД(a, b)?
4. Знайти НСД (24, -16), НСД (-24, -16).
5. Який алгоритм дозволяє визначити НСД двох елементів кільця? Чи можна користуватись ним в кільці цілих чисел, чому?
6. Який елемент називають *спільним кратним* двох елементів кільця?
7. Що називають *найменшим спільним кратним* двох елементів кільця?
8. Чому дорівнює НСК двох елементів кільця?
9. Знайти НСД (0, b), НСД (0, 0), НСК (0, b), НСК (0, 0), НСД (a, $a + b$).
10. Який вигляд має *лінійне представлення НСД* двох елементів кільця?
11. Які елементи кільця називають *взаємно простими*?
12. Перелічіть властивості взаємно простих елементів.

План практичних занять
Практичне заняття № 4

1. НСД цілих чисел. Алгоритм Евкліда
   [11] — 3.5 (в, а, б), 3.2 (а)
2. Лінійне представлення НСД цілих чисел
   [11] — 3.5 (в, а, б)

Домашнє завдання: [11] – 3.5 (е, є, ж, з)

Практичне заняття № 5

1. НСК цілих чисел
   [11] — 3.3 (ж)
2. Взаємно прості елементи
   [11] — 3.9 (а)
3. Задачі на НСД, НСК натуральних чисел
   [11] — 3.7 (б, в)

Домашнє завдання: [11] – 3.5 (ж, з) знайти НСК, 3.7 (г, е, ж)

Практичне заняття № 6

ЛАНЦЮГОВІ ДРОБИ

Основні поняття. *Скінченний ланцюговий дріб, підхідні дроби ланцюгового дробу.*

Основні формули і теореми. *Алгоритм Евкліда. Правило утворення підхідних дробів.*

Результати навчання. Знати зміст основних понять, формул та теорем. **Вміти** перетворювати звичайний дріб та квадратичну ірраціональність у ланцюговий дріб, застосовувати ланцюгові дроби при розв'язуванні арифметичних задач.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Який вигляд має скінченний ланцюговий дріб? нескінченний ланцюговий дріб?
2. Яким числом може бути початковий елемент ланцюгового дробу? Яким числом не може бути останній елемент скінченного ланцюгового дробу?
3. З якого алгоритму встановлюють ланки ланцюгового дробу при перетворенні у нього звичайного дробу $\frac{a}{b}$?
4. Що називають підхідним дробом k-го порядку?
5. Як можна визначити підхідні дроби ланцюгового дробу?
6. Які властивості мають підхідні дроби ланцюгового дробу?
7. Запишіть формулу розв'язків лінійного діофантового рівняння з двома невідомими.

План практичного заняття

1. Скінченні ланцюгові дроби
   [11] — 5.2 (е, к), 5.3 (є)
2. Нескінченні ланцюгові дроби
   [11] — 5.21 (е), 5.23 (є)
3. Підхідні дроби ланцюгового дробу
   [11] — 5.2 (е, к)
4. Лінійні діофантові рівняння
   [11] — 5.12 (б, в), 5.14

Домашнє завдання: [11] – 5.1 (б, д, є), 5.3 (а), , 5.21 (б, к), 5.23 (в), 5.16, 5.17

Практичне заняття № 7

ПРОСТІ ЕЛЕМЕНТИ КІЛЬЦЯ

Основні поняття. *Простий та складений елементи кільця, просте та складене число, канонічний запис числа, факторіальне кільце. Числові функції натурального числа.*

Основні формули і теореми. *Властивості простих елементів кільця. Властивості простих чисел. Теорема Евкліда про нескінченність множини простих чисел. Основна теорема арифметики. Формули обчислення числових функцій* $\tau(n)$, $\sigma(n)$, $\varphi(n)$.

Результати навчання. Знати зміст основних понять, формул та теорем. **Вміти** визначати чи є число простим, застосовувати властивості простих чисел при розв'язуванні арифметичних задач.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Який елемент кільця називають *простим*? *складеним*?
2. Перелічіть властивості простих елементів кільця.
3. Яким має бути кільце, щоб в ньому можна було визнати поняття «простий елемент»?
4. Що називають *простим числом*?
5. Чи існує натуральне число, яке не є ні простим, ні складеним?
6. Перелічіть властивості простих чисел.
7. Що називають канонічним записом елемента кільця? Чи однозначно він визначається?
8. Яке кільце називають факторіальним? Чи є кільце $\mathbf{Z}$ факторіальним?
9. Як можна визначити кількість натуральних дільників числа n?
10. Як можна визначити суму всіх натуральних дільників числа n?
11. Що визначає функція Ейлера для числа n?
12. Знайти $\tau(1)$, $\sigma(1)$, $\varphi(1)$, $\tau(p)$, $\sigma(p)$, $\varphi(p)$, де p – просте число.

План практичного заняття

1. Простий елемент області цілісності
   [11] —10.23, 10.22
2. Прості числа, їх властивості
   [11] — 2.1 (є)
3. Решето Ератосфена
   [11] — 2.2 (г)
4. Задачі теорії чисел
   [11] — 2.6 (д), 2.4 (а), 2.9 (а)
5. Числові функції $\tau(n)$, $\sigma(n)$, $\varphi(n)$
   [11] — 4.1 (в), 4.9 (д), 4.3 (г), 4.13 (е)

Домашнє завдання: виконати РГР (задачі 3 – 11)

Практичне заняття № 8

КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД ОДНІЄЇ ЗМІННОЇ

Основні поняття. *Многочлен від однієї змінної, кільце многочленів, канонічна форма і степінь многочлена, алгебраїчна рівність многочленів. Подільність многочленів, асоційовані многочлени, дільники одиниці в кільці многочленів, корінь многочлена.*

Основні формули і теореми. *Теорема про те, що кільце многочленів від однієї змінної над областю цілісності є областю цілісності. Степінь суми многочленів. Степінь добутку многочленів. Властивості подільності многочленів. Теорема Безу. Ознака кореня многочлена.*

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** виконувати операції додавання, множення та ділення з остачею многочленів в певному полі.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Який запис називають *канонічним представленням многочлена* $f(x)$?
2. Як виконати арифметичні дії додавання та множення двох многочленів? Запишіть загальну формулу для визначення коефіцієнтів многочлена $f(x) \cdot \varphi(x)$.
3. Що називають *коефіцієнтами* многочлена, *k-м членом многочлена*, *старшим членом* многочлена, *вільним членом* многочлена, *степенем* многочлена?
4. Сформулюйте означення алгебраїчної рівності многочленів.
5. Чи можна заздалегідь визначити степінь суми та добутку двох многочленів?
6. Чи є кільце многочленів $K[x]$ (де K – область цілісності) областю цілісності? Чи є кільце многочленів $P[x]$ (де P – поле) полем?
7. Чи можна ввести *відношення подільності* в кільці многочленів $K[x]$? Які властивості подільності із загальної теорії кілець можна перенести в $K[x]$?
8. Які многочлени називають *асоційованими*? Які елементи є дільниками одиниці в кільці $K[x]$?
9. Сформулюйте теорему та опишіть алгоритм ділення многочленів з остачею в кільці $P[x]$ (де P – поле).
10. Сформулюйте теорему Безу.
11. Сформулюйте ознаку кореня многочлена.

