Міністерство освіти і науки України
Глухівський національний педагогічний університет
імені Олександра Довженка

О. В. Заїка, Л. Ф. Сухойваненко, Т. О. Прокопець

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

Навчальний посібник

Суми – 2023

УДК 512 (075.8)
А45

Рекомендовано до друку Вченою радою
Глухівського національного педагогічного університету
імені Олександра Довженка
(протокол № 4 від 26 жовтня2022 року)

Автори:

О.В. Заїка, кандидат педагогічних наук, доцент кафедри фізико-математичної освіти та інформатики ГНПУ імені Олександра Довженка.

Л.Ф. Сухойваненко, кандидат педагогічних наук, старший викладач кафедри фізико-математичної освіти та інформатики ГНПУ імені Олександра Довженка.

Т.О. Прокопець, викладач ВСП «Глухівський агротехнічний фаховий коледж Сумського НАУ».

Рецензенти:

Н.В. Кугай, доктор педагогічних наук, доцент кафедри фізико-математичної освіти та інформатики Глухівського національного педагогічного університету імені Олександра Довженка.

Г.В. Гоменюк, кандидат педагогічних наук, в.о. завідувача кафедри математики та методики її навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка.

Заїка О. В., Сухойваненко Л.Ф. , Прокопець Т.О.

А45 Алгебра і теорія чисел : навчальний посібник / О. В. Заїка, Л.Ф. Сухойваненко, Т.О. Прокопець. – Глухів: ФОП Цьома С.П., 2023. – 264 с.

У навчальному посібнику розглянуті теоретичні основи освітнього компоненту «Алгебра і теорія чисел», приклади розв’язування типових задач курсу, підібрані завдання для проведення аудиторних занять, а також для самостійної підготовки здобувачів освіти. Посібник рекомендується для студентів спеціальності 014.04 Середня освіта (Математика), 014.09 Середня освіта (Інформатика) усіх форм навчання.

УДК 512 (075.8)

ЗМІСТ

ПЕРЕДМОВА

Мета створення даного навчального посібника – допомогти студентам у засвоєнні освітнього компоненту «Алгебра і теорія чисел».

Предметом вивчення освітнього компоненту «Алгебра і теорія чисел» є основні алгебраїчні структури (кільця, групи, поля), теорія конгруенцій, теорія многочленів.

Метою вивчення є: оволодіння майбутніми вчителями теоретико-множинною і логічною символікою, основними поняттями алгебри і теорії чисел (алгебраїчна операція, група, кільце, поле, прості числа, подільність, конгруенції, многочлени); формування чіткого уявлення про основні арифметичні застосування теорії конгруенції та основні властивості многочленів над полем комплексних, дійсних і раціональних чисел.

У посібнику розглянуто дванадцять тем із трьох модулів: алгебраїчні структури (теми один-три); теорія конгруенції (теми чотири і п’ять); теорія многочленів (теми шість – дванадцять).

Фундаментальними поняттями освітнього компоненту є: подільність, ділене, дільник, частка, остача, спільне і найменше спільне кратне, спільний і найбільший спільний дільник, взаємно прості числа, число просте і складене, канонічна форма натурального числа, числові та мультиплікативні числові функції, конгруентні числа, конгруенція, клас лишків, лишок, повна і зведена система лишків, лінійна конгруенція, розв’язок конгруенції, рівносильні конгруенції, конгруенція n-ого степеня за простим модулем, порядок числа та первісний корінь за даним модулем, ознака подільності, група, підгрупа, кільце, підкільце, поле, підполе, відображення, гомоморфізм, ізоморфізм, одиниця кільця, дільник нуля і одиниці, область цілісності, характеристика кільця, подільність у комутативному кільці, ідеал і головний ідеал кільця, конгруенція за ідеалом, клас лишків кільця за ідеалом, фактор-кільце, НСД і НСК двох елементів області цілісності, многочлен степеня n, корінь многочлена,

кратність кореня, незвідний многочлен, раціональний дріб правильний і неправильний, елементарні дроби.

Фундаментальними фактами є: властивості відношення подільності, теорема про ділення цілих чисел з остачею, теореми про існування та єдиність НСД та НСК двох цілих чисел, зв'язок між НСД і НСК двох цілих чисел, методи знаходження НСД і НСК цілих чисел, властивості простих і складених чисел, основна теорема арифметики, решето Ератосфена, властивості мультиплікативних функцій, властивості конгруенцій, теорема про існування та кількість розв’язків лінійної конгруенції, способи розв’язування лінійних конгруенцій (спосіб спроб, спосіб рівносильних перетворень, спосіб Ейлера, застосування класів лишків), теорема про кількість розв’язків конгруенції за простим модулем, властивості порядків за модулем, теорема про кількість класів первісних коренів за простим модулем (теорема Гауса), ознака Паскаля, ознаки подільності на 2, 5, 3, 9, 11, 4, 25, 50, критерій групи (підгрупи), критерій кільця (підкільця), критерій поля (підполя), теорема про зв’язок поля і області цілісності, властивості характеристики кільця, властивості відношення подільності у комутативному кільці, теорема про ідеали в кільці цілих чисел, властивості конгруенції за ідеалом, теорема про зв’язок між класами лишків кільця цілих чисел за ідеалом і класами лишків кільця цілих чисел за модулем, основна теорема про гомоморфізми кілець, основна теорема алгебри, формули Вієта, теорема про розклад правильного раціонального дробу на суму елементарних, теорема Штурма.

Фундаментальними відношеннями: відношення подільності, алгебраїчні операції як відношення, гомоморфізм, ізоморфізм, конгруентності, асоційованості.

У посібнику для кожної теми подаються теоретичні відомості (що розкривають зазначені вище фундаментальні поняття, факти та відношення), які супроводжуються прикладами розв’язування типових завдань. До кожної теми підібрано задачі для самостійного розв’язування.

Тема перша
ГРУПИ І ПІДГРУПИ

Групи

Означення. *Непорожня множина G елементів a, b, c,... називається групою, якщо в цій множині*:

1) *визначена операція* «$\circ$», *яка ставить у відповідність кожній парі елементів* (a,b) *з* G *деякий елемент* c *з* G (*в позначеннях* $a \circ b = c$);
2) *операція* «$\circ$» *асоціативна, тобто* $a\circ(b\circ c)=(a\circ b)\circ c$ *для будь-яких* a, b, c *з* G;
3) *існує елемент* $e \in G$, *нейтральний відносно операції* «$\circ$», *тобто такий, що* $a\circ e=e\circ a=a$ *для будь-якого* $a \in G$;
4) *для будь-якого елемента* $a \in G$ *існує такий елемент* $a' \in G$, *що* $a\circ a'=a'\circ a=e$ *елемент* a' *називають оберненим елементу* a.

Елемент ***e*** називають одиничним елементом або одиницею групи G; іноді одиничний елемент позначають також символом 1.

Алгебра розглядає множини, на яких між елементами визначені певні відношення, які називають *алгебраїчними операціями*. З прикладами алгебраїчних операцій ви зустрічалися ще в шкільному курсі математики, а також під час вивчення інших розділів вищої математики. До алгебраїчних операцій відносимо, наприклад, додавання і множення чисел, многочленів, додавання векторів площини, додавання матриць, об'єднання та переріз множин, додавання і множення функцій, композиція відображень тощо. Якщо ці операції виконуються над парами елементів однієї і тієї ж множини (наприклад, над парами чисел, многочленів, векторів, функцій), то їх називають *бінарними алгебраїчними операціями* або просто *бінарними операціями*.

Алгебраїчну операцію, визначену в групі, називають множенням або додаванням. Групу відносно операції множення називають *мультиплікативною,* а відносно операції додавання – *адитивною.*

Умовимося розглядати далі в основному мультиплікативні групи.

***Означення**. Непорожня множина G, в якій визначена операція множення, називається групою, якщо виконуються такі умови:*

1. *Операція множення асоціативна.*
2. *Для операції множення в множині G здійсненна обернена операція – ділення, тобто для будь-яких елементів a і b множини G кожне з рівнянь ax=b і ya = b має у множині G розв'язок і притому тільки один.*

Якщо операція множення, визначена в групі *G*, комутативна, то група *G* називається *комутативною* або *абельовою.*

Введені означення групи є еквівалентними.

Група *G* називається *скінченною,* якщо множина її елементів скінченна; вона називається *нескінченною,* якщо множина її елементів нескінченна.

Кількість елементів скінченної групи називають *порядком групи.*

З означення групи випливають такі наслідки.

1. *У кожній групі G можна виконувати лівосторонні і правосторонні скорочення: якщо $ab_1 = ab_2$ або $b_1a = b_2a$, то $b_1=b_2$.*
2. *У кожній групі G для будь-якого її елемента a існує єдиний обернений йому елемент a^{-1}, тобто такий, що $a^{-1}a = aa^{-1}=e$.*
3. *Які б не були цілі числа m і n, для кожного елемента a групи G справджуються рівності:*

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

Прикладами мультиплікативних груп є множина всіх додатних раціональних чисел, всіх відмінних від нуля раціональних чисел, множина всіх додатних дійсних чисел, всіх відмінних від нуля дійсних чисел, множина всіх відмінних від нуля комплексних чисел. Усі ці групи – нескінченні, абельові. Прикладом мультиплікативної нескінченної некомутативної групи є множина неособливих матриць *n*-го порядку над полем комплексних чисел *C*. Множина всіх комплексних коренів *n*-го степеня з 1 є мультиплікативною абельовою групою порядку *n.*

Підстановки

Важливими прикладами скінченних некомутативних груп є групи підстановок.

Нехай дано деяку множину *M,* що складається з *n* елементів. Елементи цієї множини можна перенумерувати за допомогою чисел 1, 2, 3, ... *n.* Індивідуальні властивості елементів множини *M* далі не відіграватимуть ніякої ролі, тому ми просто вважатимемо, що множина *M* складається з чисел 1, 2, 3, ..., *n.*

Означення*. Всяке розташування чисел* 1, 2, ..., *n в деякому певному порядку називається перестановкою з n чисел або з n елементів.*

Кількість різних перестановок з *n* елементів дорівнює $n! = 1 \cdot 2 \ldots n$. Прийнято вважати, що в перестановці $i_1, i_2, \ldots, i_k, \ldots, i_s, \ldots, i_n$ елементи i_k й i_s, утворюють *інверсію*, якщо $i_k > i_s$, але i_k стоїть у перестановці лівіше від i_s.

Перестановку, елементи якої утворюють парну кількість інверсій, називають *парною,* а перестановку, елементи якої утворюють непарну кількість інверсій, називають *непарною.*

Перетворення перестановки, при якому деякі два її елементи міняються місцями, а решта елементів залишаються нерухомими, називають *транспозицією.*

Як відомо, *кожна транспозиція змінює парність перестановки.*

Теорема. *При n≥2 кількість парних перестановок з n елементів дорівнює кількості непарних, тобто дорівнює* $0{,}5n!$

Відомо також, що від кожної перестановки з *n* елементів можна перейти до будь-якої іншої перестановки з цих самих елементів за допомогою кількох транспозицій.

Означення. *Всяке взаємно однозначне відображення множини* $M = \{1, 2, 3, \ldots. n\}$ *самої на себе називають підстановкою з n елементів або підстановкою n-го степеня*.

Підстановки позначатимемо великими буквами латинського алфавіту: *A, B, C* та ін.

Якщо при підстановці *A* число i ($i = 1, 2, \ldots, n$) відображається в число a_i, то записують

$$A = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \qquad (1.1)$$

тобто під кожним з чисел 1, 2, 3 ... *n* підписують те число, в яке воно відображається, і одержані два рядки беруть у дужки.

Запис (1.1) слід читати так: «при підстановці *A* 1 переходить в a_1, 2 переходить в a_2, ..., *n* переходить в a_n».

Оскільки підстановка є *взаємно однозначним відображенням,* то всі числа $a_1, a_2, ..., a_n$ різні і, отже, другий рядок у записі (1.1) являє собою деяку перестановку з елементів 1, 2, 3 .... *n.*

Слід зауважити, що стовпчики в записі (1.1) можна поміняти місцями, тобто у верхньому рядку замість перестановки 1, 2, 3, ..., *n* можна записати будь-яку іншу перестановку $b_1, b_2, ..., b_n$ з елементів 1, 2, 3, ..., *n* і потім у нижньому рядку числа a_1 ($a_2, a_3, ..., a_n$) переставити так, щоб під числом *i* (*i* =1, 2, 3, ..., *n*) стояло число a_i. У результаті одержимо запис тієї самої підстановки, але вже іншого вигляду. Наприклад,

$$\begin{pmatrix} 3 & 1 & 2 & 4 & 5 & 6 & \dots & n \\ a_3 & a_1 & a_2 & a_4 & a_5 & a_6 & \dots & a_n \end{pmatrix}$$

$$\begin{pmatrix} 3 & 4 & 5 & \dots & n & 1 & & n \\ a_3 & a_4 & a_5 & \dots & a_n & a_1 & & a_n \end{pmatrix}$$

$$\begin{pmatrix} n & n-1 & n-2 & \dots & 3 & 2 & & 1 \\ a_n & a_{n-1} & a_{n-2} & \dots & a_3 & a_2 & & a_1 \end{pmatrix}$$

є різні записи однієї і тієї самої підстановки $A = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, оскільки в кожному з них число *i* (*i* =1, 2, 3, ..., *n*) переходить в число a_i.

Отже, будь-яку підстановку *n-го* степеня можна записати за допомогою двох перестановок з чисел 1, 2, 3, ..., *n,* підписаних одна під одною:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

причому верхню перестановку $a_1, a_2, a_3, ..., a_n$ завжди можна вибрати довільно.

Навпаки, якщо під деякою перестановкою c_1, c_2, c_3... c_n з чисел 1, 2, 3, ..., n ми підпишемо будь-яку іншу перестановку d_1, d_2, ..., d_n з цих самих чисел, то отримуємо запис

$$\begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

деякої підстановки *n-го* степеня – підстановки, при якій число c_i (i = 1, 2, 3, ... n) переходить у число d_i.

Кожна підстановка *n-го* степеня звичайно може бути записана у вигляді (1.1). При такому записі підстановок різні підстановки *n-го* степеня відрізнятимуться одна від одної нижніми перестановками. Звідси випливає справедливість такого твердження.

***Теорема**. Кількість підстановок n-го степеня дорівнює n!*

***Означення.** Підстановка А називається парною, якщо парності верхньої й нижньої перестановок довільного запису її збігаються; вона називається непарною, якщо парності цих перестановок протилежні.* Рівносильним цьому означенню є таке означення.

***Означення**. Підстановка А називається парною, якщо сумарна кількість інверсій у верхній і нижній перестановках довільного запису її парне, в протилежному разі вона називається непарною.*

***Теорема.** При n ≥ 2 кількість парних підстановок n-го степеня дорівнює кількості непарних, тобто дорівнює 0,5n!*

Приклад. Визначити парність підстановки 6-го степеня

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

Розв'язання. У верхній перестановці цього запису 5 інверсій, а в нижній їх 11. Загальна кількість інверсій в обох перестановках – 16. Отже, підстановка *A* є парна. Запишемо тепер розглядувану підстановку так:

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

У верхній перестановці цього запису 0 інверсій, а в нижній – 8. Загальна кількість інверсій – 8. Цей приклад показує, що при різних записах даної підстановки парність загального числа інверсій в обох перестановках запису її зберігається, а сама кількість інверсій, взагалі кажучи, змінюється.

Групи підстановок

Візьмемо дві довільні підстановки *n-го* степеня

$$A = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, B = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}.$$

Виконаємо послідовно підстановки *A* і *B.* У результаті цього отримуємо підстановку

$$C = \begin{pmatrix} 1 & 2 & \dots & n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}.$$

Означення. *Підстановку C, що є результатом послідовного виконання підстановок A і B, називають добутком підстановки A на підстановку B і записують: C =* ***AB.***

Наприклад, якщо

$$\mathrm{A} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$

$$\mathrm{A}B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Справді, підстановка *A* відображає 1 в 2, а підстановка *B* відображає 2 в 4. Отже, *AB* відображає 1 в 4. Аналогічно відображаються й інші символи.

Операція множення підстановок n-го степеня при n≥3 некомутативна.

Справді, для підстановок

$$A\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \dots & n \\ 2 & 3 & 1 & i_4 & i_5 \dots & i_n \end{pmatrix},$$

$$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ 3 & 2 & 1 & j_4 & j_5 & \dots & j_n \end{pmatrix}$$

AB ≠ BA, оскільки підстановка *AB* відображає елемент 1 в 2, а підстановка *BA* відображає 1 в 1.

Операція множення підстановок асоціативна: (*AB*)*C* = = *A*(*BC*).

Теорема. *Множина всіх підстановок n-го степеня є група за множенням.*

Для кожної підстановки $A = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ в множині підстановок *n-го* степеня існує підстановка $A^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$, така, що $AA^{-1} = A^{-1}A = E$.

Підстановку A^{-1} називають *оберненою* для підстановки *A.*

Означення. *Групу всіх підстановок n-го степеня називають симетричною групою n-го степеня і позначають* S_n. *Порядок групи* S_n *дорівнює n*!

Теорема. *Кожну підстановку n-го степеня можна подати у вигляді добутку кількох транспозицій.* Умовимося позначати транспозицію символом **(*ij*).**

Кожну підстановку можна різними способами записати у вигляді добутку транспозицій, бо завжди до даного добутку транспозицій можна дописати, наприклад, дві транспозиції виду (*i, j*) (*i, j*), добуток яких дорівнює тотожній підстановці *E.*

Теорема. *У всіх записах даної підстановки у вигляді добутку транспозицій парність числа транспозицій буде та сама*: *вона збігається з парністю підстановки.*

Теорема. *Множина всіх парних підстановок n-го степеня є група по множенню.*

Означення. *Групу парних підстановок називають знакозмінною групою n-го степеня. Порядок цієї групи дорівнює 0,5n*!

Знакозмінна група *n*-го степеня при *n*=3 *комутативна*, а при *n*≥4 – *некомутативна*.

Підгрупи

Нехай дано групу *G* і деяку підмножину *H* цієї групи. Підмножину *H* називають *підгрупою* групи *G,* якщо вона є

групою відносно бінарної операції, визначеної в *G.*

Теорема. *Для того щоб підмножина H групи G була підгрупою цієї групи, необхідно й достатньо, щоб вона разом з будь-якими своїми елементами a і b містила й їх добуток ab і разом з кожним своїм елементом a містила також і обернений йому елемент* a^{-1}.

Кожна мультиплікативна група *G,* очевидно, має такі тривіальні підгрупи: саму групу *G* і так звану одиничну підгрупу, яка складається лише з одиничного елемента 1. Але, звичайно, в групі можуть бути й інші підгрупи. Так, група за множенням, що складається з 1 і мінус 1, і мультиплікативна група додатних раціональних чисел *Q+* є підгрупами мультиплікативної групи всіх відмінних від нуля раціональних чисел. Мультиплікативна група відмінних від нуля раціональних чисел є підгрупою групи всіх відмінних від нуля дійсних чисел. Знакозмінна група *n*-го степеня є підгрупою симетричної групи *n-го* степеня. Множина всіх матриць *n*-го порядку над числовим полем *P* детермінант кожної з яких дорівнює 1, є мультиплікативна група: її називають *унімодулярною групою матриць.* Унімодулярна група матриць є підгрупою мультиплікативної групи всіх невироджених матриць *n*-го порядку над полем *P.*

Важливим прикладом підгруп *є так* звані *циклічні підгрупи*. Нехай *G* – деяка група і *a* – довільний елемент цієї групи. Позначимо символом {*a*} підмножину групи *G,* що складається з усіх степенів елемента *a.* Підмножина {*a*} *є підгрупою групи G,* оскільки:

1. Добуток будь-яких двох елементів a^m і a^n з {*a*} міститься в {*a*}, оскільки $a^m \cdot a^n = a^n \cdot a^m = a^{m+n}$.
2. В {*a*} міститься також елемент $1 = a^0$.
3. Разом з усяким своїм елементом a^n підмножина {*a*} містить і обернений йому елемент a^{-n}.

Означення. *Підгрупа* {*a*}, *що складається з усіх степенів елемента a, називається циклічною підгрупою групи G, породженою елементом a.*

Зауважимо, що можуть бути такі два випадки: 1) усі степені елемента *a* є різні елементи групи *G*; в цьому разі *a* називають *елементом нескінченного порядку;* 2) серед

степенів елемента a є рівні між собою, наприклад $a^l=a^s$, де $s\neq l$. Це завжди буде так, якщо група G скінченна, але може трапитися й у нескінченній групі. Розглянемо другий випадок докладніше. Отже, припустимо, що $a^1=a^s$, де $s>l$. Тоді $a^{s-l}=1$, тобто існують додатні степені елемента a, які дорівнюють 1. Нехай серед усіх додатних степенів елемента a, які дорівнюють 1, n є найменший, тобто

1) $a^n = 1$, $n>0$;
2) якщо $a^l = 1$, $l > 0$, то $l>n$.

У цьому разі елемент a називають *елементом* скінченного порядку, а саме *порядку n.*

Якщо a є елемент *n-го* порядку, то породжена ним циклічна підгрупа $\{a\}$ складається з таких елементів:

$1, a, a^2, a^3,..., a^{n-2}, a^{n-1}$.

Порядок циклічної підгрупи $\{a\}$ дорівнює порядку елемента a, що породжує цю підгрупу.

Зауважимо, що в кожній групі G є єдиний елемент першого порядку – це 1. Циклічна підгрупа {1} збігається з одиничною підгрупою.

Теорема. *Якщо H і P є підгрупи групи G, то їх перетин $H\cap P$ також є підгрупа цієї групи.*

Циклічні групи

Означення. Група G називається циклічною, якщо вона складається зі степенів одного з своїх елементів a, тобто збігається з однією зі своїх циклічних підгруп $\{a\}$.

Елемент a називають *твірним елементом* циклічної групи $\{a\}$. Кожна циклічна група абельова, бо $a^m a^n = a^n a^m = a^{m+n}$.

Приклади циклічних груп.

1. Адитивна група цілих чисел є нескінченна циклічна група, її твірним елементом є число 1. За твірний елементі цієї групи, можна взяти також число мінус -1.
2. Мультиплікативна група коренів *n-го* степеня з 1 є циклічною групою порядку *n.*

Теорема. *Кожна нескінченна циклічна група ізоморфна адитивній групі цілих чисел*.

***Теорема**. Кожна циклічна група порядку n ізоморфна мультиплікативній групі коренів n-го степеня з* 1.

З теорем випливає, що адитивною групою цілих чисел і мультиплікативною групою коренів *n*-го степеня з 1 по суті вичерпуються всі циклічні групи.

***Теорема**. Кожна підгрупа циклічної групи сама циклічна.*

***Теорема**. Кожна підгрупа скінченної циклічної групи $G=<a>$ порядку n породжується елементом a^s, де s – дільник числа n, і є циклічною групою порядку t, причому n = st.*

***Теорема.** У циклічної групи порядку n є стільки підгруп, скільки є дільників у числа n.*

Розклад групи за підгрупою

Нехай дано групу *G* та підмножини *M* і *N* цієї групи. *Сукупність усіх елементів групи G, кожен з яких можна записати у вигляді добутку деякого елемента з множини M на деякий елемент з множини N, називатимемо добутком множини M на множину N і позначатимемо його символом MN.*

Звичайно, одна з множин *M* і *N* може складатися лише з одного елемента. Якщо, наприклад, множина *M* складається з елемента *a,* то мова йтиме про добуток *aN* елемента *a* на множину *N.*

З асоціативності множення в групі *G* випливає асоціативність множення підмножин цієї групи: $(MN)P = M(NP)$.

Зауважимо, що *коли Q є підгрупа групи G, то* $Q \cdot Q = Q$. Нехай *H* – довільно вибрана підгрупа групи *G.* Використавши підгрупу *H,* введемо на множині елементів *a, b, c, ...* групи *G* бінарне відношення ρ, вважаючи, що $a\rho b \leftrightarrow a^{-1}b \in H$, або, що те саме, $a\rho b \leftrightarrow b=ah$, де *h* - деякий елемент підгрупи *H,* ρ є відношення еквівалентності.

Будь-яке відношення еквівалентності, задане на множині *M,* визначає розбиття цієї множини на класи еквівалентних елементів, які не перетинаються. Отже, і відношення еквівалентності ρ визначає розбиття групи *G* на класи еквівалентних елементів.

З'ясуємо, що являють собою ці класи розбиття. Якщо *H=G,* то розбиття складається лише з одного класу. Якщо

$H=E=\{e\}$, то відношення еквівалентності є звичайна рівність, і тому кожен елемент групи G становить клас розбиття. Припустимо тепер, що H – підгрупа, відмінна від E і від G. Нехай B_i – один з класів розбиття групи G, яке матимемо при цьому, і нехай g – довільний елемент класу B_i. Тоді кожен елемент $b=gh$, де h – будь-який елемент з H, належить до B_i, оскільки $g\rho b$, і, навпаки, якщо $b \in B_i$, то $g\rho b$, тому $b=gh$, $h \in H$. Отже, $B_i=gH$. Отже, кожен клас розбиття групи G, що визначається відношенням еквівалентності ρ, коли EHG є добуток gH довільно вибраного елемента g цього класу на підгрупу H. Ці класи розбиття називають *лівими суміжними класами групи G за підгрупою H,* а саме розбиття називають *лівостороннім розкладом* групи G за підгрупою H. Про суміжний клас $B_i=gH$ говорять, що він породжується елементом g.

Елемент g довільно вибраний в суміжному класі B_i. Отже, суміжний клас $B_i = gH$ породжується будь-яким із своїх елементів і тому будь-який з елементів класу gH можна взяти за *представника* цього класу. Зауважимо, що одним із лівих суміжних класів є сама підгрупа H. Цей суміжний клас породжується одиничним елементом $\boldsymbol{e}$, а також будь-яким іншим елементом h з H, оскільки $hH=H$. Його позначають не $\boldsymbol{e}H$ або hH, а просто H.

Якщо група G скінченна, то лівосторонній розклад групи G за підгрупою H записують так:

$$G = H + g_1H + g_2H + \ldots + g_{s-1}H = \sum_{i=1}^{s-1} g_i\, H + H$$

де знаки + і $\sum$ означають об'єднання множин, що не перетинаються, тобто лівих суміжних класів. На множині елементів групи G можна було б ввести відношення еквівалентності ρ': $a\rho' b \leftrightarrow ba^{-1} \in H$, тобто $a\rho' b \leftrightarrow b=ha$, $h \in H$.

Правий суміжний клас Hg групи G за підгрупою H, породжений елементом g, правосторонній розклад скінченної групи G за підгрупою H записують так:

$$G = H + Hg_1 + Hg_2 + \ldots + Hg_{s-1} = \sum_{i=1}^{s-1} Hg_i + H.$$

Цілком природно постає питання: лівосторонній і правосторонній розклади групи G за підгрупою H – це різні розбиття групи G на підмножини чи те саме розбиття? Інакше кажучи, відношення еквівалентності ρ і ρ' – це різні відношення чи те саме бінарне відношення?

Для абельової групи G лівосторонній і правосторонній розклади за будь-якою підгрупою H збігаються, для неабельової ж групи розклади за однією підгрупою можуть збігатися, а за іншою – можуть виявитися різними.

Для скінченних груп істинне таке твердження.

***Теорема Лагранжа**. У кожній скінченній групі порядок будь-якої її підгрупи є дільником порядку групи.*

З теореми Лагранжа випливають такі наслідки:

***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 циклічна група.*

Нормальні дільники

***Означення**. Підгрупа H групи G називається нормальним дільником цієї групи або інваріантною підгрупою, якщо лівосторонній і правосторонній розклади групи G за підгрупою H збігаються.*

Лівосторонній і правосторонній розклади групи G за підгрупою H збігатимуться, очевидно, тоді і тільки тоді, коли лівий суміжний клас gH групи G за підгрупою H, породжений будь-яким елементом $g \in G$, збігатиметься з її правим суміжним класом Hg, що містить елемент g. Тому поняття нормального дільника можна означити так**.**

***Означення.** Підгрупа H групи G називається нормальним дільником цієї групи, якщо для будь-якого $g \in G$ $gH=Hg$.*

Остання умова означає, що для будь-якого $g \in G$ будь-якого $h \in H$, існують $h' \in H$, $h'' \in H$ такі, що $gh=h'$ і $hg=h''$.

Приклади нормальних дільників груп. 1. У будь-якій групі G сама група G і одинична підгрупа E є її нормальними дільниками: лівосторонній і правосторонній розклади групи G за підгрупою G складаються з одного суміжного класу G, а лівосторонній і правосторонній розклади групи

за підгрупою E складаються з усіх елементів групи G.

2. У кожній абельовій групі G будь-яка її підгрупа H є нормальним дільником, оскільки для будь-якого елемента g групи G $gH=Hg$. Зокрема, мультиплікативна група додатних дійсних чисел є нормальним дільником мультиплікативної групи всіх відмінних від нуля дійсних чисел; мультиплікативна група відмінних від нуля раціональних чисел є нормальним дільником мультиплікативної групи відмінних від нуля дійсних чисел.

Теорема. *Підгрупа H групи G є її нормальним дільником тоді і тільки тоді, коли $h \in H \to g^{-1}hg \in H$.*

Елементи a і b групи G називають *спряженими* в цій групі, якщо в G існує принаймні один такий елемент g, що $b= g^{-1}hg$.

Означення. *Підгрупа H групи G називається нормальним дільником цієї групи, якщо вона разом з кожним своїм елементом b, містить і всі елементи, спряжені з ним в G.*

Теорема. *Перетин будь-якої множини нормальних дільників групи G є нормальним дільником цієї групи.*

Фактор-групи

Нехай H – довільний нормальний дільник групи G. Оскільки кожен лівий суміжний клас gH групи G за нормальним дільником H є одночасно і правим суміжним класом Hg і навпаки, то далі ми говоритимемо просто про суміжні класи групи G за нормальним дільником H. Суміжний клас gH, породжений елементом g, позначатимемо $\overline{g}$. Виходячи з поняття добутку підмножин групи, означимо в множині суміжних класів групи G за нормальним дільником H операцію множення.

Нехай $\overline{g}_1 = g_1H$ і $\overline{g}_2 = g_2H$ – два довільні суміжні класи групи G за нормальним дільником H. Розглянемо добуток $\overline{g_1} \cdot \overline{g_2} = g_1Hg_2H$ цих суміжних класів як підмножин групи G. Оскільки множення підмножин асоціативне й $H \cdot H = H$, то

$$\overline{g}_1 \cdot \overline{g_2} = g_1H \cdot g_2H = (g_1Hg_2) \cdot H = (g_1 \cdot (g_2H)) \cdot H =$$
$$= (g_1 \cdot g_2)(H \cdot H) = g_1g_2H = \overline{g_1g_2}.$$

Тобто $\overline{g}_1 \cdot \overline{g_2} = \overline{g_1g_2}$.

Отже, *добуток двох суміжних класів групи G за нормальним дільником H як підмножин групи G є суміжним класом G за H.* Цим у множині суміжних класів групи G за нормальним дільником H визначена операція множення.

Остання рівність показує, що для відшукання добутку двох даних суміжних класів групи G за нормальним дільником H потрібно в кожному з цих класів вибрати по одному представнику і потім взяти той суміжний клас, до якого належить добуток вибраних представників.

***Теорема**. Множина суміжних класів групи G за нормальним дільником H з визначеною в ній операцією множення є група. Вона називається фактор-групою групи G за нормальним дільником H і позначається G/H.*

Встановимо деякі найпростіші властивості фактор-груп.

***Теорема**. Кожна фактор-група G/H абельової групи G також абельова.*

***Теорема.** Кожна фактор-група G/H циклічної групи G також циклічна.*

***Теорема.** Порядок будь-якої фактор-групи G/H скінченної групи G є дільником порядку цієї групи.*

Гомоморфізм груп

З поняттям гомоморфізму груп, як можна пересвідчитися далі, тісно пов'язані поняття нормального дільника групи і фактор-групи.

***Означення**. Ізоморфізм φ групи G на групу G′ – це взаємно однозначне відображення G на G′, що не порушує множення: для будь-яких елементів a, b ∈ G* $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Якщо не вимагати, щоб відображення було взаємно однозначним, а лише зберігало операцію множення, то ми приходимо до поняття гомоморфного відображення групи G в (або на) групу G'.

***Означення**. Гомоморфізмом, або гомоморфним відображенням, φ групи G в групу G′ називають відображення групи G в групу G′, яке задовольняє умову: для будь-яких елементів a, b ∈ G* $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Якщо групи G і G' – адитивні, то умову гомоморфізму можна записати так: *для будь-яких елементів* $a, b \in G$ $\varphi(a+b) = \varphi(a) + \varphi(b)$.

Якщо гомоморфне відображення $\varphi : G \to G'$ є відображенням групи G **на** групу G', то його називають *гомоморфізмом групи G на групу G'* або *епіморфізмом групи G.* В цьому разі говорять, що група G є *гомоморфним образом* групи G' і пишуть $G \sim G'$.

Щоб зазначити, що φ є гомоморфізм групи G на групу G', пишуть $\varphi : G \sim G'$.

Гомоморфізм φ відображення групи G на фактор-групу G/H називається *природним або канонічним* гомоморфізмом.

Теорема. *При гомоморфному відображені φ групи G в групу G' одиничний елемент* ***e*** *групи G відображається в одиничний елемент* ***e'*** *групи G'.*

Теорема*. Якщо φ - гомоморфізм групи G в групу* ***G'****, то* $\varphi(g^{-1}) = (\varphi(g))^{-1}$*, для* $g \in G$.

Теорема. *Якщо φ є гомоморфізм групи G в групу G', то* $\varphi(G)$ *є підгрупа групи G'.*

Означення. *Нехай φ є гомоморфне відображення групи G в групу G'. Сукупність K всіх елементів групи G, які при гомоморфізмі φ відображаються в одиницю* ***e'*** *групи G, називають ядром гомоморфізму φ і записують K= Ker φ.*

Теорема. *Ядро будь-якого гомоморфізму φ групи G є нормальним дільником групи G.*

Зауважимо, що ядром ($Ker\,\varphi$) природного гомоморфізма групи G на фактор-групу G/H є нормальний дільник H.

Теорема про гомоморфізми груп. *Нехай φ є гомоморфізм групи G на групу G' і H = Ker φ. Тоді група G ізоморфна фактор-групі G/H, причому існує такий ізоморфізм ψ фактор-групи G/H на групу G', що добуток χψ природного гомоморфізму χ : G~G/H на ізоморфізм* ψ є *гомоморфізм φ.*

Теорема Келі. *Нехай G – скінченна група порядку n. Тоді група G ізоморфна деякій підгрупі симетричної групи* S_n.

Теорема про гомоморфізми показує, що всі групи, на які може гомоморфно відображатися група G, по суті вичерпуються її фактор-групами, а всі гомоморфізми групи

G вичерпуються природними гомоморфізмами G на її фактор-групи.

Приклади розв'язування типових завдань

№1. *Множина з двох елементів* $M=\{a,b\}$ *з операцією, заданою таблицею* (*таблицею Келі*) *утворює групу* $(M,\circ)$. *Який елемент в цій групі є нейтральним?*

$\circ$	a	b
a	a	b
b	b	a

Розв'язання. Оскільки M – є групою, то її елементи задовольняють аксіоми групи. Проаналізуємо таблицю Келі. Маємо:

$$a\circ a=a,\ a\circ b=b,\ b\circ a=b,\ b\circ b=a.$$

Отже, нейтральним є елемент $a = \boldsymbol{e}$.

Відповідь: елемент a.

№2. *Довести, що множина всіх цілих чисел, які діляться на 3, є абелевою групою відносно додавання.*

Доведення. Перевіримо, чи виконуються у множині $M=\{3a,\ a\in Z\}$ аксіоми групи відносно операції додавання.

1. Нехай $a, b \in Z$, тоді $3a + 3b = 3(a+b) \in M$. Отже операція + замкнена у множині M. 1 аксіома виконується.
2. $(3a+3b)+3c = 3a+(3b+3c)$. Асоціативність виконується.
3. $e = 3\cdot0$ – нейтральний елемент, бо $3a+3\cdot0 = 3\cdot0+3a = 3a.$
4. $-3a$ – симетричний елемент для $3a$, бо $3a+(-3a) =-3a+3a = =3\cdot0$.

Отже, дана множина є групою відносно додавання. Перевіримо, чи виконується комутативність:

$$3a+3b = 3b+3a.$$

Комутативність виконується, а отже, множина всіх цілих чисел, які діляться на 3, є абелевою групою відносно додавання.

№3. *Перевірити, чи є групою множина всіх неособливих матриць другого порядку з невід'ємними елементами множення.*

Розв'язання.

$$M=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in R_{+} \cup 0\right\}.$$

Перевіримо, чи виконуються у множині M аксіоми групи відносно операції множення.

1) $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B=\begin{pmatrix} k & l \\ m & n \end{pmatrix}$ $\quad AB=\begin{pmatrix} ak+bm & al+bn \\ cm+dm & cl+dn \end{pmatrix}$.

Оскільки $ak+bm, al+bn, ck+dm, cl+dn \in R_{+} \cup 0,$ то $AB \in M$. Отже. операція множення замкнена у множені М.

2) $C=\begin{pmatrix} x & y \\ z & t \end{pmatrix}$

$$(AB)C=\begin{pmatrix} ak+bm & al+bn \\ cm+dm & cl+dn \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix}=$$

$$=\begin{pmatrix} (ak+bm)x+(al+bn)z & (ak+bm)y+(al+bn)t \\ (cm+dm)x+(cl+dn)z & (cm+dm)y+(cl+dn)t \end{pmatrix}=$$

$$=\begin{pmatrix} akx+bmx+alz+bnz & aky+bmy+alt+bnt \\ ckx+clz+dmx+dnz & cky+dmy+clt+dnt \end{pmatrix};$$

$$BC=\begin{pmatrix} kx+lz & ky+lt \\ mx+nz & my+nt \end{pmatrix};$$

$$A(BC)$$

$$=\begin{pmatrix} a(kx+lz)+b(mx+nz) & a(ky+lt)+b(my+nt) \\ c(kx+lz)+d(mx+nz) & c(ky+lt)+d(my+nt) \end{pmatrix}=$$

$$=\begin{pmatrix} akx+alz+bmx+bnz & aky+alt+bmy+bnt \\ ckx+clz+dmx+dnz & cky+clt+dmy+dnt \end{pmatrix}.$$

Отже, $(AB)C=A(BC)$ асоціативність виконується.

3) Нехай C – нейтральний елемент. Тоді $AC=A$

$$AC=\begin{pmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{pmatrix};$$

$$\begin{cases} ax+bz=a \\ ay+bt=b \\ cx+dz=c \\ cy+dt=d \end{cases} \quad \begin{cases} x=1 \\ z=0 \\ y=0 \\ t=1 \end{cases}; \quad C=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

4) Нехай B – симетричний елемент для A. Тоді $AB=C$

$$\begin{pmatrix} ak+bm & al+bn \\ ck+dm & cl+dn \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$ak+bm=1$$

$$k = \frac{1-bm}{a}.$$

З останньої рівності випливає, що існують варіанти, де $k < 0$, а це суперечить умові. Отже, остання аксіома не виконується і множина *M* не є групою відносно множення.

Відповідь: не є групою.

№4. *У мультиплікативній групі всіх неособливих матриць другого порядку знайти порядок такого елемента:*

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

Розв'язання. Нейтральним елементом мультиплікативної групи всіх неособливих матриць другого порядку є матриця $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (див. приклад № 3).

Знайдемо порядок елемента *A*:

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix};$$

$$A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

$$A^4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Оскільки одиниці групи дорівнює четверта степінь елемента *A*, то порядок елемента *A* дорівнює 4.

Відповідь: 4.

№5. *Показати, що множина всіх підстановок степеня n з операцією множення є групою.*

Розв'язання. Нехай S_n – сукупність всіх підстановок степеня *n*, тобто:

$$S_n = \left\{ \begin{pmatrix} 1 & 2 & \dots n \\ a_1 & a_2 & \dots a_n \end{pmatrix} | a_i \in M, i = 1,2,\dots n \right\}.$$

Добутком двох підстановок φ і ψ є така підстановка η, що $\eta(u)=\varphi(\psi(u))$ $u \in M$.

Наприклад,

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

Легко перевірити, що ця операція асоціативна, а одиничним елементом є одинична підстановка (тотожне відображення). Оберненою підставкою $\begin{pmatrix} 1 & 2 & \dots n \\ a_1 & a_2 & \dots a_n \end{pmatrix}$ є підстановка $\begin{pmatrix} a_1 & a_2 & \dots a_n \\ 1 & 2 & \dots n \end{pmatrix}$.

Отже, множина всіх підстановок степеня n з операцією множення є групою.

№6. *Знайти фактор-групу адитивної групи цілих чисел Z^+ за підгрупою $(mZ)^+$, де $m>1$.*

Розв'язання. Множина $Z^+/(mZ)^+$ складається з елементів:

$$Z^+/(mZ)^+=\{(mZ)^+;\ 1+(mZ)^+;\ \dots;(m-1)+(mZ)^+\}.$$

Дійсно, довільне ціле число n можна представити у вигляді $n=mq+r$, $0\le r<m$. Тоді, $n+(mZ)^+=(r+mq)+(mZ)^+=r+(mZ)^+$.

Далі, якщо $0\le i<j\le m-1$, $j-i$ не належить $(mZ)^+$, а отже, $i+(mZ)^+\ne j+(mZ)^+$.

Додаються суміжні класи за таким правилом:

$$(a+(mZ)^+)+(b+(mZ)^+)=(a+b)+(mZ)^+.$$

Отже, $Z^+/(mZ)^+$ – фактор-група порядку m.

Наприклад, при $m=3$ маємо групу

$Z^+/(3Z)^+=\{(3Z)^+;\ 1+(mZ)^+;\ 2+(mZ)^+\}$ і таблиця додавання елементів цієї групи є наступною.

+	$(3Z)^+$	$1+(mZ)^+$	$2+(mZ)^+$
$(3Z)^+$	$(3Z)^+$	$1+(mZ)^+$	$2+(mZ)^+$
$1+(mZ)^+$	$1+(mZ)^+$	$2+(mZ)^+$	$(3Z)^+$
$2+(mZ)^+$	$2+(mZ)^+$	$(3Z)^+$	$1+(mZ)^+$

№7. *Довести ізоморфізм мультиплікативної групи R^*_+ додатних дійсних чисел та адитивної групи дійсних чисел R^+.*

Розв'язання. Побудуємо відображення $f: R^*_+ \to R^+$ за таким правилом: $f(a)=lga$ $(a\in R^+)$. Оскільки $lg(ab)=lga+lgb$ $(a, b\in R^+)$, то відображення є гомоморфним.

Відомо, що логарифм задає відображення R^*_+ на R^+. Оскільки рівняння $lgx=0$ має єдиний розв'язок $x=1$, то

Ker f={1}. Тому за теоремою про гомоморфізм груп одержуємо, що $R^*_+/\{1\}$ ізоморфно R^+. Звідси випливає, ізоморфізм мультиплікативної групи R^*_+ додатних дійсних чисел та адитивної групи дійсних чисел R^+.

№8. *Виписати всі підгрупи групи* Z^+_{18}.

Розв'язання. Група $Z^+_{18}=\{(18Z)^+; 1+(18Z)^+; \dots ; 17+(18Z)^+\}$ є циклічною групою порядку 18. Твірним цієї групи є, наприклад, $1+(18Z)^+$, оскільки

$n+(18Z)^+=n(1+(18Z)^+)$, $n=0,1,\dots,17$.

Тоді за властивістю циклічних груп маємо, що будь-яка підгрупа групи Z^+_{18} є циклічною і їх стільки, скільки дільників у числа 18: 1, 2, 3, 6, 9, 18 – шість.

$G_1=<(18Z)^+>$, $G_2=<9+(18Z)^+>$, $G_3=<6+(18Z)^+>$, $G_6=<3+(18Z)^+>$, $G_9=<2+(18Z)^+>$, $G_{18}=<1+(18Z)^+>$. $|G_i|=i$ ($i=1, 2, 3, 6, 9, 18$).

Завдання для аудиторного заняття

№1. Перевірити, чи є задана множина групою*:*

а) ‹Z; -› – усіх цілих чисел з операцією віднімання;

б) ‹Q+; ·› – усіх додатних раціональних чисел з операцією множення;

в) ‹Z[i]; + › – усіх комплексних чисел $a+bi$, де $a, b \in Z$ з операцією додавання;

г) множина всіх матриць другого порядку з цілими елементами, визначник яких дорівнює одиниці.

№2. У множині $Z\times\{1;-1\}$ визначено операцію *:

$(m, a)*(n, b) = (m+n, a\cdot b)$.

Довести, що дана множина з визначеною операцію * є групою.

№3. Нехай G і F – деякі групи відносно операцій $\cdot$ і $\circ$ відповідно. Довести, що множина $G\times F$ є групою відносно операції *:

$(g_1, f_1)*(g_2, f_2) = (g_1 \cdot g_2, f_1 \circ f_2)$.

№4. Скласти таблицю Келі для операції * заданої у множині {0,1,2,3,4,5}: $a*b$ є остача від ділення $a+b$ на 6. Перевірити чиє задана множина абелевою групою.

№5. Перевірити чи є задана множина всіх цілих степенів числа 2 є мультиплікативною групою.

№6. Визначити парність підстановки

а) $A=\begin{pmatrix}1&2&3&4&5&6\\6&3&5&1&4&2\end{pmatrix}$;

б) $B=\begin{pmatrix}1&2&3&4&5&6\\1&4&2&3&5&6\end{pmatrix}$.

№7. У мультиплікативній групі всіх неособливих матриць другого порядку знайти порядок таких елементів:

а) $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$; б) $\begin{pmatrix}1&1\\0&1\end{pmatrix}$; в) $\begin{pmatrix}-2+3i&-2+2i\\1-i&3-2i\end{pmatrix}$.

№8. У мультиплікативній групі всіх комплексних чисел, відмінних від нуля, знайти підгрупу, породжену елементом:

а) $-i$;

б) $-\frac{1}{2}+\frac{i\sqrt{3}}{2}$.

№9. Знайти фактор-групу G/H у таких випадках:

а) $G=C^+$ – адитивна група комплексних чисел, $H=R^+$ – адитивна група дійсних чисел;

б) $G=C^+$ – мультиплікативна група комплексних чисел, $H=R^+$ – мультиплікативна група дійсних чисел.

№10. Чи є відображення $f: C^*\to R^*$ гомоморфним, якщо:

а) $f(z)=|z|$;

б) $f(z)=|z|^2$.

№11. Довести, що групи $(5\mathbb{Z})^+$ (адитивна група цілих чисел кратних 5) і $(2\mathbb{Z})^+$ (адитивна група цілих чисел кратних 2) ізоморфні.

№12. Довести, що задана група $(n\mathbb{Z})^+$ цілих чисел, кратних даному натуральному числу n, відносно операції додавання є циклічною і знайти її твірний елемент.

№13. Знайти всі підгрупи циклічної групи порядку 15.

Відповіді: ***№1***. а) не є групою; б) є групою; в) є групою; г) не є групою. ***№6.*** а) непарна; б) парна. ***№7***. а) 2; б) ∞; в) ∞. ***№8.*** а) {-*i*, -1, *i*, 1}; б) $\left\{-\frac{1}{2}+\frac{i\sqrt{3}}{2};-\frac{1}{2}-\frac{i\sqrt{3}}{2};1\right\}$.

Завдання для самостійного розв'язування

№1. Перевірити, чи є задана множина групою:

а) $\langle\{nz \mid z \in Z\}, +\rangle$ – усіх цілих чисел, кратних з операцією додавання;

б) $\langle Q+; : \rangle$ – усіх додатних раціональних чисел з операцією ділення;

в) $\langle Z; * \rangle$, де $a * b = a + b - 2017$;

г) множина всіх матриць виду

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

, де $a \in R \backslash \{0\}$.

№2. Нехай у множині Z^2 задано операцію

$(a, b)+(c, d) = (a+c, b+d)$.

Довести, що задана множина є абелевою групою.

№3. У множині всіх пар (a, b) раціональних чисел, де $a \neq 0$, операція множення визначається рівністю $(a, b)\ (c, d) = (ac, bc+d)$. Довести, що задана множина є групою.

№4. У множині {0, 1, 2, 3} задано операцію $*$: $a*b$ є остача від ділення добутку ab на 4. Задати операцію * таблицею Келі, і перевірити чи є задана множина групою відносно операції *.

№5. Визначити парність підстановки

а) $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$;

б) $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$.

№6. У мультиплікативній групі всіх неособливих матриць другого порядку знайти порядок таких елементів:

а) $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$; в) $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

№7. У мультиплікативній групі всіх комплексних чисел, відмінних від нуля, знайти підгрупу, породжену елементом:

а) i; б) $\frac{\sqrt{2}}{2} + \frac{i\sqrt{2}}{2}$.

№8. Знайти фактор-групу G/H у таких випадках:

а) $G = S_n$ – симетрична група, $H = A_n$ – знакозмінна група;

б) $G = (4Z)^+$, $H = (12Z)^+$.

№9. Чи є відображення $f:C^*\to R^*$ гомоморфним, якщо:

а) $f(z)=2|z|$;

б) $f(z)=1+|z|$.

№10. Довести, що задана група комплексних коренів n-го степеня з одиниці відносно операції множення є циклічною і знайти її твірний елемент.

№11. Знайти всі підгрупи циклічної групи порядку 24.