План практичного заняття

1. Многочлени над областю цілісності. Дії над ними.
   [12] — 577 (а, d) знайти суму та добуток многочленів,
2. Алгебраїчна рівність многочленів.
   [11] — 20.5 (а)
3. Кільце многочленів
   [11] — 20.15 (а, б, в)
4. Подільність многочленів.
   [11] — 21.6 (а)
5. Ділення з остачею.
   [11] — 21.12 (а)
6. Теорема Безу. Ознака кореня многочлена
   [11] — 22.13 (б), 22.20, 22.7
   Додаткові завдання:
   [11] — 21.2, 21.14-21.18, , 22.4, 22.5, 22.15, 22.8, 22.9
   [12] — 546, 547, 548,
   [13] — 555, 556, 558, 559, 579

Домашнє завдання: [11] — 23.5 виконати множення заданих многочленів, 21.12 (г), 20.15 (г,д,е), 21.16, 22.14, 22.17, 22.10, 20.22, 20.24

Практичне заняття № 9

СХЕМА ГОРНЕРА

Основні поняття. *Корінь, кратний корінь многочлена. Похідна многочлена.*

Основні формули і теореми. *Теорема Безу. Ознака кореня многочлена. Схема Горнера. Розклад многочлена за степенями лінійного двочлена. Формула значень похідних вищого порядку многочлена в точці.*

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** ділити многочлен на двочлен $x-a$ за схемою Горнера. Знаходити кратність кореня многочлена. Знаходити розклад многочлена за степенями двочлена $x-a$. Знаходити значення похідних вищого порядку многочлена при $x=a$.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Який степінь має многочлен–остача при діленні многочлена $f(x)$ на лінійний двочлен $x-c$?
2. Опишіть правило ділення многочлена $f(x)$ на лінійний двочлен $x-c$ за схемою Горнера.
3. Сформулюйте теорему Безу.
4. Де в схемі Горнера визначено значення $f(c)$?
5. Що називають *коренем многочлена* $f(x)$?
6. Сформулюйте ознаку кореня многочлена.
7. Як за схемою Горнера встановити, чи є число c коренем многочлена?
8. Що називають *k-кратним коренем многочлена* $f(x)$?
9. Як за схемою Горнера встановити, чи є число c 2-кратним, 3-кратним, …, k-кратним коренем многочлена?
10. Як за схемою Горнера знайти коефіцієнти в розкладі многочлена $f(x)$ за степенями $(x-c)$:
$$f(x)=r_n(x-c)^n+r_{n-1}(x-c)^{n-1}+r_{n-2}(x-c)^{n-2}+\ldots+r_2(x-c)^2+r_1(x-c)+r_0\,?$$
11. Як за схемою Горнера знайти значення похідних k-го порядку многочлена $f(x)$?

План практичного заняття

1. Задачі на схему Горнера:
   - ділення многочлена $f(x)$ на лінійний двочлен $x-c$;
     [12] — 549 (b, d),
   - знаходження $f(c)$,
     [12] — 554 (a, b),
   - знаходження кратності кореня $x_0=c$;
     [12] — 555 (a),
   - розклад $f(x)$ за степенями $(x-c)$
     [12] — 551, 552 (b)
   - знаходження значень похідних вищого порядку в точці

Додаткові завдання: [13] — 560, 561, 563, 564, 572.

Домашнє завдання: [11] – 22.2 (а, б), 22.3 (а,б), 25.15 (б), 25.12 (а, б)

Практичні заняття № 10, 11.

НСД МНОГОЧЛЕНІВ

Основні поняття. *Канонічна форма многочлена, степінь многочлена, найбільший спільний дільник та найменше спільне кратне двох многочленів*.

Основні формули і теореми. *Теорема про ділення з остачею в кільці многочленів над полем. Теорема про евклідовість кільця многочленів над полем. Теорема про лінійне представлення найбільшого спільного дільника двох многочленів*.

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** виконувати ділення з остачею многочленів в певному полі. Двома способами знаходити найбільший спільний дільник та найменше спільне кратне многочленів. Двома способами (за алгоритмом Евкліда та методом невизначених коефіцієнтів) знаходити лінійне представлення найбільшого спільного дільника двох многочленів.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Який многочлен називають *спільним дільником многочленів* $f(x)$ та $\varphi(x)$?
2. Що називають *найбільшим спільним дільником многочленів* $f(x)$ та $\varphi(x)$?
3. Чи однозначно визначається НСД($f(x)$, $\varphi(x)$)?
4. Чому дорівнює НСД многочленів:
$$f(x) = (3x+3)^5(x-2)^2(5x-5),$$
$$g(x) = (2x+2)^2(x-1)?$$
5. Які многочлени називають взаємно простими?
6. Чому дорівнює НСД (0, $\varphi(x)$), НСД ($f(x)$, $f(x)$), НСД (0, 0)?
7. Чому дорівнює НСД ($f(x)$, $2f(x)$), НСД ($f(x)$, $f(x)+g(x)$)?
8. Який алгоритм дозволяє визначити НСД двох елементів кільця? Чи можна користуватись ним в кільці многочленів $P[x]$, чому?
9. Який многочлен називають *спільним кратним многочленів* $f(x)$ та $\varphi(x)$?
10. Що називають *найменшим спільним кратним многочленів* $f(x)$ та $\varphi(x)$?
11. Чому дорівнює НСК многочленів:
$$f(x) = (3x+3)^5(x-2)^2(5x-5),$$
$$g(x) = (2x+2)^2(x-1)?$$
12. Як можна визначити *лінійне представлення НСД* двох многочленів?

План практичних занять
Практичне заняття№ 10

1. НСД двох многочленів.
   [11] — 23.3 (а, б)
2. НСД та НСК двох многочленів.
   [11] — 23.5 (а)
3. Алгоритм Евкліда. Взаємно прості многочлени.
   [12] — 577 (b,e, j)

Додаткові завдання:
[13] — 600, 613.