Відповіді:

№1. а) є групою; б) не є групою; в) є групою; г) є групою. ***№5.*** а) непарна; б) парна. ***№6***. а) ∞; б) ∞; в) 4. ***№7.*** а) $\{i, 1, -i, -1\}$;

б) $\left\{\frac{\sqrt{2}}{2}+\frac{i\sqrt{2}}{2}; i; -\frac{\sqrt{2}}{2}+\frac{i\sqrt{2}}{2}; -1; -\frac{\sqrt{2}}{2}-\frac{i\sqrt{2}}{2}; -i; \frac{\sqrt{2}}{2}-\frac{i\sqrt{2}}{2}; 1\right\}$.

Тема друга
КІЛЬЦЕ. ОБЛАСТЬ ЦІЛІСНОСТІ. ПОЛЕ ЧАСТОК

Елементарні відомості про кільця

Кільцем називається непорожня множина *К,* в якій визначені дві бінарні операції – додавання і множення, причому за додаванням *К* є абельова група – адитивна група кільця *К,* а операція множення – асоціативна і пов'язана дистрибутивними законами з операцією додавання. Якщо операція множення в кільці *К* комутативна, то кільце *К* називають *комутативним.*

Прикладами комутативних кілець є: множина цілих чисел, множина цілих чисел кратних деякому відмінному від 1 натуральному числу *m* (зокрема множина парних чисел), множина раціональних чисел *Q*, множина дійсних чисел *R*, множина комплексних чисел *C*, множина всіх чисел вигляду $a + b\sqrt{2}$, де *a* і *b* – будь-які раціональні числа, множина всіх дійсних неперервних функцій від дійсного змінного *x,* заданих на відрізку [0, 1], кільце Z_m класів, конгруентних за модулем *m* цілих чисел.

Прикладами некомутативних кілець є: кільце Q_n квадратних матриць *n-го* порядку над полем раціональних чисел *Q*, кільце R_n матриць *n-го* порядку над полем дійсних чисел *R*, кільце C_n матриць *n-го* порядку над полем комплексних чисел *C*.

Скалярною матрицею над полем *P* називають матрицю, яка має на головній діагоналі той самий елемент *a*, а поза головною діагоналлю – нулі. Множина R^*_n всіх скалярних матриць *n-го* порядку над полем дійсних чисел є комутативне кільце.

Означення*. Елемент $b \in K$ називають лівим* (*відповідно правим*) *дільником елемента $a \in K$, якщо існує елемент $c \in K$ такий, що $a = bc$* (відповідно $a = cb$)*; при цьому говорять також, що a є правим* (*відповідно лівим*) *кратним елемента b.*

Якщо кільце *К* – комутативне (тобто порядок слідування множників у добутку можна змінити), то поняття лівого дільника (кратного) збігається з поняттям правого дільника (кратного). Тому в цьому випадку говорять просто «дільник» і «кратне».

Зауважимо, що коли в кільці *К* немає одиниці, тобто такого елемента ***е,*** що $a\boldsymbol{e} = \boldsymbol{e}a = a$, елемент $a \in K$ може не бути дільником (лівим чи правим) самого себе. Так, у кільці парних чисел жодне з відмінних від нуля чисел не є дільником самого себе. Так само, якщо в кільці *К* немає одиниці ***е,*** то елемент *na*, де $a \in K$, а *n* – деяке ціле число, не буде, взагалі кажучи, кратним елемента *а* у смислі наведеного вище означення. Так, у кільці цілих чисел, кратних 3, елемент 5(3) = 15 не є кратним елемента 3, оскільки число 5 не є елементом кільця.

Якщо ж у кільці *К є* одиничний елемент ***е,*** то для будь-якого $a \in K$, *na* є кратним елемента *а.*

Означення*. Підмножина К′ кільця К називається підкільцем кільця К, якщо К′ є кільце відносно операцій додавання і множення, визначених у кільці К.*

Так, кільце парних чисел є підкільце кільця цілих чисел, а останнє, в свою чергу, є підкільцем кільця раціональних чисел. Кільце раціональних чисел і кільце чисел вигляду $a + b\sqrt{2}$, де *а* і *b* – будь-які раціональні числа, є підкільцями кільця дійсних чисел.

У кожному кільці *К,* очевидно, є такі підкільця: само кільце *К* і нульове підкільце, що складається лише з нуля кільця *К.* Ці підкільця називають *тривіальними.*

Теорема*. Для того, щоб непорожня підмножина К′ кільця К була його підкільцем, необхідно й достатньо, щоб сума a+b, різниця a-b й добуток ab будь-яких двох елементів a і b підмножини К′ належали до К′ .*

Нехай *К* і *К′* – два кільця. Кільця *К* й *К′* називаються *ізоморфними,* якщо існує таке взаємно однозначне відображення φ кільця *К* на кільце *К′*, що для будь-яких $a, b \in K$:

$$\varphi(a+b)=\varphi(a)+\varphi(b) \text{ і } \varphi(ab)=\varphi(a)\varphi(b).$$

Саме відображення φ з цими властивостями називають *ізоморфним відображенням.*

***Теорема**. Якщо множина F, в якій визначені бінарні операції додавання і множення, ізоморфно відображається на деяке кільце К, то множина F також є кільце відносно визначених у ній операцій.*

Кільця з одиницею

***Означення**. Ненульове кільце К, в якому є одиничний елемент **е**, називають кільцем з одиницею.*

Одиницю ***е*** кільця *К* ми часто позначатимемо також символом 1, але при цьому цей символ не слід ототожнювати з числом 1. В кільці цілих чисел, кратних довільно вибраному натуральному числу $m>1$, одиниці немає. Зокрема, немає одиниці в кільці парних чисел. Кільце цілих чисел, кільце раціональних чисел *Q*, кільце дійсних чисел *R* – кільця з одиницею. Кільцем з 1 є також кільце матриць *n-го* порядку над полем раціональних чисел (над полем дійсних чисел і над полем комплексних чисел). Одиницею цього кільця є одинична матриця

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

Нехай *К* – довільне кільце з одиницею. Для будь-якого відмінного від нуля елемента $a \in K$, правильні рівності $a \cdot 0 = 0 \cdot a = 0$ і $a\boldsymbol{e} = \boldsymbol{e}a = a$. Звідси випливає, що ***е*** і 0 є різні елементи кільця *К*, тобто $\boldsymbol{e} \neq 0$. Якщо для елемента $a \in K$ в кільці *К* існує обернений елемент a^{-1}, то тільки один. Елемент ***е*** є оберненим для самого себе. Елемент 0 не має оберненого елемента. Якщо для елемента $a \in K$ в кільці *К* існує обернений елемент a^{-1}, то *а*, за означенням дільників елемента кільця, є *дільником одиниці **е**.*

***Означення**. Елемент а, для якого в кільці К існує обернений елемент a^{-1}, називають оборотним або дільником одиниці.*

Кільце цілих чисел є найпростішим прикладом комутативного кільця, в якому тільки 1 і -1 є дільниками одиниці.

***Теорема**. Множина К* всіх дільників одиниці кільця К є група за множенням.* Групу *К** називають *групою дільників одиничного елемента,* або *групою одиниць кільця К.*

Дільники нуля. Область цілісності. Поле часток

Нехай *К* – довільне кільце.

***Означення.** Елементи a і b кільця К називаються дільниками нуля, якщо* $a \neq 0$, $b \neq 0$, а $\boldsymbol{ab = 0}$; *при цьому a називають лівим, а b – правим дільником нуля.*

В комутативних кільцях поняття лівого і правого дільника нуля, очевидно, збігаються.

***Означення**. Комутативне кільце, в якому немає дільників нуля, називають областю цілісності.*

Кожне числове кільце є областю цілісності. Областю цілісності є також будь-яке поле *P.*

Областю цілісності, з якою найчастіше доводиться зустрічатися, є кільце цілих чисел. Кільце цілих чисел є підкільцем поля раціональних чисел *Q*.

***Теорема**. Для кожної області цілісності R існує поле Q, що містить, як підкільце, область цілісності R.*

Нехай *R* – деяка область цілісності, що складається з елементів *a, b, c*... Розглянемо множину всіх можливих пар (*a,b*), де $a \in R$, $b \in R \setminus \{0\}$.

У множині цих пар визначимо відношення $(a,b)w(a',b') \leftrightarrow ab'=a'b$, яке є відношенням еквівалентності.

Як відомо, відношення еквівалентності визначає розбиття розглядуваної множини пар на класи еквівалентних між собою елементів, які називатимемо *класами еквівалентності w*. Позначимо множину всіх класів еквівалентності *w*, буквою *ρ*, а класи еквівалентності – малими буквами α, β, γ і т. д. Кожну пару, що входить до даного класу еквівалентності *ρ*, називатимемо представником цього класу.

***Означення**. Сумою ρ+σ класів ρ і σ називатимемо клас еквівалентності, що містить пару* (*ad+bc, bd*), *а добутком ρσ – клас еквівалентності, що містить пару* (*ac, bd*).

***Теорема**. Кожен елемент поля Q дорівнює частці деяких двох елементів області цілісності R.*

Нехай P – поле, що містить деяку область цілісності R. Поле P, очевидно, містить кожну частку $\frac{a}{b}$, де a – довільний, а b – будь-який відмінний від нуля елемент області цілісності R.

Означення. *Поле P, що містить область цілісності R, кожен елемент якого може бути записаний у вигляді частки деяких двох елементів області цілісності R, називають полем часток або полем відношень області цілісності R.*

Побудоване нами поле Q, є полем часток розглядуваної області цілісності R.

Поле часток Q області цілісності R з точністю до ізоморфізму однозначно визначається областю цілісності R, тобто, будь-які два поля часток однієї й тієї області цілісності R ізоморфні.

Теорема. *Нехай R – деяка область цілісності, а Q і Q' – її поля часток. Тоді між Q і Q' існує ізоморфна відповідність φ, яка тотожно відображає область цілісності R саму на себе.*

Ідеали кільця. Операції над ідеалами

У теорії кілець особливу роль, аналогічну ролі нормальних дільників у теорії груп, відіграють підкільця, що дістали назву *ідеалів*.

Означення*. Непорожня підмножина* $\boldsymbol{\alpha}$ *кільця K називається лівим* (відповідно *правим*) *ідеалом цього кільця, якщо a є підгрупа адитивної групи кільця K і якщо для будь-яких елементів $a \in \boldsymbol{\alpha}$ і $x \in K$ добуток xa* (відповідно *ax*) *міститься в* $\boldsymbol{\alpha}$*.*

Підмножина $\boldsymbol{\alpha}$ *кільця K, яка одночасно є лівим і правим ідеалом, називається двостороннім ідеалом, або просто ідеалом кільця K.*

У комутативному кільці кожен лівий і кожен правий ідеал, очевидно, є двостороннім ідеалом.

З означення випливає, що кожен лівий, правий, а отже, і двосторонній ідеал є підкільцем кільця K. Зауважимо, що оскільки ідеал – це деяка підмножина кільця K, то можна говорити про відношення включення між ідеалами даного кільця K.

Приклади ідеалів.

1. Кожне кільце K є своїм двостороннім ідеалом. Цей ідеал називають *одиничним.* У кожному кільці K нульове підкільце {0} є ідеалом, його називають *нульовим ідеалом* і позначають символом {0}.

Одиничний ідеал K кільця K містить будь-який ідеал $\boldsymbol{\alpha}$ цього кільця, а нульовий ідеал {0} міститься в кожному ідеалі кільця K. Отже, в сенсі відношення включення одиничний ідеал – найбільший, а нульовий – найменший серед ідеалів кільця K.

2. Нехай K – деяке кільце і a – будь-який елемент цього кільця. Множина Ka всіх елементів виду xa, де x – будь-який елемент кільця K, є лівий ідеал, множина aK всіх елементів виду ax – правий ідеал, а множина $m(a)$ всіх елементів виду

$$x_1 a y_1 + x_2 a y_2 + \cdots + x_n a y_n,$$

де n – будь-яке натуральне число, x_i й y_i – будь-які елементи кільця K, є двосторонній ідеал кільця K.

3. Нехай K – деяке комутативне кільце і a – будь-який елемент цього кільця. Множина елементів виду $xa + na$, де x – будь-який елемент кільця K, а n – будь-яке ціле число, є ідеал кільця K.

Цей ідеал називають *головним ідеалом, породженим елементом a,* і позначають символом (a). Серед ідеалів, що містять елемент a, головний ідеал (a) є найменшим (в смислі відношення включення).

Якщо в кільці K є одиниця $\boldsymbol{e}$, то $(a) = Ka$. Справді, з означення ідеалу (a) випливає, що $Ka \subseteq (a)$. З другого боку, $xa+na=xa+n\boldsymbol{e}a=(x+n\boldsymbol{e})a=x'a \in Ka$, тому $(a) \subseteq Ka$. Отже, $(a)=Ka$. Наприклад, головний ідеал (m) кільця цілих чисел складається з усіх цілих чисел, кратних числу m: $(m) = Zm$.

Зауважимо, що нульовий ідеал {0} кільця K *є* головний ідеал (о). Якщо в кільці K є одиниця $\boldsymbol{e}$, то одиничний ідеал K також є головним ідеалом, а саме: $K = (\boldsymbol{e})$.

4. Аналогічно тому, як ми визначили поняття головного ідеалу (a) комутативного кільця K, можна визначити поняття ідеалу, породженого кількома елементами $a_1, a_2, \ldots, a_s$. Нехай K – деяке комутативне кільце і нехай $a_1, a_2, \ldots, a_s$ – будь-які елементи цього кільця. Множина елементів виду

$$\sum_{i=1}^{s} x_i\, a_i + \sum_{j=1}^{s} n_j a_j,$$

де x_i – будь-який елемент з кільця K, n_j – будь-яке ціле число, є ідеал кільця K. Цей ідеал позначають символом $(a_1,a_2, ..., a_s)$; множину елементів $a_1, a_2, ..., a_s$ називають *базисом ідеалу* $(a_1,a_2, ..., a_s)$. Звичайно, для ідеалу $(a_1,a_2, ..., a_s)$, крім базису $a_1,a_2, ..., a_s$ можуть існувати й інші базиси, причому деякі з них можуть складатися з меншого ніж s числа елементів.

Перейдемо тепер до розгляду деяких операцій над ідеалами кільця *К.* Першою операцією, яку ми розглянемо, є операція теоретико-множинного перетину. Нехай а і b – будь-які ідеали кільця *К.*

Теорема. *Перетин $a \cap b$ ідеалів a і b кільця K є ідеал цього кільця.*

Нехай A і B – деякі непорожні підмножини кільця *К.*

Означення*. Множину всіх елементів виду $a+b$, де $a \in A$, $b \in B$, називають сумою підмножин A і B й позначають символом $A+B$.*

Якщо підмножина A складається тільки з одного елемента a, то суму $A+B$ позначають символом $a+B$. Оскільки операція додавання елементів кільця K асоціативна й комутативна, то й операція додавання підмножин кільця K також асоціативна і комутативна.

Означення. *Добутком AB підмножин A і B називають множину всіх елементів виду $\sum_{i=1}^{n} a_i b_i$, де n – деяке натуральне число, $a_i \in A$, $b_i \in B$.*

Якщо підмножина A складається лише з одного елемента a, то добуток AB позначати, символом aB. Цей добуток складається з усіх елементів виду ab, $b \in B$.

Визначена так операція множення підможин кільця K асоціативна. Якщо кільце K комутативне, то операція множення підмножин також буде комутативною.

Якщо $A_1, A_2, ..., A_s$ – підмножини кільця K, то добуток $A_1A_2 ...A_s$ (його позначають символом ΠA_i) складається з усіх сум добутків виду $a_1 ... \ a_s$, де $a_i \epsilon A_i$, $i = 1, 2, ..., s$.

Операції додавання й множення підмножин кільця можна, звичайно, застосувати до ідеалів.

Нехай a і b – довільні ідеали кільця *К.*

***Теорема**. Сума a +b ідеалів a і b кільця K є ідеал цього кільця.*

***Теорема**. Добуток ab ідеалів a і b кільця K також є ідеал кільця K.*

Операція додавання ідеалів – асоціативна і комутативна, а операція множення – асоціативна. Якщо кільце *K* – комутативне, то операція множення ідеалів також комутативна.

***Теорема**. Операції множення і додавання ідеалів кільця K пов'язані дистрибутивними законами.*

Конгруенції і класи лишків за ідеалом. Фактор-кільце

Нехай *K* – деяке кільце, а *m* – довільний ідеал цього кільця. Ми знаємо, що *K* є адитивна абельова група, а ідеал *m* – підгрупа цієї групи. Оскільки в абельовій групі всі її підгрупи є нормальними дільниками, то ідеал *m* є нормальний дільник групи *K.* Отже, існує фактор-група *K/m* групи *K* за нормальним дільником *m*. Вона складається з суміжних класів групи *K* за нормальним дільником *m*: 0+*m*, *a+m, b+m,…*

Нагадаємо, що елементи *x, y* ∈ *K* належать до того самого суміжного класу адитивної групи *K* за підгрупою *m* тоді і тільки тоді, коли (*x-y*) ∈ *m*. Оскільки група *K* – абельова, то й *K/m* – адитивна абельова група. У групі *K/m* можна так означити операцію множення, вона буде кільцем відносно визначених у ній операцій додавання і множення.

***Означення**. Вважають, що елемент x ∈ K конгруентний елементу y ∈ K за ідеалом m або за модулем m, якщо* (*x-y*) ∈ *m, тобто якщо x і y належать до того самого суміжного класу адитивної групи K за підгрупою m.*

Висловлення «*x* конгруентно за модулем *m*» скорочено записують так: *x*≡*y* (*mod m*).

Отже, *x*≡*y* (*mod m*) ↔ (*x-y*) ∈ *m.*

Якщо *m* є головний ідеал (*m*), то замість *x*≡*y* (*mod m*) можна було б писати *x*≡*y* (*mod m*). Проте в цьому випадку пишуть просто *x*≡*y* (*mod m*) і говорять: *x* конгруентне *y* за модулем *m.* У випадку, коли *x* не конгруентне *y* за модулем

m, пишуть $x \not\equiv y \pmod m$. Сформульоване вище означення визначає в множині K бінарне відношення; його називають *відношенням конгруентності* або просто *конгруентністю.* Відношення конгруентності, як випливає з його означення, задається розбиттям адитивної групи K на суміжні класи за підгрупою m і, отже, є відношенням еквівалентності на множині K, тобто воно рефлексивне, симетричне і транзитивне.

Класи еквівалентності відношення конгруентності в кільці K є, таким чином, суміжними класами групи K за підгрупою m; їх називають *класами лишків кільця K за ідеалом m, або за модулем m*.

Ми позначатимемо їх символами $\overline{a},\ \overline{b},\ \overline{c}\ldots$

Спинимося на деяких властивостях конгруенцій.

1. *Обидві частини конгруенції можна помножити на будь-яке ціле число n:*

   $\forall x, y \in K\ \forall n \in Z: x \equiv y \pmod m \rightarrow nx \equiv ny \pmod m.$
2. *До обох частин конгруенції можна додати будь-який елемент $z \in K$:*

   $\forall x, y, z \in K: x \equiv y \pmod m \rightarrow x + z \equiv y + z \pmod m.$
3. *Обидві частини конгруенції можна помножити на будь-який елемент $z \in K$:*

   $\forall x, y, z \in K: x \equiv y \pmod m \rightarrow xz \equiv yz \pmod m$ *і* $zx \equiv zy \pmod m$.
4. *Конгруенції можна почленно додавати і віднімати:*

   $\forall x, y, u, v \in K: x \equiv y \pmod m$ *і* $u \equiv v \pmod m \rightarrow x \pm u \equiv y \pm v \pmod m$.
5. *Конгруенції можна почленно перемножати:*

   $\forall x, y, u, v \in K: x \equiv y \pmod m$ *і* $u \equiv v \pmod m \rightarrow xu \equiv yv \pmod m$.

З викладеного видно, що над конгруенціями можна виконувати всі ті операції, які виконують над рівностями, за винятком скорочення обох частин конгруенції на їх спільний дільник. *Скорочувати конгруенції, взагалі кажучи, не можна.*

Наприклад, у кільці цілих чисел істинна конгруенція $16 \equiv 4 \pmod 6$, проте $4 \not\equiv 1 \pmod 6$, бо $4-1=3 \not\in (6)$. Отже, скорочувати обидві частини конгруенції $16 \equiv 4 \pmod 6$ на їх спільний дільник 4 не можна.

Зауваження. Співвідношення $x \equiv y (mod\ m)$ ми назвали конгруенцією. Проте символом $x \equiv y (mod\ m)$ часто позначають також і відношення конгруентності.

Повернемося тепер знову до фактор-групи *К/m*. Нагадаємо, що *К/m* складається з класів лишків $\overline{a}$, $\overline{b}$, $\overline{c}$... Як відомо, кожен клас $\overline{a}$ породжується будь-яким зі своїх елементів: якщо $a \in \overline{a}$, то $\overline{a} = a + m$; тому будь-який з елементів класу *a* можна вважати представником цього класу.

Додавання класів лишків (суміжних класів) означається так: якщо $a \in \overline{a}$ і $b \in \overline{b}$, то $\overline{a} + \overline{b}$ – це той клас лишків, який містить елемент *a+b.* Інакше кажучи,

$$\overline{a} + \overline{b} = (a + m) + (b + m) = (a + b) + m.$$

Означимо тепер в *К/m* операцію множення.

Нехай $a \in \overline{a}$ і $b \in \overline{b}$, *у*мовимося вважати, що $\overline{ab}$ – це клас, який містить елемент *ab,* тобто що $\overline{a}\,\overline{b} = (a + m)(b + m) = ab + m$.

Означений так добуток класів не залежить від вибору представників цих класів.

***Теорема**. Множина К/m класів лишків кільця К за ідеалом m з означеними у ній операціями додавання і множення є кільце. Це кільце називають фактор-кільцем кільця К за ідеалом m або за модулем m*.

Зауважимо, що фактор-кільце *К/m* називають також *кільцем класів лишків.* Всюди далі символ *К/m* означатиме фактор-кільце кільця *К* за модулем *m*.

Приклади. 1. У кожному кільці *К* є одиничний ідеал *К* і нульовий ідеал (о). Фактор-кільце *К/К* є нульове кільце {0}, а фактор-кільце *К/*(о) ізоморфне кільцю *К.*

2. У кільці цілих чисел візьмемо головний ідеал *m*=(*m*) (*m* – деяке відмінне від 1 натуральне число). Цей ідеал складається з усіх цілих чисел, кратних числу *m.* Ідеал (*m*) є нульовим класом лишків. Всі цілі числа, конгруентні за модулем *m* числу 1, утворюють клас лишків $\overline{1} = 1 + (m)$, конгруентні числу 2 - клас лишків $\overline{2} = 2 + (m)$, конгруентні числу 3 – клас лишків $\overline{3} = 3 + (m)$ і т. д.; всі числа,

конгруентні за модулем m числу m-1, утворюють клас лишків $\overline{m-1} = m-1+(m)$. Інших класів лишків бути не може, оскільки кожне ціле число належить до одного з перелічених нами класів.

Отже, фактор-кільце $Z/(m)$ складається з класів лишків $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$. Операції додавання і множення в кільці $Z/(m)$ виконують за такими правилами: щоб додати класи $\overline{k} = k + (m)$ і $\overline{l} = l + (m)$ треба знайти суму $k+l$ представників цих класів і потім знайти лишок від ділення $k+l$ на m; якщо цим лишком є число r, то $\overline{k} + \overline{l} = r$. Аналогічно, щоб перемножити класи $\overline{k}$ і $\overline{l}$, потрібно знайти добуток kl представників цих класів і потім знайти лишок від ділення kl на m; якщо цим лишком є число s, то $\overline{k} \cdot \overline{l} = s$. У теорії чисел кільце $Z/(m)$ називають *кільцем класів конгруентних чисел* за *модулем m або кільцем лишків за модулем m.*

Означення. *Елемент a називається простим, якщо його не можна представити у вигляді добутку двох необоротних елементів кільця К.*

Теорема. *Нехай К – область головних ідеалів, а – ненульовий елемент кільця К. Фактор-кільце К/<a> є полем тоді і тільки тоді, коли а – простий елемент.*

Теорема*. Всяка область головних ідеалів є факторіальним кільцем – областю цілісності з одиницею, в якій має місце однозначний розклад на прості множники.*

Гомоморфізми кілець. Теорема про гомоморфізми

Нехай *К і К'* – деякі кільця.

Означення*. Відображення φ: К→К' кільця К в кільце К' називається гомоморфним відображенням К в К', або гомоморфізмом К в К', якщо виконуються такі умови для будь-яких елементів a, b ∈ К:*

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$;
2) $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Якщо гомоморфне відображення φ є відображенням кільця K на кільце K', то його називають *гомоморфізмом*

кільця К на кільце К', або *епіморфізмом кільця К.* У цьому випадку говорять, що кільце *К'* є *гомоморфним образом кільця К',* і пишуть *К~К'.*

Приклади гомоморфізмів кілець.

1. Нехай *С* – кільце всіх комплексних чисел і C_2 – кільце матриць 2-го порядку над полем комплексних чисел. Розглянемо відображення ψ, яке визначають так: для будь-яких комплексних чисел *a+bi*

$$\psi(a+bi)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Відображення ψ задовольняє умови 1 і 2 означення гомоморфізму. Цей гомоморфізм є ізоморфізмом.