Домашнє завдання: [11] – 23.4, 23.5 (б, в), 23.6 (а, б), 21.20, 23.9

Практичне заняття№ 11

1. Лінійне представлення НСД (за допомогою алгоритму Евкліда).
   [12] — 578 (f), 579 (c)
   [13] — 601 (a)
2. Лінійне представлення НСД (методом невизначених коефіцієнтів).
   [12] — 579 (a)
   [13] — 607 (a)
3. Знаходження спільних коренів
   [13] — 613

Додаткові завдання: [13] — 601, 602, 606

Домашнє завдання: [12] – 578 (a, d), 579 (f), 580 (a,b)

Практичне заняття № 12

КОРЕНІ МНОГОЧЛЕНА. ФОРМУЛИ ВІЄТА

Основні поняття. *Корінь, кратний корінь многочлена, поле розкладу многочлена, алгебраїчно замкнене поле.*

Основні формули і теореми. *Ознака кореня многочлена. Теорема про найбільше можливе число коренів многочлена. Теорема Кронекера про існування кореня многочлена та наслідки з неї. Формули Вієта.*

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** застосовувати формули Вієта для дослідження рівнянь степеня $n > 2$.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Що називають *коренем многочлена*? *k-кратним коренем* многочлена?
2. Яку найбільшу кількість коренів може мати многочлен $f(x)$ степеня n?
3. Чи існує многочлен $f(x)$ степеня n, який має $n + 1$ коренів?
4. Чи існує многочлен $f(x) \in P[x]$ степеня n, який не має коренів в полі P?
5. Чи існує таке поле, в якому многочлен $f(x) \in P[x]$ степеня n, має хоча б один корінь?
6. Чи існує таке поле, яке містить всі корені многочлена $f(x) \in P[x]$ степеня n? Як називають таке поле?
7. Чи є поле **Q** полем розкладу многочлена $f(x) = x^2 - 5x + 4$?
8. Яке поле називають *алгебраїчно замкненим*? Назвіть такі поля.
9. Запишіть формули Вієта для многочлена
$$f(x) = 2x^3 + 4x^2 + 5x + 7.$$
10. Запишіть формули Вієта для многочлена
$$f(x) = 3x^4 + 11x^3 + 8x^2 + 6x + 10.$$

План практичного заняття

1. Поле розкладу многочлена.
   [11] — 31.3, 31.5
2. Формули Вієта
   [12] — 620
   [11] — 31.23, 31.13, 29.9
3. Застосування формул Вієта до задач шкільного курсу
   [11] — 28.6 (а, б, в), 28. 8 (а, б), 29.1 (а, е), 29.2 (а), 29.3 (г, в)

   Додаткові завдання:
   [11] — 29.7, 31.15, 31.19-31.22,
   [12] — 614-618, 699-702,
   [13] — 637-660, 664, 763-766, 768, 774, 776

Домашнє завдання: [11] — 31.17 (а), 31.18, 31.12, 31.15, 29.1 (в, є), 29.3 (г)

Практичне заняття № 13

МНОГОЧЛЕНИ НАД ПОЛЕМ C ТА R

Основні поняття. *Корінь многочлена, поле розкладу многочлена, незвідний над полем многочлен.*

Основні формули і теореми. *Лема про модуль старшого члена многочлена, наслідки з неї. Теорема Гаусса* («*Основна теорема алгебри*»). *Наслідок про розклад многочлена над полем комплексних чисел в добуток незвідних множників. Наслідок про спряжені комплексні корені многочлена з дійсними коефіцієнтами. Наслідок про розклад многочлена над полем дійсних чисел в добуток незвідних множників.*

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** знаходити межі комплексних і дійсних коренів многочлена. Розв'язувати алгебраїчні рівняння. Розкладати многочлени на незвідні над заданим полем множники.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Сформулюйте *Лему про модуль старшого члена многочлена* $f(x)$. Для яких значень змінної x вона справджується?
2. Чи можна встановити межі комплексних коренів многочлена $f(x)$?
3. Чи можна встановити межі дійсних коренів многочлена $f(x)$?
4. Чи може многочлен $f(x)$ з дійсними коефіцієнтами 5-го степеня не мати дійсних коренів?
5. Сформулюйте *теорему Гаусса*.
6. Чи існують незвідні над полем **C** многочлени 2-го степеня?
7. Яким є розклад многочлена на незвідні множники над полем **C**?
8. Чи може многочлен $f(x)$ з дійсними коефіцієнтами мати непарну кількість комплексних коренів?
9. Чи існують незвідні над полем **R** многочлени 2-го степеня?
10. Яким є розклад многочлена на незвідні множники над полем **R**?
11. Які алгебраїчно замкнені поля ви знаєте?
12. Чи є поле **Q**[$\sqrt{2}$] полем розкладу многочлена $f(x) = x^4 - 4$?

План практичного заняття.

1. Границі модулів коренів многочлена.
   [11] — 34.1 (а), 31.9 (а), 32.12, 32.13,
2. Звідні і незвідні многочлени над полем **C** і полем **R**.
   [11] — 31.10 (а, д)
3. Спряжені корені многочлена з дійсними коефіцієнтами.
   [11] — 32.1 (а), 31.11 (а), 32.6,

Додаткові завдання:
[12] — 589, 592,
[13] — 622-625.

Домашнє завдання: [11] — 34.1 (б, в), 31.9 (б), 32.1.(б,в), 32.2, 31.11 (б, в) (Розглянути випадки: 1) якщо $f(x) \in$ C[x], 2) якщо $f(x) \in$ R[x]),
[13] — 580

Практичні заняття № 14, 15.

РОЗВЯЗУВАННЯ АЛГЕБРАЇЧНИХ РІВНЯНЬ

Основні поняття. *Дискримінант кубічного рівняння, кубічна резольвента рівняння 4-го степеня, звідні та незвідні многочлени, канонічний розклад многочлена*.

Основні формули і теореми. *Формули Кардано. Теорема про розв'язки кубічного рівняння з дійсними коефіцієнтами в залежності від дискримінанта.*

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** розв'язувати рівняння третього та четвертого степенів. Розкладати многочлени на незвідні над заданим полем множники.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Як виконувати арифметичні операції над комплексними числами?
2. Як добути корінь n-го степеня з комплексного числа?
3. Для кубічних рівнянь якого виду застосовні *формули Кардано*?
4. У якому вигляді шукають розв'язок кубічного рівняння за формулами Кардано? Чи накладають додаткові умови на параметри цього розв'язку?
5. Що називають *дискримінантом кубічного рівняння*?
6. Запишіть формули коренів кубічного рівняння.
7. За яких умов кубічне рівняння з дійсними коефіцієнтами має один дійсний та два комплексні корені?
8. За яких умов кубічне рівняння з дійсними коефіцієнтами має три різні дійсні корені?
9. Чи може кубічне рівняння з дійсними коефіцієнтами мати подвійний дійсний корінь?
10. Поясніть етапи розв'язання рівняння 4-го степеня за *методом Феррарі*.
11. Що називають *кубічною резольвентою рівняння 4-го степеня*?
12. Який многочлен називають *звідним* над полем P?
13. Який многочлен називають *незвідним* над полем P?
14. Яким є розклад многочлена на незвідні множники над полем **C**?
15. Яким є розклад многочлена на незвідні множники над полем **R**?

План практичних занять

Практичне заняття № 14

1. Дії над комплексними числами
   [10] — 12.1, 12.9,
   [13] — 461. 462, 529
2. Розв'язування рівнянь 3-го степеня.
   [12] — 167 (с, е),
   [11] — 33.2 (г)
3. Дослідження рівнянь 3-го степеня.
   [11] — 31.16 (а), 33.3
4. Рівняння з комплексними коефіцієнтами
   [12] — 167 (р)

Додаткові завдання: [13] — 666, [11] — 33.6-33.8,

Домашнє завдання: [12] — 167 (b, l, m), [11] — 33.4, 33.5

Практичне заняття № 15

1. Рівняння 4-го степеня, метод Феррарі.
   [12] — 173(a, e, i)
2. Розклад многочленів на незвідні множники
   [12] — 173(a, e, i) розкласти на незвідні множники над полями **Q, R, C**.

Додаткові завдання: [13] — 669, 623 (i), [11] — 33.18, 32.10,

Домашнє завдання: [12] — 173(b, d, k) та розкласти на незвідні множники над полями **Q, R, C**.

Практичне заняття № 16

МНОГОЧЛЕНИ НАД ПОЛЕМ РАЦІОНАЛЬНИХ ЧИСЕЛ

Основні поняття. Корінь многочлена, незвідний над полем многочлен.

Основні формули і теореми. Критерій Ейзенштейна. Теореми про необхідні умови того, щоб нескоротний раціональний дріб, був коренем многочлена з цілими коефіцієнтами.

Результати навчання. . Знати зміст основних понять, формул та теорем. **Вміти** досліджувати на незвідність многочлени над полем **Q**. Знаходити раціональні корені многочленів з цілими коефіцієнтами.

Підготовку до практичного заняття слід розпочати з відповідей на питання:

1. Чи є примітивним многочлен
$$f(x) = 2x^4 - 7x^3 + 12x^2 - 9\,?$$
2. Чи може многочлен $f(x)$ бути незвідним над **Z**, але звідним над **Q**?
3. Сформулюйте Критерій Ейзенштейна.
4. Чи є незвідним над полем **Q** многочлен
$$f(x) = 2x^4 - 6x^3 + 9x^2 - 15x + 12\,?$$
5. Чи існують незвідні над полем **Q** многочлени 12-го степеня?
6. Сформулюйте першу необхідну умову раціонального кореня многочлена.
7. Сформулюйте другу необхідну умову раціонального кореня многочлена.
8. Чи може многочлен $f(x)$ мати дробовий корінь:
$$f(x) = x^4 - 6x^3 + 9x^2 - 15x + 4\,?$$
9. Чи є правильним твердження: «Многочлен третього степеня звідний над полем Q тоді й тільки тоді, коли один з його коренів є раціональним числом»?

План практичного заняття

1. Звідні і незвідні многочлени над полем **Q**, кільцем **Z**.
   [12] — 653 (а)
2. Цілі і раціональні корені многочлена з раціональними коефіцієнтами.
   [12] — 650 (d, b, h),
   [11] — 24.11, 35.1 (б, г) та розкласти на незвідні над Q
   [12] — 651

Додаткові завдання: [11] — 35.2-35.7, [13] — 675, 678, 680

Домашнє завдання: [12] — 653 (б), 650 (g, i, k) та розкласти на незвідні над Q ,
[11] — 35.4 (а)

Зауваження: в цій темі не використовувати формули Кардано та метод Феррарі.

РОЗРАХУНКОВА РОБОТА

1. Перевірити, чи є множина A групою відносно операції $*$, якщо:

1.1. A – множина всіх матриць другого порядку з цілими елементами, визначник яких дорівнює одиниці, $*$ – множення.

1.2. A – множина всіх матриць виду $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, де a, b – дійсні числа, що одночасно не дорівнюють нулю, $*$ – множення.

1.3. A – множина всіх матриць виду $\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$, де a, b – раціональні числа, що одночасно не дорівнюють нулю, $*$ – множення.

1.4. A – множина всіх матриць виду $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, де $a, b \in \mathbf{Q}$, $ab \neq 0$, $*$ – множення.

1.5. A – множина всіх матриць виду $\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}$, де $a, b, c \in \mathbf{Q}$, $a \neq 0$, $*$ – множення.

1.6. A – сукупність підмножин універсальної множини $\boldsymbol{U}$, $*$ – перетин множин.

1.7. A – сукупність підмножин універсальної множини $\boldsymbol{U}$, $*$ – об'єднання множин.

1.8. A – множина всіх раціональних чисел, в яких знаменник ділиться на 3, $*$ – множення.

1.9. A – множина чисел виду $a - b\sqrt{7}$, де a і b – довільні раціональні числа, що одночасно не дорівнюють нулю, $*$ – множення.

1.10. A – множина чисел виду $a + b\sqrt[3]{2}$, де $a \neq 0$, a і b – довільні дійсні числа, $*$ – множення.

1.11. A – множина многочленів другого степеня $ax^2 + bx + c$, де a, b, c – раціональні числа, $*$ – додавання.

1.12. A – множина чисел виду $lg\ a$, де a – довільне дійсне додатне число, $*$ – додавання.

1.13. $A = \{0, 1, 2, 3\}$, операція $*$ задається за правилом $a * b$ є остача від ділення добутку ab на 4.

1.14. $A = \{0, 1, 2, 3\}$, операція $*$ задається за правилом $a * b$ є остача від ділення суми $a + b$ на 4.

1.15. A – множина всіх комплексних чисел, модуль яких дорівнює 1, $*$ – множення.

2. Перевірити, чи утворює кільце (поле) множина A, якщо:

2.1. A – множина всіх многочленів $f(x)$ від однієї змінної з цілими коефіцієнтами, в яких змінна x має тільки парний степінь.