2. Нехай *К* – деяке кільце і *m* – довільний ідеал цього кільця. Розглянемо відображення х кільця *К* в фактор-кільце *К/m,* яке задається так: кожному елементу *a* ∈ *К* відповідає той клас лишків за модулем *m*, до якого належить елемент *a*, тобто клас *a* + *m.* Очевидно, що х є відображення кільця *К* на кільце *К/m.* х задовольняє вимоги означення гомоморфізму. Відображення х: *К* на *К/m* називають *природним,* або *канонічним гомоморфізмом.*

Теорема. *Якщо φ є гомоморфізм кільця К в кільце К', то:*

1) *φ (0)=0';*
2) *для будь-якого a ∈ К: φ (-a)= - φ(a);*
3) *φ(К) є підкільце кільця К';*
4) *якщо в кільці К є одиничний елемент* ***е****, то φ(****е****) – одиничний елемент кільця φ(К) й якщо для елемента a ∈ К в кільці К існує обернений елемент* a^{-1}*, то φ(*a^{-1}*) – обернений елемент елементу φ(a) кільця φ(К).*

Означення. *Нехай φ є гомоморфізм кільця К в кільце К'. Множину* И *всіх елементів кільця К, які гомоморфізмом φ відображаються в* 0' *кільця К', називають ядром гомоморфізму φ і записують И=Кerφ.*

Теорема*. Ядро И=Кerφ будь-якого гомоморфізму φ кільця К в кільце К' є ідеал кільця К.*

Теорема про гомоморфізми кілець. *Якщо φ є гомоморфізм кільця К на кільце К' і И= Кer φ, то кільце К' ізоморфне фактор-кільцю К/И, причому існує такий ізоморфізм ψ кільця К/И на кільце К', що добуток х ψ природного гомоморфізму х: К~ К/И на ізоморфізм ψ є гомоморфізм φ.*

Теорема про гомоморфізми кілець показує, що природними гомоморфізмами кільця *K* на його фактор-кільця по суті вичерпуються його гомоморфізми.

Характеристика кільця з одиницею

З'ясуємо, які ідеали є в найпростішому з кілець - кільці цілих чисел. Як відомо, кожне ціле число *n* породжує головний ідеал (*n*)=*Zn.* Такими ідеалами вичерпується множина всіх ідеалів кільця цілих чисел, оскільки має місце така теорема.

***Теорема**. Кожен ідеал кільця цілих чисел є головним ідеалом.*

Нехай *A* – довільне кільце з одиницею ***e*** і *Z* – кільце цілих чисел. Розглянемо відображення φ: *Z*→ *A,* яке задається так: $\varphi(n) = n\boldsymbol{e}$.

Очевидно, що φ є гомоморфізм кільця *Z* в кільце *A.* За теоремою множина *E*= φ(*Z*) є підкільце кільця *A.* Підкільце *E* складається з усіх цілих кратних *n**e*** одиничного елемента ***e**;* будемо називати його *підкільцем, породженим одиницею **e**.* Як легко бачити, φ є гомоморфізм кільця *Z* на підкільце *E.* Тому, за теоремою про гомоморфізми кілець, підкільце *E* ізоморфне фактор-кільцю *Z/И*, де И – ядро гомоморфізму φ: *Z*~ *E.* Оскільки в кільці цілих чисел кожен ідеал головний, то И=*(p),* де *p* - деяке невід'ємне число.

Можливі два випадки:

1. *p* = 0. Тоді *E*≅*Z/*(0) ≅Z. Тобто підкільце *E* ізоморфне кільцю цілих чисел *Z.*
2. *p* > 0. Тоді підкільце *E* ізоморфне кільцю класів лишків *Z* /(*p*).

Отже, в будь-якому кільці *A* з одиницею ***e*** підкільце *E,* породжене елементом ***e**,* ізоморфне або кільцю цілих чисел *Z*, або кільцю класів лишків *Z*/(*p*), де *p* – деяке натуральне число. Виходячи з цього, ми введемо таке означення.

***Означення**. Нехай A – деяке кільце з одиницею **e**. Ми будемо говорити, що кільце A має характеристику 0, якщо його підкільце E, породжене одиничним елементом **e**, ізоморфне кільцю цілих чисел Z; ми говоритимемо, що кільце A має характеристику p>0, якщо підкільце E ізоморфне кільцю класів лишків Z /(p).*

Зауваження. Поряд з висловом «кільце A має характеристику 0 (або p)» вживають також вирази «характеристика кільця A дорівнює 0 (або p)», «A є кільце характеристики 0 (або p)».

За означенням, кільце цілих чисел має характеристику 0, а кільце $Z/(p)$ – характеристику p.

Теорема. *Якщо кільце A має характеристику 0, то* $n\boldsymbol{e}=0$ *лише при* $n=0$; *якщо ж A має характеристику* $p>0$, *то* $p\boldsymbol{e}=0$ *і немає такого натурального числа* $m<p$, *що* $m\boldsymbol{e}=0$.

Правильна також і обернена теорема.

Теорема*. Якщо в кільці A з одиницею рівність* $n\boldsymbol{e}=0$ *справджується лише при* $n=0$, *то A має характеристику* 0; *якщо в кільці A справджується рівність* $p\boldsymbol{e}=0$ *і немає такого натурального* $m<p$, *що* $m\boldsymbol{e}=0$, *то A має характеристику p.*

З теорем випливає таке означення.

Означення*. Характеристикою кільця A з одиницею* $\boldsymbol{e}$ *називають число* 0, *якщо* $n\boldsymbol{e}=0$ *лише при* $n=0$; *характеристикою кільця A називають натуральне число p, якщо* $p\boldsymbol{e}=0$ і *немає, такого натурального числа* $m<p$, *що* $m\boldsymbol{e}=0$.

Усі числові кільця з одиницею, очевидно, мають характеристику 0. Кожне скінченне кільце A з одиницею є кільце ненульової характеристики. Справді, якщо кільце A скінченне, то серед усіх цілих додатних кратних одиничного елемента $\boldsymbol{e}$ обов'язково будуть кратні, рівні між собою, бо в противному разі кільце A було б нескінченним. Нехай $k\boldsymbol{e}=m\boldsymbol{e}$, де k і m – деякі натуральні числа, причому $m>k$. Тоді $(m-k)\boldsymbol{e}=0$ і, отже, A є кільце ненульової характеристики.

Кожне натуральне число n є характеристикою деякого кільця з одиницею: n є характеристикою кільця $Z/(n)$.

Теорема. *Якщо* R є *область цілісності характеристики 0, то*

$$\forall a \in R\ \forall n \in Z\ a \neq 0\ i\ n \neq 0\ \rightarrow na \neq 0.$$

Теорема. *Якщо* A *– кільце характеристики* p, *то* $\forall a \epsilon A: pa = 0$.

Приклади розв'язування типових завдань

№1. *Довести, що множина* $\boldsymbol{Z}[\sqrt{3}]$ *усіх чисел виду* $a + b\sqrt{3}$, *де* a *і* b *– цілі числа, є кільцем відносно звичайних операцій додавання і множення.*

Розв'язання. Перевіримо, чи виконуються у множині $\boldsymbol{Z}[\sqrt{3}]$ аксіоми кільця відносно операції додавання та множення.

1. Нехай $a, b, c, d \in Z$, тоді
$(a+b\sqrt{3})+(c+d\sqrt{3}) = a+c+b\sqrt{3}+d\sqrt{3} = (a+c)+(b+d)\sqrt{3}$
$\in \boldsymbol{Z}[\sqrt{3}]$. Отже операція + замкнена у множині $\boldsymbol{Z}[\sqrt{3}]$ 1 аксіома виконується.
2. $(a_1 + b_1\sqrt{3} + a_2 + b_2\sqrt{3}) + a_3 + b_3\sqrt{3} =$
$= a_1 + b_1\sqrt{3} + (a_2 + b_2\sqrt{3} + a_3 + b_3\sqrt{3})$.
Асоціативність виконується.
3. $e = 0 + 0\sqrt{3}$ – нейтральний елемент.
4. $-a - b\sqrt{3}$ – симетричний елемент для $a + b\sqrt{3}$.
5. $(a + b\sqrt{3}) + (c + d\sqrt{3}) = (c + d\sqrt{3}) + (a + b\sqrt{3})$.
Комутативність додавання виконується.

Отже, множина $\boldsymbol{Z}[\sqrt{3}]$ є абелевою групою відносно додавання.

6. Перевіримо, чи виконується рівність
$$((a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}))(a_3 + b_3\sqrt{3}) =$$
$$= (a_1 + b_1\sqrt{3})((a_2 + b_2\sqrt{3})(a_3 + b_3\sqrt{3}))$$
$$((a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}))(a_3 + b_3\sqrt{3}) = (a_1a_2 + a_1b_2\sqrt{3} + b_1a_2\sqrt{3} +$$
$$+3b_1b_2)(a_3 + b_3\sqrt{3}) = a_1a_2a_3 + a_1b_2a_3\sqrt{3} + b_1a_2a_3\sqrt{3} + 3b_1b_2a_3 +$$
$$+a_1a_2b_3\sqrt{3} + 3a_1b_2b_3 + 3b_1a_2b_3 + 3b_1b_2b_3\sqrt{3}$$
$$(a_1 + b_1\sqrt{3})((a_2 + b_2\sqrt{3})(a_3 + b_3\sqrt{3})) = (a_1 + b_1\sqrt{3})(a_2a_3 +$$
$$+a_2b_3\sqrt{3} + b_2a_3\sqrt{3} + 3b_2b_3) = a_1a_2a_3 + a_1a_2b_3\sqrt{3} + a_1b_2a_3\sqrt{3} +$$
$$+3a_1b_2b_3 + b_1a_2a_3\sqrt{3} + 3b_1a_2b_3 + 3b_1b_2a_3 + 3b_1b_2b_3\sqrt{3}.$$
Асоціативність множення виконується.

7. Перевіримо, чи виконується рівність
$(a_1 + b_1\sqrt{3} + a_2 + b_2\sqrt{3})(a_3 + b_3\sqrt{3}) = (a_1 + b_1\sqrt{3})(a_3 + b_3\sqrt{3}) +$
$+(a_2 + b_2\sqrt{3})(a_3 + b_3\sqrt{3})$,

$$(a_1 + b_1\sqrt{3} + a_2 + b_2\sqrt{3})(a_3 + b_3\sqrt{3}) = a_1a_3 + b_1a_3\sqrt{3} + a_2a_3 +$$
$$b_2a_3\sqrt{3} + a_1b_3\sqrt{3} + 3b_1b_3 + a_2b_3\sqrt{3} + 3b_2b_3,$$
$$(a_1 + b_1\sqrt{3})(a_3 + b_3\sqrt{3}) + (a_2 + b_2\sqrt{3})(a_3 + b_3\sqrt{3}) = a_1a_3 +$$
$$+b_1a_3\sqrt{3} + a_1b_3\sqrt{3} + 3b_1b_3 + a_2a_3 + a_2b_3\sqrt{3} + b_2a_3\sqrt{3} + 3b_2b_3.$$

Дистрибутивність виконується.

Отже, $\boldsymbol{Z}[\sqrt{3}]$ є кільцем відносно звичайних операцій додавання і множення.

№2. *Довести, що множина* Q^2 *з операціями, означеними рівностями* $(a,b)+(c,d)=(a+c,b+d)$

$(a,b)\cdot(c,d)=(ac+2bd,ad+bc)$, *є полем.*

Розв'язання. Перевіримо, чи виконуються у множині Q^2 аксіоми поля відносно заданих операцій.

1) Нехай *a, b, c, d* ∈ *Q*, тоді

$(a,b)+(c,d)=(a+c,b+d)\in Q^2$.

Отже, операція + замкнена у множині Q^2. 1 аксіома виконується.

2) Асоціативність виконується.

3) *(0, 0)*– нейтральний елемент.

4) *(-a, -b)* – симетричний елемент для *(a, b).*

5) $(a,b)+(c,d)=(c,d)+(a,b)$.

Комутативність додавання виконується.

Отже, множина Q^2 є абелевою групою відносно додавання.

6) Перевіримо, чи виконується рівність

$((a,b)\cdot(c,d))\cdot(k,l)=(a,b)\cdot((c,d)\cdot(k,l))$

$((a,b)\cdot(c,d))\cdot(k,l)=(ac+2bd,ad+bc)\cdot(k,l)=$

$=((ac+2bd)k+2(ad+bc)l,(ac+2bd)l+(ad+bc)k)=$

$=(ack+2bdk+2adl+2bcl,acl+2bdl+adk+bck).$

$(a,b)\cdot((c,d)\cdot(k,l))=(a,b)\cdot(ck+2dl,cl+dk)=$

$=(a(ck+2dl)+2b(cl+dk),a(cl+dk)+b(ck+2dl))=$

$=(ack+2adl+2bcl+2bdk,acl+adk+bck+2bdl)$.

Асоціативність множення виконується.

7) Перевіримо, чи виконується рівність

$$((a,b)+(c,d))\cdot(k,l)=(a,b)\cdot(k,l)+(c,d)\cdot(k,l)$$

$$((a,b)+(c,d))\cdot(k,l)=(a+c,b+d)\cdot(k,l)=$$
$$=((a+c)k+2(b+d)l,(a+c)l+(b+d)k)=$$
$$=(ak+ck+2bl+2dl,al+cl+bk+dk).$$
$$(a,b)\cdot(k,l)+(c,d)\cdot(k,l)=(ak+2bl,al+bk)+(ck+2dl,cl+$$
$$+dk)=(ak+2bl+ck+2dl,al+bk+cl+dk).$$

Дистрибутивність виконується.

Отже, Q^2 є кільцем відносно зазначених операцій додавання і множення.

8) $(a,b)\cdot(c,d)=(ac+2bd,ad+bc)$.

$(c,d)\cdot(a,b)=(ca+2db,cb+da)$.

Отже, $(a,b)\cdot(c,d)=(c,d)\cdot(a,b)$.

Комутативність множення виконується.

9) Для кожного елемента $(a,b)\in Q^2$ існує такий елемент $(c,d)\in Q^2$, що $(a,b)\cdot(c,d)=(k,l)\in Q^2$.

Отже, множина Q^2 є полем.

№3. *Чи є в кільці M* (2, *z*) *матриць другого порядку* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *з цілими елементами ідеалом підмножина T матриць виду* $\begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix}$, *де* $m,n\in\mathbb{Z}$.

Розв'язання. Оскільки $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\in T$, то $T\neq\varnothing$. Якщо $A, B\in T$, то $A=\begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix}, B=\begin{pmatrix} 0 & k \\ 0 & l \end{pmatrix}$, де $m, n, k, l \in Z$. Тоді $A\pm B=\begin{pmatrix} 0 & m\pm k \\ 0 & n\pm l \end{pmatrix}\in T$, оскільки $m\pm k, n\pm l\in\mathbb{Z}$.

Отже, множина T є підгрупа адитивної групи кільця M (2, z).

Нехай тепер $X\in M(2,\mathbb{Z})$ і $X=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, де $a,b,c,d\in\mathbb{Z}$ і $\mathbb{A}\in T$. Знайдемо добуток

$$XA=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix}=\begin{pmatrix} 0 & am\pm bn \\ 0 & an\pm dn \end{pmatrix}.$$

Оскільки $am+bn, cm+dn\in\mathbb{Z}$ і в матриці XA на місцях з номерами 11 і 21 стоять нулі, то $XA\in T$. Отже T – лівий

ідеал кільця $M(2,\mathbb{Z})$.

$$AX=\begin{pmatrix}0 & m\\ 0 & n\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}mc & md\\ nc & nd\end{pmatrix}\notin T.$$

Отже, Т не є правим ідеалом цього кільця.

*Відповід*ь: є лівим ідеалом.

№4. *Нехай m – довільне натуральне число. Знайти елементи кільця Z_m класів лишків за модулем m. Показати, що коли m не є простим числом, то Z_m не є полем.*

Розв'язання. Нагадаємо, що фактор-група $Z^+/(mZ)^+$ складається з елементів:

$$Z^+/(mZ)^+=\{(mZ)^+;\ 1+(mZ)^+;\ \dots;(m-1)+(mZ)^+\}.$$

Отже, фактор-кільце $Z_m=Z/mZ$ складається з таких елементів $Z_m=\{mZ;\ 1+mZ;\ \dots;(m-1)+mZ\}$.

$$(a+mZ)+(b+mZ)=c+mZ,$$
$$(a+mZ)(b+mZ)=d+mZ,$$

де c, d – відповідно остача від ділення $(a+b)$ і ab на m ($a, b \in \{0, 1, 2,\dots, m-1\}$).

Одиницею кільця Z_m є суміжний клас $1+mZ$.

Якщо m – не просте число, тоді Z_m не є полем, оскільки містить дільники нуля, які, як відомо, не є оборотними елементами. Дійсно, нехай $m=m_1m_2$ ($m_i \in N$, $m_i>1$, $i=1,2$). Тоді $m_i+mZ\neq mZ$ ($i=1,2$) і $(m_1+mZ)(m_2+mZ)=m_1m_2+mZ=mZ$.

№5. *Показати, що відображення $f: Z\to Z_m$, визначене за правилом $f(a)=a+mZ$ ($a \in Z$), є гомоморфним відображенням кільця Z на кільце Z_m.*

Розв'язання. Для довільних елементів $a, b \in Z$

$f(a+b)=(a+b)+mZ=(a+mZ)+(b+mZ)=f(a)+f(b)$;

$f(ab)=(ab)+mZ=(a+mZ)(b+mZ)=f(a)f(b)$.

Отже, відображення є гомоморфним.

№6. *З'ясувати, чи фактор-кільце $R[x]/(x^2+1)R[x]$ є полем.*

Розв'язання. Многочлен $\psi(x)=x^2+1$ не розкладається на лінійні множники у полі дійсних чисел, а, отже є простим елементом кільця $R[x]$. За теоремою задане фактор-кільце є полем.

Завдання для аудиторного заняття

№1. Які з заданих числових множин утворюють кільце відносно операцій додавання і множення?

а) $\mathbb{Z}$;

б) $\mathbb{Z}\left[-\sqrt{2}\right]$ *(множина чисел виду* $a+b\left(-\sqrt{2}\right)$, *де* $a,b\in\mathbb{Z}$ *);*

в) $m\mathbb{Z}[i]$ (*множина всіх чисел виду* $a+bi$, *де* $a, b \in m\mathbb{Z}$*);*

г) $\mathbb{Z}\left[\sqrt[3]{2}\right]$ (*множина всіх чисел виду* $a+b\sqrt[3]{2}$, *де* $a, b \in \mathbb{Z}$).

№2. Які з заданих множин матриць утворюють кільце відносно операцій додавання і множення? Які з кілець комутативні?

а) $M(n,N)$ – множина квадратних матриць *n-го* порядку, елементи яких є натуральні числа;

б) $\left\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} | a,b\in Q\right\}$;

в) $\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | a,b\in \mathbb{Z}\right\}$;

г) $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} | a,b\in \mathbb{Z}\right\}$;

д) $\left\{\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} | a,b\in \mathbb{Z}\right\}$;

е) $\left\{\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} | a,b\in Q\right\}$;

є) $\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} | a,b,c\in \mathbb{Z}\right\}$.

№3. Які із заданих множин пар цілих чисел $(a,b), a, b \in \mathbb{Z}$ утворюють кільце, якщо операції додавання і множення пар введено так (дві пари рівні, якщо рівні їхні однойменні компоненти):

а) $(a,b)+(c,d)=(ac,bd)$;
$(a,b)*(c,d)=(a+c,b+d)$;

б) $(a,b)+(c,d)=(a+c,b+d)$;
$(a,b)*(c,d)=(0,0)$;

в) $(a,b)+(c,d)=(ac,bd)$;
$(a,b)*(c,d)=(ab,cd)$;

г) $(a,b)+(c,d)=(a+c,b+d)$;
$(a,b)*(c,d)=(ac+3bd,ad+bc)$.

№4. Чи є полем множина всіх цілих чисел виду:

а) $a+b\sqrt[3]{3}$; б) $a+b\sqrt[3]{3}+c\sqrt[3]{9}$, *де* $a,b,c\in Q$.

№5. Чи є ідеалом (лівим, правим, двостороннім):

а) множина $m\mathbb{Z}$ в кільці $\mathbb{Z}$ (множина цілих чисел, кратних m);

б) множина $3\mathbb{Z}[i]$ (множина всіх чисел виду $3a + 3bi$, де $a, b \in \boldsymbol{Z}$) в кільці $\mathbb{Z}[i]$;

в) множина $\left\{\begin{pmatrix} m & n \\ 0 & 0 \end{pmatrix}\right\}$ в кільці $M(2, \boldsymbol{Z})$, якщо $m, n \in \boldsymbol{Z}$;

г) множина $\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in \mathbb{Z}\right\}$ в кільці $\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$;

д) множина $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{Z}\right\}$ в кільці $M(2, \boldsymbol{Z})$;

е) множина $\left\{\begin{pmatrix} 0 & d & e \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} \middle| d, e \in \mathbb{Z}\right\}$

в кільці $\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \middle| a, b, c \in \mathbb{Z}\right\}$;

ж) множина $\left\{\begin{pmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{pmatrix} \middle| g, h, k \in \mathbb{Z}\right\}$

в кільці $\left\{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \middle| a, b, c, d, e, f \in \mathbb{Z}\right\}$.

№6. Знайти всі елементи фактор-кілець:

а) Z_5;

б) $R[x]/(x+1)R[x]$.

№7. Чи буде відображення $f: x \to 2x$ гомоморфним відображення кільця цілих чисел в себе?

№8. З'ясувати, чи є полем фактор-кільця:

а) $Q[x]/(x^2-2)Q[x]$; б) $C[x]/(x^2+1)C[x]$.

Відповіді: ***№1.*** а) є кільцем; б) є кільцем; в) є кільцем; г) не є кільцем. ***№2***. а) не є кільцем; б) є комутативним кільцем; в) є кільцем, не комутативним; г) є комутативним кільцем; д) є кільцем, не комутативним; е) є комутативним кільцем; є) є комутативним кільцем. ***№3.*** а) є кільцем; б) є кільцем; в) не є кільцем; г) не є кільцем. ***№4***. а) не є полем; б) є полем. ***№5.*** а) є двостороннім ідеалом; б) є двостороннім ідеалом; в) є правим ідеалом; г) є двостороннім ідеалом; д) не є ідеалом; е) є двостороннім ідеалом; ж) є двостороннім ідеалом.

Завдання для самостійного розв'язування

№1. Які з заданих числових множин утворюють кільце відносно операцій додавання і множення?

а) $5\mathbb{Z}$ (множина цілих чисел , кратних 5);

б) $m\mathbb{Z}\left[\sqrt{2}\right]$ (множина чисел виду $a+b\sqrt{2}$, де $a,b\in m\mathbb{Z}$);

в) $\mathbb{Z}[i]$ (множина всіх чисел виду $a+bi$, де $a,b\in\mathbb{Z}$);

г) $\mathbb{Z}\left[\sqrt{2i}\right]$ (множина всіх чисел виду $a+b\left(i\sqrt{2}\right)$, де $a,b\in\mathbb{Z}$).

№2. Які з заданих множин матриць утворюють кільце відносно операцій додавання і множення? Які з кілець комутативні?

а) $M(n,\mathbb{Z})$ – множина квадратних матриць *n*-го порядку, елементи яких є цілі числа;

б) $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}$;

в) $\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}$;

г) $\left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\middle| a,b\in Q\right\}$;

д) $\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}$;

е) $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\middle| a,b\in Q\right\}$.

№3. Які із заданих множин пар цілих чисел $(a,b), a,b\in\mathbb{Z}$ утворюють кільце, якщо операції додавання і множення пар введено так (дві пари рівні, якщо рівні їхні однойменні компоненти):

а) $(a,b)+(c,d)=(a+c,b+d)$;

$(a,b)\cdot(c,d)=(a+b+c+d,0)$;

б) $(a,b)+(c,d)=(a+c,b+d)$;

$(a,b)\cdot(c,d)=(ac,bd)$;

в) $(a,b)+(c,d)=(a+c,b+d)$;

$(a,b)\cdot(c,d)=(ac+bd,ad+bc)$;

г) $(a,b)+(c,d)=(a+c,b+d)$;

$(a,b)\cdot(c,d)=(ac-3bd,ad+bc)$.

№4. Нехай у множині R^3 задано операції

$$(a,b,c)+(a_1,b_1,c_1)=(a+a_1,b+b_1,c+c_1),$$

$$(a,b,c)\cdot(a_1,b_1,c_1)=(aa_1-bb_1,ab_1+ba_1,ac_1+ca_1).$$

Чи є полем множина R^3?