2.2. A – множина всіх многочленів $f(x)$ від однієї змінної з цілими коефіцієнтами, в яких змінна x має тільки непарний степінь.

2.3. A – множина всіх многочленів $f(x)$ від однієї змінної з цілими коефіцієнтами, які не містять вільного члена.

2.4. A – множина всіх многочленів $f(x)$ від однієї змінної з цілими коефіцієнтами, степінь яких не перевищує числа 10.

2.5. A – множина всіх многочленів $f(x)$ від однієї змінної з цілими коефіцієнтами, в яких вільний член є парним числом.

2.6. A – множина всіх многочленів $f(x)$ від однієї змінної з цілими коефіцієнтами, степінь яких не менший числа 2.

2.7. A – множина чисел виду $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, де a, b, c – довільні раціональні числа.

2.8. A – множина чисел виду $u\sqrt[3]{3} + v$, де u, v – довільні раціональні числа.

2.9. $\mathcal{A}$ – множина всіх підмножин деякої множини M, якщо операції додавання і множення задано так:

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

$$A \cdot B = A \cap B, \qquad A, B \in \mathcal{A}.$$

2.10. A – множина всіх матриць виду $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, де a, b – цілі числа.

2.11. A – множина всіх матриць виду $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, де a, b – раціональні числа, що одночасно не дорівнюють нулю.

2.12. A – множина всіх матриць виду $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, де a, b – раціональні числа.

2.13. A – множина всіх матриць виду $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, де a, b – раціональні числа, $ab \neq 0$.

2.14. A – множина всіх матриць виду $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, де a, b – раціональні числа.

2.15. A – множина всіх матриць виду $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, де a, b – раціональні числа

3. Замінити букви такими цифрами, щоб

3.1. $\overline{22mk1} \vdots 99$.

3.2. $\overline{1992ab} \vdots 72$.

3.3. $\overline{88x5y} \vdots 36$.

3.4. $\overline{1cd44} \vdots 33$.

3.5. $\overline{364rs2} \vdots 88$.

3.6. $\overline{x1998y} \vdots 99$.

3.7. $\overline{15a12b} \vdots 33$.

3.8. $\overline{234cd} \vdots 44$.

3.9. $\overline{2x35y6} \vdots 72$.

3.10. $\overline{3a7k9} \vdots 99$.

3.11. $\overline{154ab} \vdots 72$.

3.12. $\overline{40x6y} \vdots 36$.

3.13. $\overline{70cd5} \vdots 33$.

3.14. $\overline{x026y3} \vdots 99$.

3.15. $\overline{5a12b8} \vdots 66$

4. Простим чи складеним є число:

4.1. 3367.

4.2. 3691.

4.3. 6233.

4.4. 4021.

4.5. 9703.

4.6. 4883.

4.7. 6493.

4.8. 3629.

4.9. 6191.

4.10. 5017.

4.11. 6613.

4.12. 3989.

4.13. 5543.

4.14. 3347.

4.15. 2831.

5. Застосувавши Решето Ератосфена знайти всі прості числа, які містяться між числами:

5.1. 1300 і 1350.

5.2. 1350 і 1400.

5.3. 1400 і 1450.

5.4. 1450 і 1500.

5.5. 1500 і 1550.

5.6. 1550 і 1600.

5.7. 1600 і 1650.

5.8. 1650 і 1700.

5.9. 1700 і 1750.

5.10. 1750 і 1800.

5.11. 1800 і 1850.

5.12. 1850 і 1900.

5.13. 1900 і 1950.

5.14. 1950 і 2000.

5.15. 2000 і 2050.

6. Знайти таке просте число *p*, щоб простими були також числа:

6.1. $2p^2 + 1$.

6.2. $p + 10$ і $p + 14$.

6.3. $p^2 + 8$.

6.4. $8p^2 + 1$ і $8p^2 + 2p + 1$.

6.5. $2p + 1$ і $4p + 1$.

6.6. $p^2 - 6$ і $p^2 + 6$.

6.7. $2p^2 - 9$ і $2p^2 + 9$.

Довести, що одночасно простими не можуть бути такі числа:

6.8. p, $p + 2$ і $p + 5$.

6.9. $7k$, $7k + 4$ і $7k + 5$.

6.10. $2^n - 1$ і $2^n + 1$, де $n > 2$.

6.11. Довести, що з усіх цілих чисел виду $2p + 1$, де p – просте число, тільки одне є точним кубом.

6.12. Нехай p – просте число і $p > 5$. Довести, що p^2 при діленні на 30 дає остачу 1 або 19.

6.13. Довести, що якщо p – просте число і $p \geq 5$, то

$$(p^2 - 1) \,\vdots\, 24.$$

6.14. Довести, що якщо p, q – прості числа, більші від 3, то

$$(p^2 - q^2) \,\vdots\, 24.$$

6.15. Чи є простим число $n^8 + n^4 + 1$ $(n \in \mathbf{N},\ n > 1)$?

7. Знайти значення числових функцій $\tau(n)$, $\sigma(n)$, $\varphi(n)$ для числа n:

7.1. 22968. 7.2. 38675. 7.3. 1638.

7.4. 48951. 7.5. 11385. 7.6. 224224.

7.7. 9975. 7.8. 180063. 7.9. 27027.

7.10. 27104. 7.11. 16660. 7.12. 11286.

7.13. 5096. 7.14. 33534. 7.15. 51425.

8. Знайти натуральне число n, якщо:

8.1. $\tau(n) = 1$, 2 або 3 відповідно.

8.2. $\tau(n) = 4$, 5 або 6 відповідно.

8.3. n має тільки два простих дільники, $\tau(n) = 12$, $\sigma(n) = 1240$.

8.4. $n \,\vdots\, 12$ і $\tau(n) = 14$.

8.5. n – найменше натуральне число, для якого $\tau(n) = 14$.

8.6. n – найменше натуральне число, для якого $\tau(n) = 18$.

8.7. n – найменше натуральне число, для якого $\tau(n) = 100$.

8.8. n – найменше натуральне число виду $2^x p_1 p_2$, де p_1, p_2 – різні непарні прості числа і $\sigma(n) = 3n$.

8.9. $n = 2^x \cdot 5^y \cdot 7^z$ $(x, y, z \in \mathbf{N})$, $\tau(5n) = \tau(n) + 8$, $\tau(7n) = \tau(n) + 12$, $\tau(8n) = \tau(n) + 18$.

8.10. Нехай $n \in \mathbf{N}$. Знайти $\tau(n^3)$, якщо $\tau(n^2) = 15$ і n має тільки два простих дільники.