№5. Чи є ідеалом (лівим, правим, двостороннім)

а) множина $2\boldsymbol{Z}[\sqrt{3}]$ (множина чисел виду $2a+2b\sqrt{3}$, де $a, b \in \boldsymbol{Z}$) в кільці $\boldsymbol{Z}[\sqrt{3}]$;

б) множина $\left\{\begin{pmatrix} m & 0 \\ n & 0 \end{pmatrix}\right\}$ в кільці $M(2,\boldsymbol{Z})$, якщо $m, n \in \boldsymbol{Z}$;

в) множина $\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\middle| a,b\in\mathbb{Z}\right\}$ в кільці $M(2,\boldsymbol{Z})$;

г) множина $\left\{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}\middle| a,b,c\in\mathbb{Z}\right\}$ в кільці $M(3,\boldsymbol{Z})$;

д) множина $\left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{pmatrix}\middle| a\in\mathbb{Z}\right\}$ в кільці $M(3,\boldsymbol{Z})$;

е) множина $\left\{\begin{pmatrix} 0 & l & 2m \\ 0 & 0 & 2n \\ 0 & 0 & 0 \end{pmatrix}\middle| l,m,n\in\mathbb{Z}\right\}$

в кільці $\left\{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}\middle| a,b,c,d,e,f\in\mathbb{Z}\right\}$.

№6. Знайти всі елементи фактор-кілець:

а) Z_6;

б) $R[x]/xR[x]$.

№7. Чи будуть ізоморфними кільця

$Z[\sqrt{2}] = \{a + b\sqrt{2} | a, b \epsilon Z\}$ та $Z[\sqrt{3}] = \{m + n\sqrt{3} | m, n \epsilon Z\}$.

№8. З'ясувати, чи є полем фактор-кільця:

а) $R[x]/xR[x]$;

б) $Z_2[x]/(x^2+1)Z_2[x]$.

Відповіді: ***№1***. а) є кільцем; б) є кільцем; в) є кільцем; г) є кільцем. ***№2***. а) є кільцем, не комутативним; б) є комутативним кільцем; в) є комутативним кільцем; г) є кільцем, не комутативним; д) є комутативним кільцем; е) є кільцем, не комутативним***.*** ***№3.*** а) не є кільцем; б) є кільцем; в) є кільцем; г) не є кільцем. ***№4***. не є полем. ***№5.*** а) є двостороннім ідеалом; б) є лівим ідеалом; в) не є ідеалом; г) не є ідеалом; д) не є ідеалом; е) є лівим ідеалом.

Тема третя
ТЕОРІЯ ПОДІЛЬНОСТІ

Означення й основні властивості подільності

У множині натуральних чисел N визначені операції додавання і множення, але не завжди здійсненні обернені їм операції віднімання й ділення. Щоб операція віднімання завжди була здійсненна, у математиці вводять число 0 і числа, протилежні натуральним числам – від'ємні числа: -1, -2, -3, ... Натуральні числа, протилежні їм та число 0 утворюють *множину цілих чисел,* яку ми позначатимемо буквою Z.

У множині цілих чисел визначені операції додавання і множення й здійсненна операція віднімання. Операції додавання і множення цілих чисел, як відомо, асоціативні, комутативні й пов'язані дистрибутивним законом. Отже, множина цілих чисел є комутативне кільце; його називають *кільцем цілих чисел.*

***Означення**. Якщо для цілих чисел a і b в кільці цілих чисел існує таке число q, що $a = bq$, то кажуть, що a ділиться на b або b ділить a і пишуть відповідно $a \vdots b$, b/a.* Число a при цьому називають *кратним* числа b, а b називають *дільником a.* Зрозуміло, якщо $a = bq$, то число q також є дільником числа a. Якщо в кільці Z не існує числа q, такого, що $a = bq$, то кажуть, що *a не ділиться* на b або *b не ділить a.*

Наведемо деякі властивості подільності цілих чисел, що випливають з означення.

Для будь-якого $a \in Z$:

1. $0 \vdots a = 0$.
2. $a \vdots a$, $a \vdots (-a)$, $a \vdots 1$, $a \vdots (-1)$.
3. $a \vdots b \to a \vdots (-b)$ і $(-a) \vdots b$ і $(-a) \vdots (-b)$.
4. $a \vdots b$ і $b \vdots c \to a \vdots c$.
5. $a \vdots c$ і $b \vdots c \to (a+b) \vdots c$ і $(a-b) \vdots c$.
6. $a \vdots b \to ac \vdots b$.
7. $a_1 \vdots c$ і $a_2 \vdots c$ ... $a_n \vdots c \to (a_1b_1+a_2b_2+...+a_nb_n) \vdots c$.

За властивістю 3 з подільності цілого числа a на ціле число b випливає подільність $\pm a$ на $\pm b$. Тому при вивченні

питання про подільність цілих чисел можна обмежитися розглядом лише цілих додатних чисел. Зокрема, всюди далі ми розглядатимемо лише додатні дільники цілих чисел.

Ділення з остачею

Важливу роль у теорії подільності цілих чисел відіграє така теорема.

Теорема (про ділення з остачею). *Які б не були ціле число a і натуральне число b, завжди існує єдина пара цілих чисел q і r, така, що a=bq+r, 0≤r<b.*

Число *q* називають *неповною часткою, r – остачею.*

Теорема*. Для будь-яких цілих чисел a і b, де b≠0, існує одна і тільки одна пара чисел q* і *r, така, що a=bq+r, 0≤r<|b|.*

Наслідок. *Ціле число a тоді і тільки тоді кратне цілому числу b≠0, коли остача від ділення a на b дорівнює нулю.*

Найбільший спільний дільник двох чисел і алгоритм Евкліда

Означення*. Ціле число* δ *називається спільним дільником цілих чисел a і b, якщо кожне з цих чисел ділиться на* δ*. Найбільший із спільних дільників чисел a і b називають найбільшим спільним дільником цих чисел* (скорочено НСД) *і позначають символом* (*a, b*) або НСД (*a*; *b*)*.*

Цілі числи *a* і *b,* найбільший спільний дільник яких дорівнює 1, називають *взаємно простими.*

Теорема. *Якщо ціле число a ділиться на натуральне число b, то множина спільних дільників чисел a і b збігається з множиною дільників числа b. Зокрема,* НСД (*a, b*) = *b.*

Теорема*. Якщо цілі числа a, b, q, r пов'язані співвідношенням a=bq+r, то множина спільних дільників чисел a і b збігається з множиною спільних дільників чисел b і r. Зокрема,* НСД (*a, b*) = НСД (*b, r*)*.*

Ще Евклід у книзі VII своїх «Начал» виклав спосіб знаходження НСД двох чисел, який відомий тепер як спосіб послідовного ділення, або алгоритм Евкліда. Полягає він ось у чому. Нехай *a* і *b* – натуральні числа. Якщо *a* не ділиться на *b,* то за теоремою про ділення з остачею *a* = = $bq_1 + r_1$, $0<r_1<b$. Якщо *b* не ділиться на r_1, то за цією самою

теоремою $b = r_1q_2 + +r_2$, $0<r_2<r_1$. Якщо r_1 не ділиться на r_2, то $r_1=r_2q_3+r_3$, $0<r_3<r_2$ і т. д. Цей процес послідовного ділення не може продовжуватись нескінченно, бо в противному разі множина натуральних чисел $r_1 > r_2 > r_3 > ... > r_{n-1} > r_n ...$ не матиме найменшого числа, а це суперечить принципу найменшого числа. Отже, існує таке n, що r_{n-1} ділиться на r_n. Процес послідовного ділення закінчиться через $n + 1$ кроків, і ми отримали таку систему рівностей:

$$a = bq_1 + r_1, b = r_1q_2 + r_2, r_1 = r_2q_3 + r_3, ...,$$

$$r_{n-1} = r_nq_{n+1}.$$

Розглядаючи ці рівності зверху вниз, на підставі теореми приходимо до висновку, що множина спільних дільників чисел a і b збігається з множиною спільних дільників чисел b і r_1, з множиною спільних дільників чисел r_1 і r_2, r_2 і r_3 і т. д. Отже, множина спільних дільників чисел a і b збігається з множиною спільних дільників чисел r_{n-1} і r_n, тобто за теоремою вона збігається з множиною дільників числа r_n.

Зокрема, $(a,b)=(b,r_1)=(r_1,r_2)=...=(r_{n-1}, r_n)=r_n$. Отже, ми довели таку теорему:

Теорема. НСД *чисел a і b дорівнює останній відмінній від нуля остачі* r_n *в алгоритмі Евкліда.*

З викладеного вище випливає також правильність такого твердження:

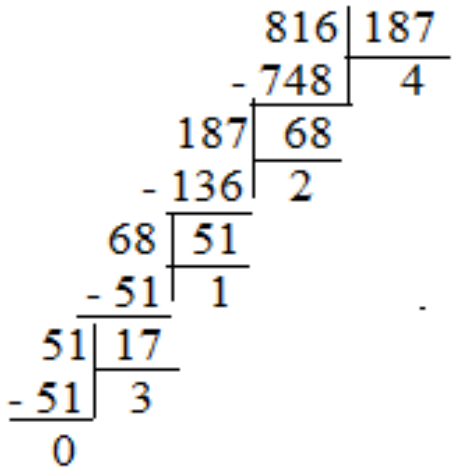
Теорема. *Множина спільних дільників чисел a і b збігається з множиною дільників* НСД (*a, b*) *цих чисел.*

З цієї теореми випливає такий наслідок: НСД *чисел a і b ділиться на будь-який їх спільний дільник.*

Очевидно також, що додатний спільний дільник чисел a і b, який ділиться на будь-який їх спільний дільник, є найбільшим серед спільних дільників цих чисел.

Виходячи з щойно викладеного, поняття найбільшого спільного дільника двох чисел можна означити так: *найбільшим спільним дільником чисел a і b називається такий додатний їх спільний дільник d, який ділиться на будь-який спільний дільник* δ *цих чисел.*

Приклад. Застосуємо алгоритм Евкліда для знаходження найбільшого спільного дільника чисел 816 і 187. Маємо:



Отже,

816=187·4 + 68, 187 = 68·2 + 51,

68 = 51·1 + 17, 51 = 17·3+0.

Остання відмінна від 0 остача дорівнює 17. Отже, (816, 187) = 17.

Теорема. *Якщо натуральні числа a і b помножити на натуральне число m, то їх* НСД *також помножиться на m, тобто* (*am, bm*) = (*a, b*) *m.*

Теорема*. Якщо натуральні числа a і b поділити на якийнебудь їх спільний дільник* δ, *то* НСД *цих чисел також поділиться на* δ.

З теорем випливають такі наслідки:

Наслідок 1. *Частки* (*a/d*) *і* (*b/d*) *від ділення чисел a і b на їх найбільший спільний дільник d взаємно прості.*

Наслідок 2. *Якщо частки* (*a/d*) *і* (*b/d*) *від ділення чисел a і b на їх спільний дільник d взаємно прості, то d є найбільший спільний дільник цих чисел.*

Найбільший спільний дільник кількох чисел

Якщо кожне з цілих чисел $a_1, a_2, ..., a_n$ ділиться на ціле число δ, то число δ називають *спільним дільником чисел* $a_1, a_2, ... a_n$. Найбільший із спільних дільників чисел $a_1, a_2, ..., a_n$ називають *найбільшим спільним дільником* цих чисел і позначають символом $(a_1, a_2, ..., a_n)$ або НСД $(a_1, a_2, ..., a_n)$.

Якщо найбільший спільний дільник чисел $a_1, a_2, ..., a_n$ дорівнює 1, то ці числа називають *взаємно простими.*

Якщо кожне з чисел $a_1, a_2, ..., a_n$ взаємно просте з будь-яким іншим з них, то числа $a_1, a_2, ..., a_n$ називають *попарно взаємно простими.*

З означень безпосередньо випливає, що коли числа $a_1, a_2, ..., a_n$ попарно взаємно прості, то вони і взаємно прості.

Обернене твердження неправильне.

Наприклад. Числа 15, 10, 13 – взаємно прості, але не попарно взаємно прості, бо (15, 10) = 5.

У випадку двох чисел поняття «попарно взаємно прості» збігається з поняттям «взаємно прості».

Нехай $a_1, a_2, ..., a_n$ – будь-які цілі числа, серед яких принаймні одне відмінне від 0. Введемо такі позначення:

$(a_1, a_2) = d_2, (d_2, a_3) = d_3, ..., (d_{n-2}, a_{n-1}) = d_{n-1}, (d_{n-1}, a_n) = d_n$.

Теорема. *Множина спільних дільників чисел $a_1, a_2, a_3, ..., a_n$ збігається з множиною дільників числа d_n.*

Теорема. *Число d_n є найбільшим спільним дільником чисел $a_1, a_2, ..., a_n$.*

Отже, задача знаходження найбільшого спільного дільника чисел $a_1, a_2, ..., a_n$ зводиться до знаходження чисел $d_2, d_3, ..., d_{n-1}, d_n$, тобто до знаходження найбільшого спільного дільника двох чисел.

Оскільки множина спільних дільників чисел $a_1, a_2, ..., a_n$ збігається з множиною дільників їх найбільшого спільного дільника d, то *найбільший спільний дільник d чисел $a_1, a_2, ..., a_n$ ділиться на будь-який спільний дільник δ цих чисел.* З другого боку, додатний спільний дільник чисел $a_1, a_2, ..., a_n$, який ділиться на будь-який їх спільний дільник, є найбільшим серед спільних дільників цих чисел. Отже, *найбільшим спільним дільником чисел $a_1, a_2, ..., a_n$ називається додатний спільний дільник цих чисел, який ділиться на будь-який їх спільний дільник.*

Взаємно прості числа

Теорема. $\forall a, b, c \in Z: \text{НСД}(a, b) = 1 \rightarrow \text{НСД}(ac, b) = \text{НСД}(c, b)$.

Теорема. *Якщо число a взаємно просте з кожним з чисел b і c, то a взаємно просте й з добутком bc.*

Цю теорему можна узагальнити так: *якщо число a взаємно просте з кожним з чисел $b_1, b_2, ..., b_n$, то a взаємно*

просте й з добутком цих чисел $b_1b_2...b_n$.

Теорема. *Якщо добуток ab ділиться на c, причому b і c взаємно прості, то a ділиться на c.*

Теорема. *Якщо a ділиться на кожне з чисел b і c, причому b і c взаємно прості, то a ділиться і на добуток bc.*

Найменше спільне кратне

Нехай $a_1, a_2, ..., a_n$ – будь-які цілі числа. Числа $a_1a_2 ... a_n$, , $2a_1\ a_2 ... a_n$, $3a_1\ a_2 ... a_n$, ..., $ma_1\ a_2 ... a_n$ діляться на кожне з чисел $a_1, a_2, ..., a_n$. Отже, існує нескінченна множина цілих чисел, які діляться на $a_1, a_2, ..., a_n$.

Означення. *Ціле число, яке ділиться на кожне з чисел $a_1, a_2, ..., a_n$, називають спільним кратним цих чисел.*

Найменше з додатних спільних кратних чисел $a_1, a_2, ..., a_n$ називають *найменшим спільним кратним* цих чисел.

Найменше спільне кратне чисел $a_1, a_2, ..., a_n$ (скорочено НСК) позначають *символом* $[a_1, a_2, ..., a_n]$ або НСК $[a_1, a_2, ..., a_n]$.

З'ясуємо насамперед як знайти найменше спільне кратне двох натуральних чисел *a* і *b.*

Нехай *M* – будь-яке спільне кратне натуральних чисел *a* і *b.* Оскільки *M* ділиться на *a,* то $M = a \cdot k$, де *k* – деяке ціле число. Але *M* ділиться також і на *b.* Тому $\frac{M}{b} = \frac{ak}{b}$ – також є деяке ціле число.

Позначимо НСД (*a, b*) чисел *a* і *b* через *d.* Тоді $a=a_1d$, $b=b_1d$,

$$\frac{M}{b} = \frac{ak}{b} = \frac{a_1dk}{b_1d} = \frac{a_1k}{b_1}.$$

Оскільки $\frac{a_1k}{b_1}$ є ціле число і числа a_1 і b_1 взаємно прості НСД $(a_1, b_1)=1$, то *k* ділиться на b_1, тобто

$k = b_1 \cdot t = \frac{b}{d} \cdot t$, *де t* – деяке ціле число.

З викладеного вище випливає, що $M = \frac{ab}{d} \cdot t$.

Теорема. *Найменше спільне кратне натуральних чисел a і b дорівнює добутку цих чисел, поділеному на їх найбільший спільний дільник, тобто*

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

Найменше спільне кратне чисел *a* і *b* позначимо через *m.* Тоді формулу запишемо так: *M = m • t.*

Звідси випливає правильність такої теореми:

Теорема*. Будь-яке спільне кратне M чисел a і b ділиться на їх найменше спільне кратне* НСК [*a, b*].

Розглянемо питання про знаходження найменшого спільного кратного натуральних чисел a_1, a_2, ..., a_n при $n > 2$.

Введемо такі позначення:

$$\text{НСК } [a_1, a_2] = m_2, \text{НСК } [m_2, a_3] = m_3,$$

$$\dots, \text{НСК } [m_{n-1}, a_n] = m_n.$$

Теорема. *Множина спільних кратних чисел a_1, a_2, ..., a_n збігається з множиною кратних числа m_n.*

Теорема*. Число m_n є найменшим спільним кратним чисел a_1, a_2,..., a_n.*

Таким чином, знаходження найменшого спільного кратного кількох чисел зводиться до знаходження найменшого спільного кратного двох чисел.

Приклад. Знайти НСК [245, 147, 84].

Знаходимо спочатку НСК [247, 147]. Як відомо, $\text{НСК } [245, 147] = \frac{245 \cdot 147}{\text{НСД } (245,147)}$.

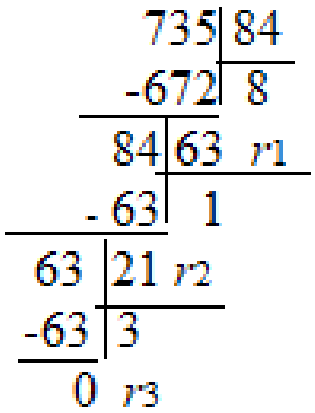
Застосовуючи алгоритм Евкліда, знаходимо:

$$\begin{array}{r|l} 245 & 147 \\ \hline -147 & 1 \\ \hline 147 & 98 \quad r1 \\ \hline -98 & 1 \\ \hline 98 & 49 \quad r2 \\ \hline -98 & 2 \\ \hline 0 \quad r3 & \end{array}$$

Отже, НСД (245, 147) =49.

Тоді, НСК [245, 147] =735.

Знайдемо тепер НСК [245, 147, 84]. За теоремою, $\text{НСК } [245, 147, 84] = \text{НСК } [735, 84] = \frac{735 \cdot 84}{\text{НСД } (735,84)}$



Отже, НСД (735, 147) =21.

НСК $[245, 147, 84] = \frac{735 \cdot 84}{21} = 2940.$

Прості числа

Означення. *Відмінне від* 1 *натуральне число а називають простим, якщо воно не має дільників, відмінних від* 1 *і а. Його називають складеним, якщо воно має дільники, відмінні від* 1 *і а.*

Простими є, *наприклад*, числа 2, 7, 13; числа 4, 9, 15 – складені. Число **1 не належить** ні до простих, ні до складених чисел.

Теорема*. Всяке натуральне число а або ділиться на дане просте число р, або взаємно просте з р.*

Теорема. *Якщо добуток кількох натуральних чисел ділиться на просте число р, то принаймні один із співмножників ділиться на р.*

Теорема*. Найменший відмінний від* 1 *дільник більшого від* 1 *натурального числа а є число просте.*

Теорема. *Найменший відмінний від одиниці дільник складеного числа а не більший за* $\sqrt{a}$ *.*

Нескінченість множини простих чисел. Решето Ератосфена

***Теорема* (*Евкліда*).** *Множина простих чисел нескінченна.*

Природно постає запитання: як у ряду натуральних чисел виділити всі прості числа?

Таблицю всіх простих чисел, що не перевищують даного натурального числа *М*, можна скласти так. Випишемо

підряд усі натуральні числа від 2 до M: 2, 3, 4, 5, ... , M.

Далі закреслимо в ряду всі числа, кратні 2, крім самого числа 2. Першим числом у ряду, яке залишилося після цього, є число 3. Число 3 не ділиться на 2, бо в противному разі ми закреслили б його: отже, число 3 ділиться лише на 1 і на самого себе, тому воно просте. Закреслимо тепер у ряду всі числа, кратні 3, крім самого числа 3. Першим числом, яке залишилося після цього в ряду, є число 5; воно не ділиться ні на 2, ні на 3, бо в противному разі воно виявилося б закресленим; отже, 5 ділиться тільки на 1 і на самого себе, тому воно просте число і т.д.

Уперше для складання таблиць простих чисел описаний щойно метод застосував грецький математик Ератосфен. Він записував числа на папері, але їх не закреслював, а проколював. Внаслідок цього він отримував дещо схоже на решето: складені числа «просіювалися» крізь це решето, а прості числа залишалися. Тому цей метод називають *решетом Ератосфена.*

Метод Ератосфена поступово удосконалювався, завдяки чому складання таблиць простих чисел спрощувалося. Це, в свою чергу, дало можливість скласти таблиці простих чисел, що містять порівняно велику кількість чисел. Тепер складено таблиці простих чисел приблизно до 10 мільйонів.

Основна теорема арифметики

Розглянемо тепер теорему, яка відіграє фундаментальну роль як у теорії подільності, так і в усій теорії чисел, її називають основною теоремою арифметики.

***Теорема* (*Основна теорема арифметики*).** *Кожне відмінне від* 1 *натуральне число n можна записати у вигляді добутку простих чисел і притому єдиним способом, якщо не брати до уваги порядку розміщення співмножників.*

Запис $n = p_1p_2 \dots p_s$ натурального числа n у вигляді добутку простих чисел $p_1, p_2, \dots, p_s$ називають також *розкладом* числа n у добуток простих множників, або *розкладом на прості множники*.

Основна теорема арифметики показує, що всі натуральні числа отримують з простих чисел за допомогою

операції множення: кожне натуральне число (складене) – є деякий добуток простих чисел, причому різні добутки дають різні числа. Тепер зрозуміло, чому одиницю не слід вважати простим числом: віднісши 1 до простих чисел, ми порушили б єдиність розкладу числа в добуток простих чисел, оскільки до будь-якого добутку можна приєднати множником 1.

Канонічний розклад складеного числа

У розкладі $n = p_1 p_2 \ldots p_s$ натурального числа n на прості множники $p_1, p_2, \ldots, p_s$ деякі з цих множників можуть повторюватись. Якщо простий множник p_i повторюється в розкладі k раз, то його називають *k-кратним множником числа n,* або кажуть, що множник p_i має кратність k.

Позначимо символами $p_1\ p_2, \ldots, p_m$ $(m \le s)$ різні множники в розкладі. Нехай множник p_i $(i = 1, 2, \ldots, m)$ має кратність k_i. Тоді розклад числа n у добуток простих множників можна записати так:

$$n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}.$$

Цей запис називають *канонічним розкладом числа n на прості множники, або канонічним зображенням числа n.*

Оскільки число n єдиним способом записується у вигляді добутку простих чисел, то й канонічне зображення числа n існує тільки одне.

Приклад. Знайти канонічний розклад числа 12600.

Маємо: 12600=126·100

12600	2·2·5·5 (100)
126	2
63	3
21	3
7	7
1	

12 600 = 2·2·2·3·3·5·5·7 = $2^3 \cdot 3^2 \cdot 5^2 \cdot 7$.

З єдиності канонічного зображення числа випливає правильність такого твердження.

Теорема. *Якщо* $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$ *– канонічний розклад числа n, то всі дільники цього числа збігаються з числами*

вигляду $d = p_1^{s_1} p_2^{s_2} \dots p_m^{s_m}$, де $0 \le s_i \le k_i$, $i = 1, 2 \dots m$.

Візьмемо тепер довільні два натуральні числа a і b. Припустимо, що вони мають такі канонічні розклади:

$$a = r_1^{l_1} r_2^{l_2} \dots r_m^{l_m}, \; b = q_1^{s_1} q_2^{s_2} \dots q_t^{s_t}.$$

Позначимо символами $p_1 p_2 \dots p_s$ всі різні множники, кожен з яких входить до розкладу принаймні одного з чисел a і b. Якщо простий множник p_i не зустрічається в розкладі якого-небудь з чисел a і b, то вважатимемо, що він входить до цього розкладу в нульовому степені. За цієї умови канонічні розклади чисел a і b можна записати так: $a = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $b = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$, де кожен з показників k_i і m_i, $i = 1, 2, \dots, s$, є ціле невід'ємне число. Для чисел a і b правильні такі твердження.

***Теорема**. Найбільшим спільним дільником чисел a і b є число* НСД $(a, b) = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, *де* $l_i = \min(k_i, m_i)$, $i = 1, 2, \dots, s$.

Теорема. *Найменшим спільним кратним чисел a і b є число* НСК $[a, b] = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, *де* $n_i = max(k_i, m_i)$, $i = 1, 2, \dots, s$.

Теореми поширюються на будь-яке скінченне число натуральних чисел. Зауважимо, що з цих теорем випливають відомі читачеві з шкільного курсу математики правила знаходження найбільшого спільного дільника і найменшого спільного кратного кількох чисел.

Щоб знайти НСД *даних чисел, треба кожне з цих чисел розкласти в добуток простих множників і взяти добуток спільних простих множників з найменшими показниками, з якими вони входять у всі розклади.*

Щоб знайти НСК *даних чисел, потрібно кожне з них розкласти в добуток простих множників і взяти добуток усіх простих множників з найбільшими показниками, з якими вони входять у всі розклади.*

Подільність в області цілісності

В теорії кілець особливої уваги заслуговують кільця, які за своїми властивостями досить близькі до кільця цілих чисел. Зокрема, для цих кілець можна розвинути теорію подільності, аналогічну теорії подільності цілих чисел. Ці кільця отримали назву *кілець головних ідеалів.*

Нехай K – область цілісності з одиницею. Оскільки область цілісності – комутативне кільце, то в ній поняття правого і лівого дільника елемента збігаються і тому означення подільності формулюється так.

Означення. *Якщо для елементів a і b області цілісності R в R існує такий елемент c, що a=bc, то говорять, що a ділиться на b, або b ділить a і пишуть відповідно* $a \vdots b$; b/a або $a \equiv 0 \pmod b$.

Як бачимо, це означення є поширенням на область цілісності означення подільності в кільці цілих чисел, яке є конкретним прикладом області цілісності.

З означення випливають такі *властивості подільності в області цілісності*: $\forall a, b, c \in R$:

1. $a \vdots b$ *і* $b \vdots c \rightarrow a \vdots c$.
2. $a \vdots c$ *і* $b \vdots c \rightarrow (a+b) \vdots c$ *і* $(a-b) \vdots c$.
3. $a \vdots b \rightarrow ac \vdots b$.
4. $a_1 \vdots c, a_2 \vdots c \ldots a_n \vdots c \rightarrow (a_1 b_1 + a_2 b_2 + \cdots + a_n b_n) \vdots c$.
5. Кожен елемент $a \in R$ ділиться на будь-який дільник ε одиниці $\boldsymbol{e}$.
6. Якщо $a \in R$ ділиться на $b \in R$, то a ділиться і на $b\varepsilon$, де ε – будь-який дільник одиниці.
7. Кожен з дільників одного з елементів $a \in R$ і $a\varepsilon \in R$, де ε – будь-який дільник одиниці, є дільником і іншого.

Всюди далі будемо розглядати елементи області цілісності R, відмінні від нуля.

Означення*. Елементи a і b області цілісності R називаються асоційованими, якщо кожен з них є дільником іншого: a=bc, b=ad.*

Означення*. Елементи a і b області цілісності R називаються асоційованими, якщо b=aε , де ε – деякий дільник одиниці.*

В кільці цілих чисел, наприклад, асоційованими є кожні два числа m і $(-m)$.

Таким чином, два асоційовані елементи a і b породжують той самий головний ідеал.

Нехай a і b – довільні елементи області цілісності R.

Означення*. Елемент c ∈ R називається спільним дільником елементів a і b, якщо кожен з цих елементів ділиться на c.*

За властивістю 5, всі дільники одиниці ***e*** області цілісності R є спільними дільниками елементів a і b. Але в елементів a і b можуть бути і інші спільні дільники. Означення НСД двох цілих чисел, за яким найбільшим спільним дільником називають найбільший із спільних дільників, поширити на область цілісності не можна, оскільки в довільній області цілісності R немає відношення порядку. Проте відомо й інше означення НСД двох чисел, а саме: НСД двох чисел називають такий спільний дільник цих чисел, який ділиться на будь-який інший їхній спільний дільник. Саме це означення можна поширити на область цілісності.

***Означення**. Найбільшим спільним дільником елементів a і b області цілісності R називається такий спільний дільник цих елементів, який ділиться на будь-який інший їхній спільний дільник.*

Щоб зазначити, що d є найбільший спільний дільник елементів a і b, пишуть $d=(a,b)$.

Якщо також $d'=(a, b)$, то елементи d і d' діляться один на одного і, отже, вони асоційовані. З другого боку, якщо $d=(a, b)$ і ε – будь-який дільник одиниці, то, очевидно, $d\varepsilon=(a, b)$. Отже, найбільший спільний дільник елементів a і b визначається з точністю до множника ε, що є дільником одиниці.

***Означення**. Елементи $a, b \in R$ називаються взаємно простими, якщо вони не мають спільних дільників, відмінних від дільників одиниці, тобто якщо* $(a, b)=1$.

Нехай ε – будь-який дільник одиниці і a – довільний елемент області цілісності R. Всі дільники елемента a, відмінні від $a\varepsilon$ і ε, якщо такі існують, називають нетривіальними, або власними. Так, в кільці цілих чисел тривіальними дільниками числа 10 є числа ±1, ±10 і нетривіальними – числа ±2, ±5.

***Означення**. Елемент $a \in R$ називається нерозкладним, або простим, якщо він не є дільником одиниці й не має нетривіальних дільників; елемент $a \in R$ називається розкладним, або складеним, якщо він має нетривіальні дільники.*

Інакше кажучи, елемент $a \in R$ називається розкладним, якщо його можна записати у вигляді добутку $a=bc$ двох

нетривіальних множників b і c; він називається нерозкладним, якщо його не можна записати у вигляді добутку двох нетривіальних дільників.

Наведемо такі дві властивості нерозкладних елементів.

1) Якщо елемент $p \in R$ нерозкладний, то і будь-який асоційований з ним елемент $p\varepsilon$ є також нерозкладний.
2) Якщо a – будь-який, ap – нерозкладний елемент з R, то або a ділиться на p, або a і p – взаємно прості.

Кільце головних ідеалів

Означення. *Кільцем головних ідеалів називається область цілісності з одиницею, в якій кожен ідеал є головний.*

Найпростішим *прикладом* кілець головних ідеалів є кільце цілих чисел Z: кільце Z є область цілісності з 1 і кожен його ідеал головний.

Всюди далі вважатимемо, що R – кільце головних ідеалів.

Теорема. *Будь-які два елементи a і b кільця головних ідеалів R мають найбільший спільний дільник d, причому $d = ra + sb$, де r і s – деякі елементи кільця R.*

Теорема. *Елементи a і b кільця головних ідеалів R взаємно прості тоді і тільки тоді, коли в кільці R є такі елементи r і s, що $ra + sb = 1$.*

Теорема. *Якщо елемент $a \in R$ взаємно простий з кожним із елементів $b \in R$ і $c \in R$, то він взаємно простий і з добутком цих елементів.*

Теорема. *Якщо добуток елементів $a \in R$ і $b \in R$ ділиться на елемент $c \in R$, але a і c взаємно прості, то b ділиться на c.*

Теорема. *Якщо елемент $a \in R$ ділиться на кожен з елементів $b \in R$ і $c \in R$, які між собою взаємно прості, то a ділиться і на добуток bc.*

Теорема. *Якщо R – кільце головних ідеалів і p – простий елемент цього кільця, то фактор-кільце $K/(p)$* є поле.

Наслідок. *Якщо добуток кількох елементів кільця головних ідеалів R ділиться на простий елемент $p \in R$, то принаймні один із співмножників ділиться на p.*

Теорема. *В кільці головних ідеалів R кожен відмінний від нуля елемент, що не є дільником одиниці, розкладається в добуток простих множників.*

Теорема*. Якщо* $a=p_1p_2p_3...p_r=q_1q_2...q_s$ *є два розклади елемента a кільця головних ідеалів R в добуток простих множників, то* $r = s$ *і, при відповідній нумерації співмножників, справджуються рівності* $q_i= \varepsilon_i p_i$ ($i = =1, 2, ..., r$), *де* ε_i *– деякий дільник одиниці кільця R.*

Є області цілісності, в яких **не справджується** теорема про розклад елементів області цілісності в добутки простих множників, а також області цілісності, в яких розклад елементів на прості множники хоч і можливий, але не однозначний. Наведемо приклади таких областей цілісності, не вивчаючи їх докладно.

Нехай *К* – множина всіх дійсних чисел виду

$$c = a_1 2^{r_1} + a_2 2^{r_2} + \cdots + a_n 2^{r_n},$$

де *n* – будь-яке натуральне число, $a_1, a_2, ..., a_n$ – будь-які цілі числа й $r_1, r_2, ...r_n$ – будь-які числа виду $\frac{m}{2^k}$ (m, k - цілі невід'ємні числа). Сума, різниця й добуток чисел такого виду – числа такого самого виду. Отже, *К* – кільце. Коли $n = = 1$ і $r_1 = 0$ маємо $c = a_1$; тому *К* містить усі цілі числа, зокрема 1. Легко бачити, що кільце *К* є область цілісності. У цій області цілісності число 2 розкладається на множники так:

$$2 = 2^{\frac{1}{2}}2^{\frac{1}{2}} = 2^{\frac{1}{2}}2^{\frac{1}{4}}2^{\frac{1}{4}} = 2^{\frac{1}{2}}2^{\frac{1}{4}}2^{\frac{1}{8}}2^{\frac{1}{8}} = \cdots.$$

Можна довести, що числа виду $2^{\frac{1}{2^k}}$, де k – ціле невід'ємне число, не є дільниками одиниці в кільці *К*. Таким чином, число 2 не можна розкласти на прості множники в кільці *К*.

Евклідові кільця

Порівняно з кільцями головних ідеалів більш близькими до кільця цілих чисел за своїми властивостями є кільця, в яких істинна теорема, що є аналогом теореми

про ділення з остачею в кільці цілих чисел. Ці кільця називають *евклідовими.* Вони означаються так.

***Означення**. Область цілісності R з одиницею називається евклідовим кільцем, якщо існує відображення φ множини відмінних від* 0 *елементів цієї області цілісності в множину цілих невід'ємних чисел N^0, тобто* $\varphi: R/\{0\} \to N^0$ *, яке задовольняє таку вимогу: для будь-яких елементів a, b ∈ R, b≠0 в R існують такі елементи q і r, що a = bq+r, причому або r =* 0, *або* $\varphi(r)<\varphi(b)$.

Кільце цілих чисел *Z* – евклідове; відображення *φ*, про яке йде мова в означенні, задається так: $\varphi(a)=|a|$, для всіх $a\neq 0$. Евклідовим також є кільце многочленів від невідомого *x* з коефіцієнтами з поля *P.*

***Теорема**. Кожне евклідове кільце R є кільцем головних ідеалів.*

Зауважимо, що обернене твердження неправильне: існують кільця головних ідеалів, які не є евклідовими.

Методу, який би давав змогу відшукати найбільший спільний дільник будь-яких двох елементів *a* і *b* довільного кільця головних ідеалів *R*, не існує. В евклідових же кільцях його можна відшукати за допомогою відомого алгоритму Евкліда. Справді, нехай a_0 і a_1 – будь-які відмінні від нуля елементи евклідового кільця *R* і нехай $\varphi(a_0)\geq\varphi(a_1)$. Тоді, за означенням евклідового кільця, в *R* існують такі елементи q_1 і a_2, що $a_0 = a_1q_1 + a_2$, причому або $a_2 = 0$, або $\varphi(a_1)>\varphi(a_2)$. Якщо $a_2\neq 0$, то в *R* існують такі елементи q_2 і a_3, що $a_1 = a_2q_2 + a_3$, причому або $a_3 = 0$, або $\varphi(a_2)>\varphi(a_3)$. Якщо $a_3\neq 0$, то в *R* існують такі елементи q_3 і a_4, що $a_2 = a_3 q_3 + a_4$ і т. д.

Оскільки $\varphi(a_1)>\varphi(a_2)>\ldots>\varphi(a_{s-1})>\varphi(a_s)>\ldots$, то цей процес послідовного ділення не може продовжуватись нескінченно: в противному разі множина цілих невід'ємних чисел не мала б найменшого числа. Отже, через кілька кроків ми дійдемо до ділення з остачею рівною нулю: $a_{m-1}=a_mq_m$. Таким чином, ми матимемо рівності

$$a_0 = a_1q_1 + a_2$$

$$a_1 = a_2q_2 + a_3$$

…

$$a_{m-2} = a_{m-1}q_{m-1} + a_m$$

$$a_{m-1} = a_m q_m .$$

Остання рівність означає, що a_m є дільником a_{m-1}. Оскільки кожен з доданків правої частини передостанньої рівності ділиться на a_m, то і її ліва частина ділиться на a_m, тобто a_m є дільником a_{m-2}. Аналогічними міркуваннями ми доведемо, що a_m є дільником a_{m-3}, a_{m-4}, ..., a_2, a_1, a_0. Отже, a_m є спільним дільником елементів a_0 і a_1. Покажемо тепер, що a_m ділиться на будь-який спільний дільник елементів a_0 і a_1. Нехай b – довільно вибраний спільний дільник a_0 і a_1. Тоді з рівності $a_0 = a_1q_1 + a_2$ випливає, що a_2 ділиться на b, з рівності $a_1 = a_2q_2 + a_3$ випливає, що a_3 ділиться на b і т. д. Нарешті, з рівності $a_{m-2}=a_{m-1}q_{m-1}+a_m$ випливає, що a_m ділиться на b. Таким чином, елемент a_m є спільним дільником елементів a_0 і a_1 і ділиться на будь-який спільний дільник цих елементів, тобто *a_m є найбільшим спільним дільником елементів a_0 і a_1.*

Приклади розв'язування типових завдань

№1. *При діленні цілого числа a на* 17 *неповна частка дорівнює* 13*. Знайти найбільше значення a.*

Розв'язання. За умовою $a=17\cdot13+r$, де r – остача від ділення, $0\le r<17$. Максимального значення a набуде, якщо $r=16$, отже $a=17\cdot13+16=237$.

*Відповід*ь: *a=2*37.

№2. *При діленні цілого числа a=50 на b остача дорівнює r=6. Знайти b та неповну частку.*

Розв'язання. За умовою $50=bq+6$, $0\le r<b$, $6<b$.

$bq=50-6$, $bq=44$. Знайдемо дільники числа 44.

$44=2\cdot2\cdot11$.

Тоді, оскільки $b>6$, то $b=11$, 22 або 44. Тоді q відповідно буде дорівнювати 4, 2 або 1.

Відповідь: (b, q): (11, 4), (22, 2), (44, 1).

№3. *Знайти неповну частку і остачу від ділення цілого числа a на ціле число, якщо:*

а) a=37, b=8; б) a=-8, b= 37.

Розв'язання. Щоб знайти неповну частку і остачу від ділення треба знайти найбільше ціле число k, яке кратне b і не перевищує a. Тоді неповну частку q отримують як частку від ділення k на b, а остачу r – як різницю між a і k.

а) a=37, b=8.

k =32=8·4= b· q, q=4, r=37-32=5,

37=8·4+5;

б) a=-8, b= 37.

k =-37=37· (-1)= b· q, q=-1, r=-8-(-37)=29;

-8=37· (-1)+29.

Відповідь: а) q=4, r=5; б) q=-1, r=29.

№4. *Довести, що* $n(n+1)(2n+1) \vdots 6$ при довільному натуральному n.

Доведення. Перший метод – метод математичної індукції.

1) Нехай n=1, тоді $1(1+1)(2+1)=6 \vdots 6$.
2) Припустимо, що при $n=k$ твердження істинне: $k(k+1)(2k+1) \vdots 6$. Доведемо справедливість і при $n=k+1$. Тобто $(k+1)(k+2)(2k+3) \vdots 6$.

$$(k+1)(k+2)(2k+3) = k(k+1)(2k+1) + 6(k+1)^2.$$

Тоді твердження доведено.

3) $n(n+1)(2n+1) \vdots 6$ при довільному натуральному n.

Другий метод – метод повної індукції.

Оскільки $n(n+1)$ є добуток двох послідовних натуральних чисел, то він ділиться на 2. Оскільки 6=2·3, а числа 2 і 3 не мають спільних дільників, то для того, щоб $n(n+1)(2n+1) \vdots 6$, треба показати, що $n(n+1)(2n+1) \vdots 3$. За теоремою про ділення з остачею можливі такі випадки:

$$\text{а) } n = 3k; \quad \text{б) } n = 3k+1; \quad \text{в) } n = 3k+2,$$

де k – деяке ціле невід'ємне число.

а) $3k\,(3k+1)(6k+1) \vdots 3$;

б) $(3k+1)(3k+2)(6k+3) \vdots 3$;

в) $(3k+2)(3k+3)(6k+5) \vdots 3$.

Отже, $n(n+1)(2n+1)\vdots 3$.

А значить $n(n+1)(2n+1)\vdots 6$.

Третій метод – штучний.

Оскільки

$$n(n+1)(2n+1) = n(n+1)[(n-1)+(n+2)] = \\ = (n-1)n(n+1) + n(n+1)(n+2),$$

а кожний доданок є добутком трьох послідовних чисел, то він ділиться на число 6.

№5. *Просте чи складене число* 323*?*

Розв'язання. Відомо, що натуральне число n більше за 1 є простим тоді і тільки тоді, коли воно не ділиться на жодне з простих чисел, які не перевищують $\sqrt{n}$. $\sqrt{328} \approx 18$, випишемо всі прості числа менші за 18: 2, 3, 5, 7, 11, 13, 17. Перевіряємо чи ділиться число 323 на кожне із цих чисел. За ознаками подільності на 2, 3, 5, 11 число 323 не ділиться. Безпосередньо діленням перевіряємо подільність на 13 – число не ділиться, на 17 – ділиться. Отже, число 323 не є простим.

*Відповід*ь: число 323 є складеним.

Зауваження. Якщо існує точне значення $\sqrt{n} = k, k \in N$, то n є складеним числом, бо ділиться на k.

№6. *Знайти натуральні числа m і n, якщо:*

$$\begin{cases} m + n = 168, \\ (m, n) = 24. \end{cases}$$

Розв'язання. Скористаємося властивостями спільного дільника: якщо НСД $(a,b)=d$, $a=da_1$, $b=db_1$, то НСД $(a_1,b_1)=1$. За умовою $(m, n)=24$, $m=24m_1$, $n=24n_1$, НСД $(m_1,n_1)=1$. За умовою $m+n=168$, $24m_1+24n_1=168$, $m_1+n_1=7$. Оскільки НСД $(m_1, n_1)=1$, то маємо такі варіанти: $(m_1, n_1)=(6; 1)$, $(m_1,n_1)=(2; 5)$, $(m_1, n_1)=(3; 4)$ та навпаки. Тоді самі числа m і n дорівнюють відповідно: 144 і 24, 48 і 120, 72 і 96 і навпаки.

№7. *Яку найбільшу кількість однакових букетів можна скласти із 24 волошок і 32 ромашок, використавши всі квіти?*

Розв'язання. Кількість букетів повинна бути спільним дільником чисел 24 і 32.

$24=2\cdot2\cdot2\cdot3=2^3\cdot3$ $32=2\cdot2\cdot2\cdot2\cdot2=2^5$.

Отже, найбільша кількість букетів є 2^3=8.

Тоді у кожному букеті буде по три волошки і 4 ромашки.

Завдання для аудиторного заняття

№1. Знайти неповну частку і остачу при діленні цілого числа a на ціле число b, якщо:

а) a=131, b=31;

б) a=31, b=131;

в) a=-131, b=31.

№2. При діленні цілого числа a на ціле число b дістають неповну частку q і остачу r. Знайти b і q, якщо:

а) a=100, r=6; б) a=148, r=37; в) a=298, r=10.

№3. При діленні цілого числа a на ціле число b утворюється неповна частка q остача r. Знайти b і r, якщо:

а) a = 371, q= 14; б) a = 826, q=83; в) a= 441, q=25.

№4. Довести, що:

а) з трьох послідових цілих чисел одне і тільки одне ділиться на 3;

б) з двох послідовних парних цілих чисел одне і тільки одне ділиться на 4;

в) добуток двох послідовних цілих чисел ділиться на 2;

г) добуток трьох послідовних цілих чисел ділиться на 6.

№5. Довести, що для довільних натуральних чисел n:

а) $\left(n^3-n\right)\vdots 6$;

б) $\left(n^5-n\right)\vdots 30$;

в) $(n^5-5n^3+4n)\vdots 120$.

№6. Чи є числа 127, 919, 1033, 1643, 1657, 2647, 2773, 3163, 3621 простими?

№7. Знайти канонічний розклад числа n, якщо:

а) n = 160; б) n =494; в) n =1800; г) n= 3551.

№8. Довести, що дане число a є складеним:

а) $a=20^{30}-1$;

б) $a=n^4+4, n\neq \pm 1$;

в) $a=n^4+n^2+1, n>1$;

№9. Знайти найбільший спільний дільник чисел:

а) -231 і 546;

б) 1001 і 6253;

в) 1066 і 1970;

г) 3763 і 3337;

д) 6791400 і 178500;

е) Т та Н, де Т – номер телефону деканату, а Н – рік заснування факультету;

є) двох послідовних цілих чисел n і n+1;

ж) 819, 702 і 689; з)2737, 9163 і 9639;

і) 3655, 2516, 731 і 663;

к) років народження всіх членів вашої сім'ї.

№10. Знайти найменше спільне кратне чисел:

а) 360 і 504;

б) 187 і 533;

в) –2520 і 6600;

г) двох послідовних цілих чисел n і n+1;

д) 91, 252 і 462;

е) 84, 147 і 245;

є) n, n+1 і n+2, де $n \in Z$.

№11. Знайти натуральні числа a і b, якщо:

а) $\begin{cases} a+b=150, \\ \text{НСД}(a,b)=30; \end{cases}$

б) $\begin{cases} a+b=144, \\ \text{НСД}(a,b)=24; \end{cases}$

в) $\begin{cases} ab=20, \\ \text{НСК}[a,b]=10; \end{cases}$

г) $\begin{cases} ab=8400, \\ \text{НСД}(a,b)=20; \end{cases}$

д) $\begin{cases} ab=720, \\ \text{НСД}(a,b)=4; \end{cases}$

е) $\begin{cases} \dfrac{a}{\text{НСД}(a,b)}+\dfrac{b}{\text{НСД}(a,b)}=18, \\ \text{НСК}[a,b]=975; \end{cases}$

є) $\begin{cases} ab=168, \\ \text{НСД}(a,b)=14. \end{cases}$

№12. Знайти натуральні числа a і b, якщо:

а) НСД $(a, b) = 15$, НСК $[a, b] = 420$;

б) НСД $(a, b) = 12$, НСК $[a, b] = 840$;

в) НСД $(a, b)\cdot$НСК $[a, b] = 504$; $\frac{\text{НСК } [a,b]}{\text{НСД } (a,b)} = 14.$

Відповіді: ***№1***. а) $q = 4$, $r = 7$; б) $q = 0$, $r = 31$; в) $q = -5$, $r = 24$. ***№2.*** а) $b_1 = 47$, $q_1 = 2$; $b_2 = 94$, $q_2 = 1$; б) $b = 111$, $q = 1$; в) $b_1 = 288$, $q_1 = 1$; $b_2 = 144$, $q_2 = 2$; $b_3 = 72$, $q_3 = 4$; $b_4 = 36$, $q_4 = 8$; $b_5 = 18$, $q_5 = 16$. ***№3***. а) $b_1 = 25$, $r_1 = 21$; $b_2 = 26$, $r_2 = 7$; б) таких b і r не існує; в) $b = 17$, $r = 16$. ***№6.*** Прості числа: 127, 919, 1033, 1657, 2647, 3163. ***№7.*** а) $2^5\cdot5$; б) $2\cdot13\cdot19$; в) $2^3\cdot3^2\cdot5^2$; г) $53\cdot67$. ***№9***. а) 21; б) 13; в) 2; г) 71; д) 420; є) 1; ж) 13; з) 119; і) 17. ***№10.*** а) 2520; б) 99671; в) 138600; г) $n(n+1)$; д)36036; е) 2940; є) $1/2n(n+1)(n+2)$ при n парному, $n(n+1)(n+2)$ при n непарному. ***№11***. а) $a_1 = 30$, $b_1 = 120$; $a_2 = 60$, $b_2 = 90$ і навпаки; б) $a = 24$, $b = 120$ і навпаки; в) $a = 2$, $b = 10$ і навпаки; г) $a_1 = 20$, $b_1 = 420$; $a_2 = 60$, $b_2 = 140$ і навпаки; д) $a_1 = 4$, $b_1 = 180$; $a_2 = 20$, $b_2 = 36$ і навпаки; е) $a = 75$, $b = 195$ і навпаки; є) не існує.

Завдання для самостійного розв'язування

№1. Знайти неповну частку і остачу при діленні цілого числа a на ціле число b, якщо:

а) $a=31$, $b=-131$;

б) $a=-31$, $b=-131$;

в) $a=-131$, $b=-31$.

№2. При діленні цілого числа a на ціле число b дістають неповну частку q і остачу r . Знайти b і q, якщо:

а) $a=497$, $r=16$;

б) $a=28$, $r=2$;

в) $a=14$, $r=14$.