8.11. $n = 3^x \cdot 5^y \cdot 7^z$ $(x, y, z \in \mathbf{N})$ і $\varphi(n) = 3600$.

8.12. $n = pq$, де p, q – різні прості числа такі, що $p - q = 2$ і $\varphi(n) = 120$.

8.13. $n = p^2 q^2$, де p, q – різні прості числа, і $\varphi(n) = 11424$.

8.14. Довести, що $\tau(n)$ непарне тоді і тільки тоді, коли n – квадрат натурального числа.

8.15. Довести, що $\varphi(n)$ – парне число при $n \geq 3$.

9. Розкласти в ланцюговий дріб:

9.1. а) $-\dfrac{324}{1173}$, б) $\dfrac{\sqrt{7}+2}{2}$.

9.2. а) $\dfrac{1527}{2314}$, б) $\dfrac{\sqrt{7}-2}{3}$.

9.3. а) $\dfrac{2115}{8412}$, б) $\dfrac{\sqrt{15}-2}{3}$.

9.4. а) $-\dfrac{1843}{1125}$, б) $\dfrac{\sqrt{15}+4}{7}$.

9.5. а) $-\dfrac{7316}{234}$, б) $\dfrac{\sqrt{33}-4}{5}$.

9.6. а) $\dfrac{856}{1123}$, б) $\dfrac{\sqrt{33}+2}{3}$.

9.7. а) $\dfrac{734}{2517}$, б) $5-\sqrt{15}$.

9.8. а) $-\dfrac{8164}{1512}$, б) $\dfrac{6-\sqrt{3}}{2}$.

9.9. а) $\dfrac{2513}{956}$, б) $\dfrac{5\sqrt{13}-13}{3}$.

9.10. а) $\dfrac{4848}{731}$, б) $\dfrac{\sqrt{101}-1}{4}$.

9.11. а) $-\dfrac{2354}{4318}$, б) $\dfrac{3+\sqrt{37}}{4}$.

9.12. а) $\dfrac{1745}{843}$, б) $\sqrt{71}$.

9.13. а) $\dfrac{2125}{6342}$, б) $\sqrt{47}$.

9.14. а) $\dfrac{1713}{875}$, б) $\dfrac{8-\sqrt{3}}{3}$.

9.15. а) $\dfrac{4116}{6315}$, б) $\dfrac{\sqrt{13}}{2}$.

10. Знайти квадратичну ірраціональність α, якщо α розкладається в такий ланцюговий дріб:

10.1. [3; (1, 1, 4)] .

10.2. [2; 1, 2, (1, 1, 5)] .

10.3. [6; 1, (2, 1, 3)] .

10.4. [1; (1, 2, 11)] .

10.5. [2; (3, 1, 4)] .

10.6. [3; 1, 7, (2, 3)] .

10.7. [5; 1, 1, (2, 3, 4)] .

10.8. [5; 12, 3, (2, 0, 1)] .

10.9 [0; 1, 5, 6, (2, 8)] .

10.10. [1; (2, 3, 4)].

10.11. [1; 2, (3,4)].

10.12. [9; 2, (1, 4, 3)] .

10.13. [1; 2, (1, 1, 2, 2)] .

10.14. [15; 2, 0, (1, 1, 3)] .

10.15. [8; (2, 3, 5)] .

11. Розв'язати лінійне діофантове рівняння

11.1. $91x-28y=35$.

11.2. $23x+15y=19$.

11.3. $50x-42y=34$.

11.4. $47x-105y=4$.

11.5. $47x-111y=89$.

11.6. Відгадати день народження, якщо сума добутків числа місяця на 12 і номера місяця на 31 дорівнює 339.

11.7. Для перевезення зерна є мішки по 60 і 80 кг. Скільки таких мішків потрібно для перевезення 440 кг зерна?

11.8. На будівництво газопроводу на трасу завдовжки 283 м було доставлено труби, довжина яких 5 і 7 м. Скільки труб доставили?

11.9. Скільки квитків по 30 і 50 грн. можна купити на 1490 грн?

11.10. Один майстер робить на довгому полотні мітку синім олівцем від краю через кожні 36 см. Інший – мітку червоним олівцем від краю через кожні 25 см. Чи може синя мітка опинитися на відстані1 см від деякої червоної?

11.11. Студенту необхідно розв'язати 20 завдань. За кожне правильно розв'язане завдання він отримає 8 балів, за неправильно розв'язане – мінус 5 балів, за завдання, яке він не розпочинав – 0 балів. Студент отримав 13 балів. Скільки завдань він спробував розв'язати?

11.12. Купили 30 птахів за 30 монет однієї вартості: за кожних трьох горобців заплатили 1 монету, за кожні дві горлиці також 1 монету і за кожного голуба по – 2 монети. Скільки купили птахів кожного виду?

11.13. 26 студентів посадили разом 88 дерев, причому кожен студент I, II та III курсу повинен був посадити відповідно 6, 4 та 2 дерева. Скільки було студентів I, II та III курсів?

11.14. Скільки точок з цілими координатами лежать на прямій $31x-47y=23$ між прямими $x=-50$ та $x=23$?

11.15. Скільки точок з цілими координатами лежать на прямій $101x-39y=89$ між прямими $x=0$ та $x=100$?

12. Знайти лінійне представлення найбільшого спільного дільника (НСД) многочленів

12.1. $f(x)=x^5-5x^4-2x^3+12x^2-2x+12,$

$\varphi(x)=x^3-5x^2-3x+17.$

12.2. $f(x)=3x^4-5x^3+4x^2-2x+1,$

$\varphi(x)=3x^3-2x^2+x-1.$

12.3. $f(x)=x^5+5x^4+9x^3+7x^2+5x+3,$

$\varphi(x)=3x^3-2x^2+x-1.$

12.4. $f(x)=x^6-4x^5+11x^4-27x^3+37x^2-35x+35,$

$\varphi(x)=3x^3-2x^2+x-1.$

12.5. $f(x)=3x^7+6x^6-3x^5+4x^4+14x^3-6x^2-4x+4,$

$\varphi(x)=3x^6-3x^4+7x^3-6x+2.$

12.6. $f(x)=3x^5+5x^4-16x^3-6x^2-5x-6,$

$\varphi(x)=3x^4-4x^3-x^2-x-2.$

12.7. $f(x)=4x^4-2x^3-16x^2+5x+9,$

$\varphi(x)=2x^3-x^2-5x+4.$

12.8. $f(x)=x^5-5x^4-2x^3+12x^2-2x+12,$

$\varphi(x)=x^3-5x^2-3x+17.$

12.9. $f(x)=3x^4-5x^3+4x^2-2x+1,$

$\varphi(x)=3x^3-2x^2+x-1.$

12.10. $f(x)=x^5+5x^4+9x^3+7x^2+5x+3,$

$\varphi(x)=3x^3-2x^2+x-1.$

12.11. $f(x)=x^6-4x^5+11x^4-27x^3+37x^2-35x+35,$

$\varphi(x)=3x^3-2x^2+x-1.$

12.12. $f(x)=3x^7+6x^6-3x^5+4x^4+14x^3-6x^2-4x+4,$

$\varphi(x)=3x^6-3x^4+7x^3-6x+2.$

12.13. $f(x)=3x^5+5x^4-16x^3-6x^2-5x-6,$

$\varphi(x)=3x^4-4x^3-x^2-x-2.$

12.14. $f(x)=4x^4-2x^3-16x^2+5x+9,$

$\varphi(x)=2x^3-x^2-5x+4.$

13. Застосовуючи формули Вієта, розв'язати задачу:

13.1. Знайти коефіцієнти a, b рівняння

$$x^4 + x^3 - 18x^2 + ax + b = 0,$$

якщо відомо, що серед його коренів є три однакові цілі числа.

13.2. Знайти коефіцієнти p, q рівняння

$$x^4 - 10x^3 + 37x^2 + px + q = 0,$$

якщо відомо, що серед його коренів є дві пари рівних між собою чисел.

13.3. Для рівняння

$$x^3 + ax^2 + bx + 1 = 0$$

добуток суми його коренів на суму їх обернених величин виразити через коефіцієнти a і b.

13.4. Показати, що рівність $ab = c$ виражає необхідну й достатню умову того, що серед коренів рівняння

$$x^3 + ax^2 + bx + c = 0$$

є два числа, сума яких дорівнює нулю.

13.5. Розв'язати рівняння

$$12x^3 + 4x^2 - 17x + 6 = 0,$$

якщо відомо, що серед його коренів є два числа, обернені за абсолютною величиною і протилежні за знаком.

13.6. Квадратне рівняння

$$ax^2 + bx + c = 0$$

має два кореня. Скласти нове квадратне рівняння, у якого один з коренів на одиницю менше більшого кореня, а інший на одиницю більше меншого кореня даного рівняння.

13.7. Записати рівняння третього степеня за його коренями x_1^2, x_1x_2, x_2^2, якщо числа x_1 та x_2 є коренями рівняння

$$x^2 + px + q = 0.$$

13.8. При якому додатному значенні p корені рівняння

$$2x^2 - (p+2)x + 7 = p^2$$

є оберненими за величиною та протилежними за знаком? Знайти ці корені.

13.9. Визначити, при яких значеннях m один з коренів рівняння

$$x^3 - (m^2 - m + 7)x - (3m^2 - 3m - 6) = 0$$

дорівнює – 1. Знайти два інших кореня відповідно до цих значень m.

13.10. Розв’язати рівняння

$$x^3 - 3\sqrt{3}x^2 + 7x - \sqrt{3} = 0,$$

якщо відомо, що один з його коренів відрізняється від деякого іншого кореня на $\sqrt{2}$.

13.11. Розв’язати рівняння

$$8x^3 + 4x^2 - 34x + 15 = 0,$$

якщо відомо, що два з його коренів x_1 та x_2 задовольняють співвідношення

$$2x_1 - 4x_2 = 1.$$

13.12. Скласти рівняння четвертого степеня з коренями $x_1, x_2, \frac{1}{x_1}, \frac{1}{x_2}$, якщо x_1 та x_2 – корені рівняння

$$ax^2 + bx + c = 0 \quad (c \neq 0).$$

13.13. Розв’язати рівняння

$$x^4 - 6x^3 + 7x^2 + 6x - 2 = 0,$$

якщо відомо, що воно має принаймні одну пару коренів, різниця між якими дорівнює 1.

13.14. Розв’язати рівняння

$$3x^3 + 2\sqrt{3}x^2 - 21x + 6\sqrt{3} = 0,$$

якщо відомо, що добуток двох його коренів дорівнює 1.

13.15. Знайти коефіцієнти рівняння

$$x^2 + px + q = 0$$

за умови, що різниця коренів рівняння дорівнює 5, а різниця їх кубів дорівнює 35.

14. Розв'язати систему рівнянь:

14.1.

$$\begin{cases} \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}=3, \\ \dfrac{1}{xy}+\dfrac{1}{yz}+\dfrac{1}{zx}=3, \\ \dfrac{1}{xyz}=1. \end{cases}$$

14.2.

$$\begin{cases} \sqrt{\dfrac{x}{y}}+\sqrt{\dfrac{y}{z}}+\sqrt{\dfrac{z}{x}}=3, \\ \sqrt{\dfrac{y}{x}}+\sqrt{\dfrac{z}{y}}+\sqrt{\dfrac{x}{z}}=3, \\ \sqrt{xyz}=1. \end{cases}$$

14.3.

$$\begin{cases} \sqrt[4]{x}+\sqrt[4]{y}=3, \\ x+y=17 \end{cases}$$

14.4

$$\begin{cases} (u^2+v^2)(u+v)=15uv, \\ (u^4+v^4)(u^2+v^2)=85u^2v^2. \end{cases}$$

14.5.

$$\begin{cases} 9(u^4+v^4)=17(u+v)^2, \\ 3uv=-2(u+v). \end{cases}$$

14.6

$$\begin{cases} x^2+y^2-x-y=102, \\ xy+x+y=69. \end{cases}$$

14.7.

$$\begin{cases} x^3+x^3y^3+y^3=17, \\ x+xy+y=5. \end{cases}$$

14.8

$$\begin{cases} x^3+y^3=19, \\ (xy+8)(x+y)=2. \end{cases}$$

14.9.

$$\begin{cases} \dfrac{1}{x^2+y^2}+2xy=\dfrac{21}{5}, \\ \dfrac{1}{2xy}+x^2+y^2=\dfrac{21}{4}. \end{cases}$$

14.10

$$\begin{cases} x+y+z=6, \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}=1{,}5, \\ xyz=8. \end{cases}$$

14.11.

$$\begin{cases} x^4+6x^2y^2+y^4=136, \\ x^3y+xy^3=30. \end{cases}$$

14.12

$$\begin{cases} 10(x^4+y^4)=-17(x^3y+xy^3), \\ x^2+y^2=5. \end{cases}$$

14.13.