№3. При діленні цілого числа a на ціле число b утворюється неповна частка q остача r. Знайти b і r, якщо:

а) $a = 57$, $q=0$;

б) $a = 13127$, $q=121$;

в) $a= 100$, $q=100$.

№4. Довести, що:

а) з п'яти послідовних цілих чисел одне і тільки одне ділиться на 5;

б) з n послідовних цілих чисел одне і тільки одне ділиться на n;

в) добуток чотирьох послідовних цілих чисел ділиться на 12;

г) добуток n послідовних цілих чисел ділиться на $n!$.

№5. Довести, що для довільних натуральних чисел m і n:

а) $\left(n^7 - n\right) \vdots 42$;

б) $mn\left(n^4 - n^4\right) \vdots 30$;

в) $\left(n\left(n^2 + 5\right)\right) \vdots 6$.

№6. Чи є числа 3623, 3631, 3763, 3767, 3769, 7429 простими?

№7. Знайти канонічний розклад числа n, якщо:

а) n = 1001;

б) n =1769;

в) n =82798848;

г) n= 1009.

№8. Довести, що дане число a є складеним:

а) $a = n^8 + 4, n \neq \pm 1$;

б) $a = n^8 + n^4 + 1, n > 1$.

№9. Знайти найбільший спільний дільник чисел:

а) 1173 і 323;

б) 2091 і 1681;

в) 2585 і 7975;

г) 299, 391 і 667.

№10. Знайти найменше спільне кратне чисел

а) 252 і 468;

б) 279 і 372;

в) 1058, 1403 і 3266;

г) 126, 420 і 525.

№11. Знайти натуральні числа a і b, якщо:

а) $\begin{cases} \frac{a}{b} = \frac{11}{7}, \\ \text{НСД}(a, b) = 45; \end{cases}$ б) $\begin{cases} \frac{a}{b} = \frac{5}{9}, \\ \text{НСД}(a, b) = 28; \end{cases}$

в) $\begin{cases} (a, b) = 4, \\ \text{НСК}[a, b] = 24; \end{cases}$ г) $\begin{cases} \text{НСД}(a, b) = 4, \\ \text{НСК}[a, b] = 12; \end{cases}$

д) $\begin{cases} \text{НСД}(a, b) = 24, \\ \text{НСК}[a, b] = 2496; \end{cases}$ е) $\begin{cases} a + b = 667, \\ \text{НСК}[a, b] = 120(a, b). \end{cases}$

№12. Знайти натуральні числа a і b, якщо:

а) НСД $(a, b) = 5$, НСК $(a, b) = 260$;

б) $a + b = 667$, $\frac{\text{НСК}\,(a,b)}{\text{НСД}\,(a,b)} = 120$.

Відповіді: ***№1***. а) $q = 0$, $r = 31$; б) $q = 1$, $r = 100$; в) $q=5$, $r = 24$. ***№2***. а) $b_1 = 481$, $q_1 = 1$; $b_2 = 37$, $q_2 = 13$; б) $b_1 = 6$, $q_1=1$; $b_2 = 13$, $q_2 = 2$; в) за b можна взяти довільне ціле число, таке, що $|b|>14$, $q=0$. ***№3***. а) b – довільне ціле число, причому $|b|>57$, $r = 57$; б) $b = 108$, $r = 59$; в) $b = 1$, $r = 0$. ***№6***. Прості числа: 3623, 3631, 3767, 3769. ***№7***. а) $7\cdot11\cdot13$; б) $29\cdot61$; в) $2^8\cdot3^5\cdot11^3$; г) 1009. ***№9***. а) 17; б) 41; в) 55; г) 23. ***№10***. а) 3276; б) 1116; в) 4582198; г) 88200. ***№11***. а) $a = 495$, $b=315$ і навпаки; б) $a = 140$, $b = 252$ і навпаки; в) $a_1 = 4$, $b_1 = =24$; $a_2= 8$, $b_2 = 12$ і навпаки; г) $a = 4$, $b = 12$ і навпаки; д) $a_1 = 24$, $b_1 = 2496$; $a_2 = 8$, $b_2 = 12$ і навпаки; е) $a_1 = 552$, $b_1 = 115$; $a_2 = 435$, $b_2 = 232$ і навпаки.

Тема четверта
ТЕОРІЯ КОНГРУЕНЦІЙ
КОНГРУЕНЦІЇ В КІЛЬЦІ ЦІЛИХ ЧИСЕЛ

Властивості конгруенцій за даним модулем

У другій темі вже було введено відношення конгруентності в будь-якому кільці K за ідеалом m, або за модулем m, і розглянуто деякі його властивості. Розглянемо тепер це поняття в кільці цілих чисел – комутативному кільці з одиницею.

Спочатку сформулюємо деякі означення і властивості стосовно цих чисел.

***Означення**. Числа a і b називаються конгруентними за модулем m, якщо остачі при діленні їх на число m рівні між собою, тобто* $a = mq+r$, $b=mq_1+r$ *і* $0 \le r<m$.

Записують це, як було домовлено, так:

$$a \equiv b \pmod m.$$

Якщо розглядається кілька чисел, конгруентних між собою за тим самим модулем m, то роблять такий запис:

$$a \equiv b \equiv c \equiv d \pmod m.$$

Наприклад, $2 \equiv 5 \equiv 8 \pmod 3$.

***Теорема**. Для того, щоб числа a і b були конгруентні за модулем m, необхідно і достатньо, щоб різниця a-b ділилася на m, або що те ж саме,* $a = b + mt$, *де t – довільне ціле число.*

Розглянемо спочатку конгруенції при незмінному модулі.

1. *Конгруенції за тим самим модулем можна почленно додавати.*
2. *Конгруенції за тим самим модулем можна почленно віднімати.*
3. *До обох частин конгруенції можна додати будь-яке ціле число, тобто з конгруенції* $a \equiv b \pmod m$ *випливає* $a+c \equiv a \equiv b+c \pmod m$, *де c – довільне ціле число.*
4. *З однієї частини конгруенції до другої її частини можна переносити доданок з протилежним знаком, тобто з*

$a+b\equiv c\ (mod\ m)$ випливає $a\equiv c-b\ (mod m)$.

5. *До будь-якої частини конгруенції можна додати або відняти довільне ціле число, кратне модулю, тобто з конгруенції $a\equiv b\ (mod\ m)$ випливає $a+km\equiv b\ (mod\ m)$ або $a\equiv b+km\ (mod\ m)$.*
6. *Конгруенції за одним модулем можна почленно перемножити.*

   Наслідок. *Конгруенцію можна піднести до будь-якого натурального степеня n.*
7. *Обидві частини конгруенції можна помножити на те саме ціле число, тобто при $a\equiv b\ (mod\ m)$ і k цілому істинна конгруенція $ak\equiv bk\ (mod\ m)$.*
8. *Обидві частини конгруенції можна поділити на їх спільний дільник d, якщо він взаємно простий з модулем m.*
9. *Якщо у виразі*

$$f(a_1, a_2, \dots, a_k) = \sum A a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$$

всі коефіцієнти A і числа a_1, a_2, ..., a_k замінити на конгруентні їм за модулем m коефіцієнти B і числа b_1, b_2,...,b_k відповідно, то новий вираз

$$g(b_1, b_2, \dots, b_k) = \sum B b_1^{n_1} b_2^{n_2} \dots b_k^{n_k}$$

буде конгруентний за модулем m до заданого

$$f(a_1, a_2, \dots, a_k) \equiv g(b_1 \dots b_k)(mod\ m)$$

Наслідок 1. *Якщо $a_i \equiv b_i\ (mod\ m)$ i = 1,...,k, то*

$$f(a_1, a_2, \dots, a_k) \equiv f(b_1 \dots b_k)(mod\ m).$$

Наслідок 2. *Якщо в многочлені з цілими коефіцієнтами*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

заданому на множині цілих чисел, всі коефіцієнти a_i замінити коефіцієнтами b_i конгруентними з a_i за модулем m, то отримуємо многочлен $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$ конгруентний з многочленом f(x), тобто

$$\forall x \in Z \; f(x) \equiv g(x) (mod\ m).$$

Наслідок 3. *Якщо $x \equiv y$ $(mod\ m)$, то для многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ виконується конгруенція $f(x) \equiv f(y) (mod\ m)$.*

Властивості конгруенцій за різними модулями

Зазначені вище властивості залишаються справедливими (тому продовжимо нумерацію).

10. *Обидві частини конгруенції і модуль можна множити на те саме ціле число.*
11. *Обидві частини конгруенції і модуль можна скоротити на спільний дільник.*
12. *Якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який дорівнює спільному найменшому кратному цих модулів.*
13. *Якщо конгруенція має місце за модулем m, число d – дільник m, тоді вона має місце і за модулем d.*
14. *Якщо одна частина конгруенції і модуль діляться на число d, то й друга частина конгруенції ділиться на це число.*
15. *Якщо $a \equiv b$ $(mod\ m)$, то* НСД *чисел* (a, m) *і* (b, m) *рівні між собою* НСД(a,m)=НСД(b,m).

Класи чисел за даним модулем

У другій темі вже зазначалося, що відношення конгруентності ділить кільце *K* на класи чисел, конгруентних між собою за даним модулем – класи лишків. Лишком класу за модулем m називається будь-яке число цього класу. Кільце цілих чисел Z за модулем m розпадається на m класів лишків, кожний з яких породжується будь-яким числом цього класу.

До класу лишків, який містить число a, належать усі цілі числа x виду $x=a+mt$, де t – будь-яке ціле число. Цей клас ми позначали символом $\overline{a}$. Позначатимемо далі цей клас символом $K_a^{(m)}$. Очевидно, що його можна позначити і символом $K_{a+mt}^{(m)}$, бо число $a+mt \in K_a^{(m)}$. Іншими словами, правильна така рівність: $K_a^{(m)} = K_{a+mt}^{(m)}$ при будь-якому цілому значенні t.

Оскільки відношення конгруентності є відношенням еквівалентності, то різні класи лишків за модулем m не мають спільних елементів. Тим самим можна стверджувати, що два класи лишків *збігаються, якщо вони мають хоч один спільний елемент*.

***Теорема**. Кожний клас лишків $K_a^{(m)}$ за модулем m розпадається на d ($d \geq 1$) класів лишків за модулем dm, а саме:* $\left\{K_a^{(dm)}, K_{a+m}^{(dm)}, K_{a+2m}^{(dm)}, \ldots, K_{a+(d-1)m}^{(dm)}\right\}$.

Фактор-кільце класів лишків за даним модулем

У фактор-множині Z/m класів лишків за даним модулем m вводяться операції додавання й множення, погоджені з операціями додавання й множення в кільці цілих чисел, а саме:

Сумою класів $K_a^{(m)}$ і $K_b^{(m)}$ називається такий клас $K_{a+b}^{(m)}$, який містить в собі число $a + b$.

Добутком класів $K_a^{(m)}$ і $K_b^{(m)}$ називається такий клас $K_{ab}^{(m)}$, який містить у собі число ab.

Приклад. За модулем $m = 6$ кільце цілих чисел утворює фактор-множину класів лишків:

$$\left\{K_0^{(6)}, K_1^{(6)}, K_2^{(6)}, K_3^{(6)}, K_4^{(6)}, K_5^{(6)}\right\}.$$

Очевидно:

$$K_3^{(6)} + K_4^{(6)} = K_7^{(6)} = K_1^{(6)},\ K_2^{(6)} \cdot K_5^{(6)} = K_{10}^{(6)} = K_4^{(6)}.$$

***Теорема**. Фактор-множина класів лишків за даним модулем є комутативним кільцем з одиницею.*

Відповідно до цього фактор-множину класів лишків за модулем m називають *фактор-кільце*. Позначатимемо його Z/m.

***Теорема**. Якщо m – складене число, то Z/m є комутативне кільце з дільниками нуля. Якщо ж m – просте число, то Z/m – поле.*

Приклад. Розглянемо кільце *Z/7*:

$$Z/7 = \left\{K_0^{(7)}, K_1^{(7)}, K_2^{(7)}, K_3^{(7)}, K_4^{(7)}, K_5^{(7)}, K_6^{(7)}\right\}.$$

Для ненульових елементів знайдемо обернений.

Елемент $K_p^{(7)} \neq K_0^{(7)}$	$K_0^{(7)}$	$K_2^{(7)}$	$K_3^{(7)}$	$K_4^{(7)}$	$K_5^{(7)}$	$K_6^{(7)}$
Обернений до $K_p^{(7)}$ елемент	$K_1^{(7)}$	$K_4^{(7)}$	$K_5^{(7)}$	$K_2^{(7)}$	$K_3^{(7)}$	$K_6^{(7)}$
Добуток	$K_1^{(7)}$	$K_8^{(7)} = K_1^{(7)}$	$K_{15}^{(7)} = K_1^{(7)}$	$K_8^{(7)} = K_1^{(7)}$	$K_{15}^{(7)} = K_1^{(7)}$	$K_{36}^{(7)} = K_1^{(7)}$

Повна система лишків

У кожному класі $K_a^{(m)}$ лишків за модулем *m* можна знайти *найменший невід'ємний лишок* – остачу *r* від ділення *a* на *m: a=mq+r,* де 0≤*r*<*m,* і *абсолютно найменший лишок* – лишок, який за абсолютною величиною менший від всіх абсолютних величин лишків класу $K_a^{(m)}$.

Наприклад, у класі $K_5^{(7)}$ за модулем *m*=7 (цей клас складають елементи *x*=*a*+*mt*=5+7*t*):

$$K_5^{(7)} = \{\dots, -16, -9, -2, 5, 12, 19, 26, \dots\}$$

найменшим невід'ємним лишком є число *r*=5 (яке задовольняє нерівності 0≤*r*<*m*), а абсолютно найменшим лишком є число (-2), бо його абсолютна величина менша від абсолютних величин всіх інших лишків даного класу. Звичайно, може бути, що найменший невід'ємний лишок і абсолютно найменший лишок даного класу $K_a^{(m)}$ збігаються.

Наприклад, у класі $K_3^{(7)}$ (який складають елементи *x*=*a*+*mt*=3+7*t*): $K_3^{(7)}$ ={..., -11, -4, 3, 10, 17, 24,...} число 3 і є найменшим невід'ємним і абсолютно найменшим лишком.

***Означення**. Система лишків, утворена з m чисел, взятих по одному з кожного класу, називається повною системою лишків за модулем m.* Скорочено позначатимемо її буквами ПСЛ.

Наприклад, при m=7 повними системами лишків є такі системи чисел:

p_1={0, 1, 2, 3, 4, 5, 6},

p_2={-3, -2, -1, 0, 1, 2, 3},

p_3={-24, -9, -1, 56, 1, 16, 73} і т.д.

Система p_1 складається з найменших невід'ємних лишків усіх класів, система p_2 – з абсолютно найменших лишків, а система p_3 – з довільних 7 чисел, узятих по одному з кожного класу:

$$-24 \in K_4^{(7)}, -9 \in K_5^{(7)}, -1 \in K_6^{(7)}, 56 \in K_0^{(7)}, 1 \in K_1^{(7)},$$

$$16 \in K_2^{(7)}, 73 \in K_3^{(7)}.$$

***Теорема**. Якщо* $(a,m)=1$*, b – довільне число, а x пробігає* ПСЛ *за модулем m, то й форма ax + b також пробігає* ПСЛ *за модулем m.*

Зведена система лишків

Уведемо тепер поняття найбільшого спільного дільника класу лишків за модулем m. Згідно з властивістю 15, усі числа того самого класу $K_a^{(m)}$ мають однаковий НСД за модулем m: якщо $a, b \in K_a^{(m)}$, тобто $a \equiv b \pmod m$, то $(a, m)=(b,m)$.

***Означення**. Найбільшим спільним дільником класу* $K_a^{(m)}$ *називається найбільший спільний дільник чисел a і m. Якщо* НСД$(a, m)=1$*, то клас* $K_a^{(m)}$ *називається взаємно простим з модулем m.*

***Означення**. Система лишків, узятих по одному з кожного класу, взаємно простого з модулем, називається зведеною системою лишків.*

Скорочено позначатимемо цю систему буквами ЗСЛ.

Приклад. Якщо m = 8, то ПСЛ (остачі від ділення чисел на 8) є 0,1, 2, 3, 4, 5, 6, 7. Члени 1, 3, 5, 7 взаємнопрості з числом 8. Вони й утворюють ЗСЛ. Отже,

ПСЛ = {0, 1, 2, 3, 4, 5, 6, 7}, ЗСЛ= {1, 3, 5, 7}.

Відповідно до цього класи $K_1^{(8)}, K_3^{(8)}, K_5^{(8)}, K_7^{(8)}$ взаємно прості з модулем *m.*

Означення. *Функцією Ейлера* $\varphi(m)$ *називається функція, визначена на множині натуральних чисел; значення* $\varphi(m)$ *є кількість невід'ємних чисел, менших за m і взаємно простих з m.*

Наприклад, $\varphi(8) = 4$, бо існує 4 невід'ємних числа, менших за 8 і взаємно простих з 8, а саме числа 1, 3, 5, 7.

Аналогічно легко встановити, що: $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$ тощо.

Зазначимо ще, що $\varphi(1)=1$, бо існує одне невід'ємне число - нуль, менше за 1 та взаємно просте з ним.

Очевидно, число $\varphi(m)$ дорівнює кількості чисел, які утворюють ЗСЛ за модулем *m*.

Теорема*. Якщо* НСД(*a,m*)=1, *x пробігає* ЗСЛ *за модулем m, то лінійна форма y=ax також пробігає* ЗСЛ *за модулем m.*

Зауваження. Якщо число $\tilde{x}_i$ є лишок ЗСЛ за модулем *m* і належить класу $K_i^{(m)}$, то добуток $a\tilde{x}_i$ хоч і належатиме до ЗСЛ за модулем *m*, але може належати зовсім іншому класу. Тільки в тому випадку, коли *a*=*km*+1, добуток знову належатиме класу $K_i^{(m)}$.

Наприклад, при модулі *m* = 8 ЗСЛ з найменших невід'ємних лишків складається з чисел 1, 3, 5, 7, які відповідно належать класам $K_1^{(8)}, K_3^{(8)}, K_5^{(8)}, K_7^{(8)}$. Якщо *a*=11, то добутки $a\cdot\tilde{x}_i$ є числами 11, 33, 55, 77, які належать відповідно до класів $K_3^{(8)}, K_1^{(8)}, K_7^{(8)}, K_7^{(8)}$.

Властивості функції Ейлера

У теорії чисел використовують ряд спеціальних функцій, які дають важливу арифметичну характеристику цілих чисел. Одним з найпростіших прикладів є функція $f(x) = [x]$ (читається «ант'є від *x*»), яка задана на множині всіх дійсних чисел; $[x]$ – це найбільше ціле число, яке не перевищує *x.* Так, [8,6]=8, а [-9,3]=-10.

За допомогою функції $[x]$ можна, *наприклад*, вказати степінь, з яким у канонічний розклад числа $n!$ входить простий множник p. Цей степінь дорівнюватиме такому натуральному числу:

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right],(p^k\le n<p^{k+1}).$$

Наприклад. Якщо $n = 9$, то просте число 2 в канонічний розклад числа $9!=1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9$ входить в степені 7, бо:

$$\left[\frac{9}{2}\right]+\left[\frac{9}{2^2}\right]+\left[\frac{9}{2^3}\right]=4+2+1=7.$$

Число 3 входить у степені

$$\left[\frac{9}{3}\right]+\left[\frac{9}{3^2}\right]=3+1=4,$$

а 5 і 7 – у степені 1, бо $\left[\frac{9}{5}\right]=1$ і $\left[\frac{9}{7}\right]=1$. Отже, число $9!$ в канонічному вигляді можна записати так:

$$9! = 2^7\cdot 3^4\cdot 5\cdot 7.$$

Серед числових функцій особливу роль відіграють так звані *мультиплікативні* функції.

***Означення**. Числова функція $f(n)$, визначена на множині натуральних чисел, називається мультиплікативною, якщо для кожного n, $f(n)\ne 0$ і для будь-яких взаємно простих натуральних чисел n і m:*

$$f(nm)=f(n)f(m).$$

Мультиплікативні функції мають такі властивості:

1) *якщо $f(n)$ – мультиплікативна функція, то $f(1) = 1$.*
   Справді, $f(n)=f(1\cdot n)=f(1)f(n)$, звідки $f(1) = 1$.
2) *якщо $f(n)$ – мультиплікативна функція і числа $n_1, n_2, ..., n_k$ попарно взаємно прості, то*
   $$f(n_1\cdot n_2\cdot\ldots\cdot n_k)=f(n_1)\cdot f(n_2)\cdot\ldots\cdot f(n_k).$$
3) *добуток мультиплікативних функцій є мультиплікативна функція.*

Розглянемо *властивості* функції Ейлера $\varphi(m)$.

***Теорема**. Функція Ейлера $\varphi(m)$ мультиплікативна.*

***Теорема**. Якщо p – просте число, а k – натуральне число, то $\varphi(p^k) = p^k(1 - \frac{1}{p})$.*

***Теорема**. Якщо канонічний розклад числа m має вигляд $m = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, то $\varphi(m) = m \prod_{i=1}^{s}(1 - \frac{1}{p_i})$.*

Приклад. Для $m = 360 = 2^3 \cdot 3^2 \cdot 5$

$$\varphi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 96.$$

***Теорема**. Сума значень функції Ейлера для всіх дільників d_j числа m дорівнює m (формула Гаусса):*

$$\sum_j \phi(d_j) = m.$$

Теореми Ейлера і Ферма

З властивостей систем лишків безпосередньо випливають відомі теореми Ейлера і Ферма.

***Теорема* Ейлера.** *Якщо m – натуральне число* і $m > 1$, НСД $(a, m)=1$, *то* $a^{\varphi(m)} \equiv 1 \pmod m$.

***Теорема Ферма.** Якщо число p просте і* НСД $(a, p)=1$, *то* $a^{p-1} \equiv 1 \pmod p$.

Приклад. Знайти остачу від ділення числа 42^{50} на 17.

Оскільки 17 – просте число і НСД (42, 17) =1, то за теоремою Ферма $42^{16} \equiv 1 \pmod{17}$. Підносячи до куба обидві частини конгруенції, далі маємо

$42^{48} \equiv 1 \pmod{17}$.

Крім того, $42 \equiv 8 \pmod{17}$, а в квадраті це дає $42^2 \equiv 8^2 \pmod{17}$, $42^2 \equiv 64 \pmod{17}$, $64=17 \cdot 3+13$, тоді $42^2 \equiv 13 \pmod{17}$.

Потім отримуємо $[42^{48} \equiv 1 \pmod{17}$ і $42^2 \equiv 13 \pmod{17}] \rightarrow [42^{50} \equiv 13 \pmod{17}]$. Отже, остача дорівнює 13.

Конгруенції з одним невідомим за модулем

Означення*. Конгруенціями з одним невідомим за модулем m називаються конгруенції виду*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (mod\ m),$$

де в лівій частині міститься многочлен з цілими коефіцієнтами. Якщо a_n не ділиться на число *m,* то *n* називається *степенем конгруенції;* при a_n:*m* старший член $a_n x^n \equiv 0 (mod\ m)$ і його можна відкинути.

Розв'язком конгруенції $f(x) \equiv 0\ (mod\ m)$ є будь-яке ціле число *a*, яке задовольняє конгруенцію, тобто $f(a) \equiv 0\ (mod\ m)$. Легко зрозуміти, що в цьому випадку разом з числом *a* конгруенцію задовольняють всі числа класу $K_a^{(m)}$ конгруентні *з a* за модулем *m.* Саме це стверджує наслідок 3 властивості 9.

Означення. *Розв'язком конгруенції* $f(x) \equiv 0 (mod\ m)$ *називається клас лишків за модулем m, кожне число якого задовольняє цю конгруенцію.*

Оскільки класів чисел за даним модулем *m* є *m*, то конгруенція може мати лише скінченну кількість розв'язків або може не мати їх зовсім.

Наприклад, конгруенція $2x \equiv 3 (mod\ 4)$ не має розв'язків, бо з неї випливає рівність $2x = 3 + 4t$. Така рівність неможлива, бо при будь-яких *x* і *t* ліва частина рівності – парне число, а права – непарне число.

Щоб знайти розв'язки, досить підставити в конгруенцію замість невідомого *x* числа з різних класів за модулем *m.* Для цього можна перебрати ПСЛ з найменших невід'ємних лишків, а ще краще – повну систему абсолютно найменших лишків.

Наприклад. Щоб знайти розв'язки конгруенції $2x^2 - 5x - 2 \equiv 0\ (mod\ 5)$, знайдемо ПСЛ з найменших невід'ємних лишків за модулем 5: 0, 1, 2, 3, 4.

У результаті підстановки в конгруенцію впевнюємося, що числа 1 і 4 задовольняють її. Отже, розв'язком конгруенції є класи лишків $K_1^{(5)}$ і $K_4^{(5)}$.

Конгруенції розв'язують за допомогою побудови більш простих конгруенцій, рівносильних заданим.