$$\begin{cases} x\sqrt{y}+y\sqrt{x}=30, \\ x\sqrt{x}+y\sqrt{y}=35. \end{cases}$$

14.14

$$\begin{cases} x^4+x^2y^2+y^4=91, \\ x^2+xy+y^2=13. \end{cases}$$

14.15.

$$\begin{cases} x^3+y^3=19, \\ x^2y+xy^2=-6. \end{cases}$$

Питання, що виносяться на екзамен

1. Поняття групи. Найпростіші властивості груп.
2. Групи підстановок. Групи самосуміщень ромба, трикутника, квадрата.
3. Кільце. Найпростіші властивості кільця.
4. Поле. Приклади числових полів (**Q**, **R**, **C**).
5. Дільники нуля та одиниці в кільці. Область цілісності.
6. Подільність в комутативному кільці. Властивості подільності.
7. Асоційовані елементи в області цілісності.
8. Теорема про ділення з остачею в кільці цілих чисел.
9. Евклідове кільце. Чи є кільце цілих чисел евклідовим ?
10. НСД елементів області цілісності. Лінійне представлення НСД елементів кільця.
11. Взаємно прості елементи. Ознака взаємної простоти. Властивості взаємно простих елементів.
12. Алгоритм Евкліда для знаходження НСД елементів кільця.
13. НСК елементів евклідового кільця.
14. Прості елементи кільця, їх властивості.
15. Прості числа, їх властивості.
16. Нескінченність множини простих чисел. Решето Ератосфена.
17. Канонічний запис чисел. Знаходження НСД, НСК двох чисел, записаних в канонічному вигляді.
18. Числові функції $\tau(n)$, $\sigma(n)$, функція Ейлера. Формули для їх обчислення.
19. Ознаки подільності на 2, 4, 8, 3, 9, 11.
20. Ланцюгові дроби. Перетворення звичайного дробу у ланцюговий.
21. Підхідні дроби ланцюгового дробу.
22. Кільце многочленів К[x] від однієї змінної над областю цілісності К.
23. Подільність в кільці многочленів К[x] (К – область цілісності).
24. Дільники одиниці в К[x].
25. Теорема про ділення з остачею в кільці многочленів Р[x], де Р – поле. Наслідок.
26. Чи є кільце многочленів Р[x] (Р – поле) евклідовим?
27. Теорема Безу.
28. Означення і ознака кореня многочлена $f(x) \in$ Р[x] (Р – поле). Кратні корені многочлена.
29. Схема Горнера.
30. Розклад многочлена $f(x)$ за степенями лінійного двочлена $x - c$.
31. НСД елементів кільця Р[x] (Р – поле). Його лінійне представлення.
32. Взаємно прості многочлени від однієї змінної, їх властивості.
33. НСК двох многочленів від однієї змінної.
34. Похідна многочлена. Критерій кратного кореня многочлена.

35. Звідні і незвідні над полем P многочлени від однієї змінної. Властивості незвідних многочленів. Канонічний розклад многочлена з P[x].
36. Теорема про найбільшу можливу кількість коренів многочлена з P[x] (P – поле). Поле розкладу многочлена $f(x)$. Алгебраїчно замкнені поля.
37. Формули Вієта для многочлена f(x) степеня n.
38. Лема про модуль старшого члена многочлена $f(x) \in \mathbf{C}[x]$.
39. Границі модулів коренів многочлена $f(x)$.
40. Існування дійсного кореня многочлена $f(x)$ непарного степеня з дійсними коефіцієнтами.
41. Існування кореня многочлена $f(x)$ з числовими коефіцієнтами (теорема Гаусса).
42. Наслідок з теореми Гаусса про незвідні многочлени над полем **C**. Канонічний розклад многочлена $f(x)$ над полем **C**.
43. Наслідок з теореми Гаусса про спряжені корені многочлена $f(x)$ з дійсними коефіцієнтами.
44. Наслідок з теореми Гаусса про незвідні многочлени над полем **R**. Канонічний розклад многочлена $f(x)$ над полем **R**.
45. Рівняння третього степеня з одним невідомим. Виведення і аналіз формули Кардано.
46. Дослідження рівняння третього степеня з дійсними коефіцієнтами за дискримінантом.
47. Розв’язування рівняння четвертого степеня з одним невідомим методом Феррарі.
48. Властивості многочленів від однієї змінної з раціональними коефіцієнтами. Звідність многочленів від однієї змінної над полем **Q** і кільцем **Z**.
49. Критерій незвідності многочленів від однієї змінної над полем **Q**.
50. Цілі і раціональні корені многочлена $f(x)$ з цілими коефіцієнтами.

Інформаційні джерела для вивчення курсу

1. Завало С.Т. Курс алгебри. – К.: Вища шк., 1985. – 503 с.
2. Завало С.Т., Костарчук В.Н., Хацет Б.І. Алгебра і теорія чисел: В 2-х ч. – К.: Вища шк., 1976. – Ч.2. 384 с.
3. Курош А.Г. Курс высшей алгебры. – М.: Наука, 1971. – 432 с.
4. Куликов Л.Я. Алгебра и теория чисел. – М.: Высш. шк., 1979. – 559 с.
5. Фаддеев Д.К. Лекции по алгебре. – М.: Наука, 1984. – 416 с.
6. Бородін О.І. Теорія чисел. – К.: Вища шк., 1970. – 274 с.
7. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 176 с.
8. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с.
9. Михелович Ш.Х. Теория чисел. – М.: Высш. шк., 1967. – 336 с.
10. Завало С.Т., Левіщенко С.С., Пилаєв В.В., Рокицький І.О. Алгебра і теорія чисел. Практикум: В 2-х ч. – К.: Вища шк., 1983. – Ч.1. – 232 с.
11. Завало С.Т., Левіщенко С.С., Пилаєв В.В., Рокицький І.О. Алгебра і теорія чисел. Практикум: В 2-х ч. – К.: Вища шк., 1985. – Ч.2. 264 с.
12. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. – М.: Наука, 1977. – 288 с.
13. Окунев Л.Я. Сборник задач по высшей алгебре. – М.: Просвещение, 1964. – 185 с.

Інформаційні ресурси:

www.moodle.udu.edu.ua Алгебра і теорія чисел (4 Ф) Верпатова Н.Ю.

ЗМІСТ

ВИДАВНИЦТВО
УКРАЇНСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
імені Михайла Драгоманова

Віддруковано з оригіналів.

Видавництво Українського державного університету
імені Михайла Драгоманова.
01601, м. Київ-30, вул. Пирогова, 9
Свідоцтво про реєстрацію ДК 7896 від 25.07.2023.
(044) 239-30-26.