***Означення**. Конгруенції називаються рівносильними, якщо множини їх розв'язків збігаються.*

Щоб побудувати рівносильні конгруенції, над заданою конгруенцією проводять операції, які ґрунтуються на властивостях, розглянутих вище. *До операцій, які не порушують множину розв'язків конгруенцій, належать такі:*

а) додавання до обох частин конгруенції будь-якого многочлена $f(x)$ з цілими коефіцієнтами;
б) додавання до однієї з частин конгруенції многочлена з коефіцієнтами, кратними модулю;
в) множення обох частин конгруенції на число, взаємно просте з модулем;
г) множення обох частин конгруенції і модуля на те саме додатне число.

Наприклад, конгруенцію $2x^2-5x-2 \equiv 0 \pmod 5$, можна спростити так. Відкинемо спочатку член мінус $(-5x)$, коефіцієнт якого кратний модулю. Маємо конгруенцію $2x^2-2 \equiv 0 \pmod 5$.

Далі, скорочуючи на число 2 ліву (і праву) частину, маємо конгруенцію $x^2-1 \equiv 0 \pmod 5$, рівносильну даній конгруенції. Підставляючи в неї числа з ПСЛ, встановлюємо, що розв'язками конгруенції є класи лишків $K_1^{(5)}$ і $K_4^{(5)}$.

Конгруенції першого степеня мають вигляд:

$$a_1x + a_0 \equiv 0 \pmod m.$$

Переносячи вільний член у праву частину конгруенції і змінюючи позначення коефіцієнтів, отримуємо $ax \equiv b \pmod m$.

При розв'язуванні таких конгруенцій розглядають два випадки: НСД $(a, m)=1$ і НСД $(a, m)=d>1$.

***Теорема**. Якщо* НСД $(a, m)=1$, *то конгруенція* $ax \equiv b \pmod m$ *має єдиний розв'язок.*

***Теорема.** Якщо* НСД $(a, m)=d>0$ *і число* b *не ділиться на* d, *то конгруенція* $ax \equiv b \pmod m$ *не має розв'язків.*

***Теорема**. Якщо* НСД $(a, m)=d>1$ *і* $b:d$, *то конгруенція* $ax \equiv b \pmod m$ *має* d *розв'язків.*

Наприклад. Розв'яжемо конгруенцію

$$6x \equiv 15 \ (mod\ 21).$$

Оскільки (6, 21) = 3 і 15 ділиться на число 3, то вихідна конгруенція має три розв'язки. Скорочуючи всі члени конгруенцій і модуль на 3, отримуємо конгруенцію, рівносильну даній, $2x \equiv 5 \ (mod\ 7)$, яка вже буде мати за цим новим модулем єдиний розв'язок, бо НСД (2,7)=1.

Перевіряючи числа, які входять в ПСЛ за модулем 7: 0, 1, 2, 3, 4, 5, 6, знаходимо, що тільки число j=6 є розв'язком $2x \equiv 5 \ (mod\ 7)$. Отже, клас $K_6^{(7)}$ є її розв'язком.

А за модулем m=21 він розпадається на класи лишків $К_6^{(21)}$, $К_{6+7}^{(21)} = К_{13}^{(21)}$, $К_{13+7}^{(21)} = К_{20}^{(21)}$, які є розв'язками вихідної конгруенції.

Способи розв'язування конгруенцій першого степеня

Розглянемо найбільш поширені способи розв'язування конгруенцій першого степеня.

1. *Підстановка в конгруенцію чисел* ПСЛ. Цей спосіб використовують при невеликих модулях. При великих модулях підстановку лишків ПСЛ проводять на заключному етапі побудови рівносильних конгруенцій.

2. *Зведення конгруенцій першого степеня до рівносильної їй конгруенції з коефіцієнтом при x, рівному одиниці.* Цей спосіб полягає в проведенні низки рівносильних перетворень заданої конгруенції за допомогою операцій, розглянутих у п. 9.

Наприклад. Конгруенція $22x \equiv 9 (mod\ 29)$ має єдиний розв'язок, бо НСД (22,29) = 1. Його можна знайти так. Додамо до лівої частини конгруенції $(-29x)$. Отримуємо $-7x \equiv 9 \ (mod\ 29)$. Помножимо обидві частини конгруенції на 4: $-28x \equiv 36 (mod\ 29)$.

Додамо до її лівої частини $29x$, отримуємо $x \equiv 36 \ (mod\ 29)$, або $x \equiv 7 \ (mod\ 29)$. Отже, розв'язком заданої конгруенції є клас $K_7^{(29)}$.

3. *Спосіб Ейлера.*

Нехай задано конгруенцію $ax \equiv b(mod\ m)$, де НСД $(a,m)=1$. Конгруенція має єдиний розв'язок. За теоремою Ейлера $a^{\varphi(m)} \equiv 1(mod\ m)$.

Істинною є і така конгруенція:

$a^{\varphi(m)}b \equiv b(mod\ m)$ або $a(a^{\varphi(m)-1}b) \equiv b(mod\ m)$.

Порівнюючи конгруенції, бачимо, що

$x \equiv a^{\varphi(m)-1}b(mod\ m)$.

Наприклад. Розв'язком конгруенції $3x \equiv 2(mod\ 8)$ за формулою Ейлера є клас чисел x,

$x \equiv 3^{\varphi(8)-1} \cdot 2(mod\ 8)$. $\varphi(8)=4$ (це числа 1, 3, 5, 7). Тоді

$x \equiv 3^3 \cdot 2(mod\ 8)$ або $x \equiv 9 \cdot 3 \cdot 2(mod\ 8)$, $x \equiv 6(mod\ 8)$.

Приклади розв'язування типових завдань

№1. *Дано три числа*: 78, 210, 346. *Чи конгруентні вони з* 27 *за модулем* 11?

Розв'язання. Віднімемо від даних чисел 27, отримаємо числа 51, 183, 319. Із цих трьох чисел тільки 319 ділиться на 11, а тому тільки 346 конгруентно з 27 за модулем 11, тобто $346 \equiv 27$ (*mod* 11).

Відповідь: конгруентне тільки 346.

№2. *Дано множину сукупність чисел* (9, 2, 16, 20, 27, 39, 46, 85). *Чи можна вважати дану множину чисел повною системою лишків за модулем* 8?

Розв'язання. Згідно з означенням повної системи лишків за модулем m сукупність відповідних чисел при діленні на m повинна давати в остачі числа 0, 1, 2, …, m-1.

Легко встановити, виконуючи послідовне ділення чисел даної множини на число 8, що остачі будуть рівними числам 1, 2, 0, 4, 3, 7, 6, 5, а отже, дану множину можна розглядати як повну систему лишків за модулем 8.

Відповідь: так.

№3. *Написати повну систему абсолютно найменших лишків за модулем* 7 *і* 8.

Розв'язання. Якщо модуль m – непарне число, то в шуканій системі лишків можливе найбільше по абсолютній

величині число $\frac{m-1}{2}$; якщо m – парне число, то – $\frac{m}{2}$. Шуканими повними системами лишків будуть системи: (-3, -2, -1, 0, 1, 2, 3), якщо модуль дорівнює 7, і (-3, -2, -1, 0, 1, 2, 3, 4) або (-4, -3, - 2, -1, 0, 1, 2, 3), якщо модуль дорівнює 8.

№4. *Дана повна система лишків* (9, 2, 16, 20, 27, 39, 46, 85) *за модулем* 8. *Вибрати з цих чисел ті, які входять в зведену систему лишків за модулем* 8.

Розв'язання. Відповідно до означення із даної системи необхідно вибрати всі числа, які взаємо прості з модулем. Тому зведена система лишків за модулем 8 буде мати вигляд: (9, 27, 39, 85).

Зауважимо, що зведена система лишків за модулем m містить $\varphi(m)$ чисел; $\varphi(8) = 4$, тобто шукана система повинна містити чотири числа.

Відповідь: (9, 27, 39, 85).

№5. *Показати, що*

$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1 \ (mod\ 7)$.

Розв'язання. Використаємо теорему Ферма:

якщо НСД $(a,p) = 1$, то $a^{p-1} \equiv 1 \ (mod\ p)$.

Числа 1, 2, 3, 4, 5, 6 взаємо прості з числом 7. На основі вказаної теореми

$$a^6 \equiv 1 \ (mod\ 7), \qquad (4.1)$$

де $a = 1, 2, 3, 4, 5, 6$.

Конгруенцію (4.1) почленно піднесемо до куба, отримаємо:

$$a^{18} \equiv 1 \ (mod\ 7). \qquad (4.2)$$

Додаючи почленно конгруенції вигляду (4.2) при $a = 1, 2, 3, 4, 5, 6$, маємо:

$$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv 6 \equiv -1 \ (mod\ 7).$$

Зауваження. Розв'язання значно спрощується, якщо показник степеня є непарне число. Нехай треба показати, що

$$1^{11} + 2^{11} + 3^{11} + 4^{11} \equiv 0 \ (mod\ 5).$$

В лівій частині конгруенції в якості основ фігурує зведена система найменших додатних лишків за модулем 5. У випадку непарних показників, використовуючи систему абсолютно найменших лишків за модулем 5, отримаємо:

$$1^{11} + 2^{11} + 3^{11} + 4^{11} \equiv 1^{11} + 2^{11} + (-2)^{11} + (-1)^{11} \equiv 0 \ (mod\ 5).$$

№6. *Знайти остачу від ділення числа* 7^{402} *на* 101.

Розв'язання. 101 – просте число. Числа 7 і 101 взаємно прості, а тому із теореми Ферма випливає, що

$$7^{100} \equiv 1 \ (mod\ 101).$$

Піднесемо цю конгруенцію почленно до четвертого степеня. Отримаємо:

$$7^{400} \equiv 1 \ (mod\ 101).$$

Крім того, $7^2 \equiv 49$ (*mod* 101). Перемножимо ці конгруенції:

$$7^{402} \equiv 49 \ (mod\ 101).$$

З останньої конгруенції випливає, що шукана остача від ділення буде число 49.

*Відповід*ь: 49.

№7. *Знайти останні дві цифри числа* 243^{402}.

Розв'язання. Очевидно, достатньо знайти остачу, отриману при діленні числа 243^{402} на 100.

$$243^{402} \equiv 43^{402} \ (mod\ 100).$$

Але НСД (43,100) = 1, а тому

$$43^{\varphi(100)} \equiv 1 \ (mod\ 100),$$

тобто

$$43^{40} \equiv 1 \ (mod\ 100).$$

Піднесемо останню конгруенцію почленно до десятого степеня:

$$43^{400} \equiv 1 \ (mod\ 100).$$

Візьмемо таку конгруенцію

$$43^2 \equiv 49 \ (mod\ 100);$$

перемножимо останні дві конгруенції, отримаємо:

$$43^{402} \equiv 49 \ (mod\ 100).$$

Отже, шукана остача дорівнює 49.

*Відповід*ь: 49.

№8. *Розв'язати конгруенцію* $5x \equiv 2$ (*mod* 8).

Розв'язання.

І спосіб.

Оскільки НСД (5,8)=1, то конгруенція має єдиний розв'язок. Знайдемо його за допомогою формули

$$x \equiv ba^{\varphi(m)\,-\,1} \ (mod\ m).$$

Тоді

$$x \equiv 2 \cdot 5^{\varphi(8)-1} \ (mod\ 8),$$
$$x \equiv 2 \cdot 5^3 = 250 \equiv 2 \ (mod\ 8).$$

II спосіб.

Розв'яжемо цю конгруенцію методом спроб, який заснований на властивості повної системи лишків, яка пробігає значення 0,1, 2,…7.

Якщо $x = 0$, то $5 \cdot 0 = 0$ не задовольняє конгруенцію $5x \equiv 2 \ (mod\ 8)$.

Якщо $x = 1$, то $5 \cdot 1 = 5$ не задовольняє конгруенцію $5x \equiv 2 \ (mod\ 8)$.

Якщо $x = 2$, то $5 \cdot 2 = 10$, $(10 - 2) \vdots 8$, а отже, $x = 2$ є розв'язком даної конгруенції. Оскільки конгруенція має лише один розв'язок, то процес знаходження розв'язку завершено. Конгруенція задовольняє цілий ряд чисел за даним модулем; отже, розв'язок конгруенції отримаємо у вигляді:

$$x \equiv 2 \ (mod\ 8).$$

III спосіб.

Зауваження. Відмітимо, що метод розв'язання конгруенцій, що заснований на використанні теореми Ейлера і Ферма, а також метод спроб неможна віднести до раціональних методів розв'язку конгруенцій.

В ряді випадків результат може бути отриманий швидше, якщо використовувати штучний прийом, що заснований на наступній властивості конгруенцій: до будь-якої частини конгруенції можна додати число, кратне модулю.

$5x \equiv 2 \ (mod\ 8)$. Додамо до правої частини конгруенції число 8, рівне модулю, отримаємо:

$$5x \equiv 10 \ (mod\ 8).$$

Поділимо обидві частини на число 5, взаємо просте з модулем 8, отримаємо:

$$x \equiv 2 \ (mod\ 8).$$

№9. *Розв'язати конгруенцію* $115x \equiv 85 \ (mod\ 355)$.

Розв'язання. Оскільки НСД (115, 355) = 5 і 85 ділиться на 5, то дана конгруенція має 5 розв'язків.

Скоротимо обидві частини і модуль на 5:

$$23x \equiv 17 \ (mod\ 71).$$

Отримана конгруенція має єдиний розв'язок. Додамо до правої частини конгруенції число 213=71·3, отримуємо : $23x \equiv 230 \pmod{71}$. Поділимо обидві частини рівняння на 23:

$$x \equiv 10 \pmod{71}.$$

Отже, дана конгруенція має наступні розв'язки:

$$x \equiv 10 \pmod{355}, x \equiv 10+71 \equiv 81 \pmod{355},$$
$$x \equiv 81+71 \equiv 152 \pmod{355},$$
$$x \equiv 152+71 \equiv 223 \pmod{355},$$
$$x \equiv 223+71 \equiv 294 \pmod{355}.$$

Завдання для аудиторного заняття

№1. Серед чисел 216, 134, 214, 303, 21 знайти всі пари чисел, конгруентні між собою за модулем 5.

№2. Серед чисел 217, 42, 182, 214 знайти всі пари чисел, конгруентних між собою за модулем 12.

№3. Дано три числа: 137, 343, 633. Які із даних чисел конгруентне з числом 13 за модулем 31?

№4. Написати повну систему найменших додатних лишків за модулями: а) 6; б) 11; в) 15.

№5. Написати повну систему найменших невід'ємних лишків за модулями: а) 5; б) 11; в) 14.

№6. Написати повну систему абсолютно найменших лишків за модулями: а) 11; б) 9; в) 7.

№7. Написати зведену систему лишків за модулями: а)5; б)9; в)12; г) 15.

№8. Показати, що*:*

а) $1^{16} + 3^{16} + 7^{16} + 9^{16} \equiv 4 \pmod{10}$*;*

б) $1^{11} + 2^{11} + 4^{11} + 5^{11} + 7^{11} + 8^{11} \equiv 0 \pmod{9}$*;*

в) $1^{13} + 5^{13} + 7^{13} + 11^{13} \equiv 0 \pmod{12}$*.*

№9. Знайти остачу від ділення числа 7^{1199} на число 1000.

№10. Знайти дві останні цифри чисел:

а) 17^{61}; б) 19^{79}; в) 7^{114}.

№11. Розв'язати конгруенції:

а) $2x \equiv 3 \pmod{5}$*;* б) $7x \equiv 10 \pmod{11}$*;*

в) $7x \equiv 11 \pmod{15}$*;* г) $3x \equiv 5 \pmod{11}$*;*

д) $10x \equiv 15 \pmod{25}$*;* е) $28x \equiv 40 \pmod{44}$*;*

є) $21x \equiv 33 \pmod{45}$*;* ж) $21x \equiv 35 \pmod{77}$*.*

Відповіді: ***№1***. 216 і 21; 134 і 214. ***№2.*** Серед чисел немає конгруентних за модулем 12. ***№3***. 137 та 633. ***№4***. а) 1, 2, 3, 4, 5, 6. ***№5.*** а) 0, 1, 2, 3, 4. ***№6***. а) -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5. ***№7***. в) 1, 5, 7, 11. ***№9***. 143. ***№10***. а) 17; б) 79; в) 01. ***№11.*** а) 4; б) 3; в) 8; г) 9; д) 4, 9, 14, 19, 24; е) 3, 14, 25, 36; є) 8, 23, 38; ж) 9, 20, 31, 42, 53, 64, 75.

Завдання для самостійного розв'язування.

№1. Серед чисел 135, 106, 181, 225, 167, 452 знайти всі пари чисел, конгруентних між собою за модулем 15.

№2. Дано три числа: 217, 201, 186. Які із даних чисел конгруентне з числом 11 за модулем 19?

№3. Дано три числа: 234, 634, 104. Які із даних чисел конгруентне з числом 9 за модулем 25?

№4. Написати повну систему найменших додатних лишків за модулями: а) 9; б) 13; в)16.

№5. Написати повну систему найменших невід'ємних лишків за модулями: а) 7; б) 12; в) 15.

№6. Написати повну систему абсолютно найменших лишків за модулями: а) 8; б) 12; в) 13.

№7. Написати зведену систему лишків за модулями: а)7; б)11; в)14; г) 11; д) 12; е) 14; ж) 15.

№8. Показати, що:

а) $1^{14} + 5^{14} + 7^{14} + 11^{14} \equiv 4 \pmod{12}$;

б) $1^{17} + 3^{17} + 5^{17} + 9^{17} + 11^{17} + 13^{17} \equiv 0 \pmod{14}$.

№9. Знайти остачу від ділення:

а) числа 11^{1201} на число 1000;

б) числа 3^{157} на число 100.

№10. Знайти дві останні цифри чисел:

а) 11^{203};

б)7^{302}.

№11. Розв'язати конгруенції:

а) $3x \equiv 4 \pmod{7}$; б) $12x \equiv 7 \pmod{13}$;

в) $5x \equiv 3 \pmod{17}$; г) $9x \equiv 2 \pmod{14}$;

д) $9x \equiv 12 \pmod{21}$; е) $24x \equiv 14 \pmod{26}$;

є) $30x \equiv 18 \pmod{102}$.

Відповіді: ***№1***. 135 і 225; 106 і 181; 167 і 452. ***№2.*** 201. ***№9***. а) 11; б) 63. ***№10***. а) 31; б) 49. ***№11***. а) 6; б) 6; в) 4; е) 6, 19; є) 4, 21, 38, 55, 72, 89.

Тема п'ята
ТЕОРІЯ КОНГРУЕНЦІЙ
КОНГРУЕНЦІЇ ВИЩИХ СТЕПЕНІВ

Побудова рівносильних конгруенцій

Розглянемо методику розв'язування конгруенцій *n*-го порядку

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0\equiv 0 \pmod p \qquad (5.1)$$

де p – просте число. За допомогою операцій, описаних у темі чотири, можна побудувати рівносильну до даної конгруенції конгруенцію степеня, не вище p-1, з коефіцієнтами, які є найменшими невід'ємними або абсолютно найменшими лишками ПСЛ за модулем *p.*

Побудову такої конгруенції можна провести у такому порядку.

а) *Замінити всі коефіцієнти a_i многочлена $f(x)$ відповідними їм найменшими невід'ємними або абсолютно найменшими лишками з ПСЛ за модулем p.*

Наприклад, конгруенція

$$12x^8 - 17x^3+12x^2 - 8\equiv 0 \pmod 7$$

рівносильна конгруенції:

$$5x^8 - 3x^3 + 5x^2 - 1\equiv 0 \pmod 7,$$

яку ми отримали, відкинувши з першої конгруенції многочлен $7x^8 - 14x^3 + 7x^2 - 7$, що має коефіцієнти, кратні модулю 7, тому $7x^8 - 14x^3+7x^2 - 7 \equiv 0 \pmod 7$.

б) *Зробити коефіцієнт біля старшого члена конгруенції рівним одиниці.*

Можна вважати, що НСД $(a_n, p)=1$. Справді, якщо a_n і просте число p не взаємно прості, то НСД $(a_n, p)=p$, тобто $a_n:p$. Але тоді у конгруенції можна відкинути старший член і вона вже не буде конгруенцією *n-го* степеня.

За теоремою теми чотири, за умови НСД $(a_n, p)=1$, конгруенція $a_nx\equiv 1 \pmod p$ має єдиний розв'язок. Нехай найменший невід'ємний лишок цього класу-розв'язку є x_0.

Отже, $a_n x_0 \equiv 1 (mod\ p)$ і $a_n x_0 x^n \equiv x^n (mod\ p)$. Тому, помноживши конгруенцію (5.1) на число x_0, отримуємо

$$a_n x_0 x^n + a_{n-1} x_0 x^{n-1} + \ldots + a_1 x_0 x + a_0 x_0 \equiv 0 (mod\ p)$$

або

$$x^n + a_{n-1} x_0 x^{n-1} \ldots + a_1 x_0 x + a_0 x_0 \equiv 0 (mod\ p).$$

Приклад. Розглянемо конгруенцію $5x \equiv 1\ (mod\ 7)$.

Перевіряючи числа, які входять в ПСЛ за модулем 7: 0, 1, 2, 3, 4, 5, 6, знаходимо, що тільки число $j=3$ є розв'язком $5x \equiv 1\ (mod\ 7)$. Отже, клас $K_3^{(7)}$ є її розв'язком:

$$K_3^{(7)} = \{\ldots, -11, -4, 3, 10, 17, \ldots\}.$$

Тоді обидві частини конгруенції

$$5x^8 - 3x^3 + 5x^2 - 1 \equiv 0\ (mod\ 7)$$

можна помножити на будь-яке число цього класу лишків. Помножимо, наприклад, їх на число $x_0 = 3$. Отримуємо:

$$15x^8 - 9x^3 + 15x^2 - 3 \equiv 0\ (mod\ 7),$$

або

$$x^8 - 2x^3 + x^2 - 3 \equiv (mod\ 7),$$

в якій коефіцієнт при старшому члені дорівнює одиниці.

в) *Понизити степінь конгруенції.*

Якщо степінь $n \geq p$, то конгруенцію (5.1) можна замінити рівносильною їй конгруенцією степеня, не вищого $p - 1$. За наслідком теореми Ферма (тема чотири) для будь-якого цілого числа x і простого p: $x^p \equiv x\ (mod\ p)$ або $x^p - x \equiv 0\ (mod\ p)$.

З другого боку, поділивши многочлен $f(x)$ на $x^p - x$, отримуємо $f(x) = (x^p - x)g(x) + r(x)$.

Враховуючи це, матимемо

$$f(x) = (x^p - x)g(x) + r(x) \equiv r(x)(mod\ p),$$

тобто $f(x) \equiv r(x)(mod\ p)$.

Звідси випливає, що конгруенції $f(x) \equiv 0(mod\ p)$ і $r(x) \equiv 0(mod\ p)$ рівносильні.

Під час перетворення конгруенції ділення многочлена $f(x)$ на x^p-x не виконують, а користуються деякими простими конгруенціями. Поділимо n на число p-1, поставивши умову, що остача m може дорівнювати лишкам 1, 2,..., p-1 за модулем p. Тоді $n=(p-1)k+m$ $(1<m<p-1)$.

На основі теореми Ейлера $x^{p-1}\equiv 1(mod\ p)$.

Тому $x^n\equiv x^{(p-1)k+m}\equiv x^{(p-1)k}x^m\equiv 1\cdot x^m(mod\ p)$,
тобто $x^n\equiv x^m\ (mod\ p)$.

Наприклад. Конгруенція

$$x^{16}-3x^{13}+5x^8-4x^7+3x^4+x+1\equiv 0(mod\ 7)$$

$$x^{6\cdot 2+4}-3x^{6\cdot 2+1}+5x^{6\cdot 1+2}-4x^{6\cdot 1+1}+3x^4+x+1\equiv$$
$$\equiv 0(mod\ 7)$$

$$x^4-3x+5x^2-4x+3x^4+x+1\equiv 0(mod\ 7),$$
тобто $4x^4+5x^2-6x+1\equiv 0(mod\ 7)$

Кількість розв'язків конгруенції *n*-го степеня

***Теорема**. Конгруенція n-го степеня за простим модулем може мати не більш як n розв'язків.*

Наприклад, конгруенцію $3x^2\equiv 5\ (mod\ 7)$ задовольняє число $x=2$ і, очевидно, $x=-2$. Оскільки $-2\equiv 5(mod\ 7)$, то $K_2^{(7)}, K_5^{(7)}$ є розв'язками цієї конгруенції і більше розв'язків шукати не треба – за попередньою теоремою їх не існує.

Введемо поняття тотожної конгруенції.

***Означення**. Якщо всі коефіцієнти многочлена $f(x)$ є кратними модуля, то конгруенція*

$f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_0\equiv 0\ (mod\ p)$ *називається тотожною конгруенцією.*

Таку конгруенцію задовольняє будь-яке числове значення x; про степінь такої конгруенції можна говорити лише умовно, бо і старший член, і будь-які інші члени можна відкинути, як кратні модулю m.

Встановимо достатню ознаку того, що дана конгруенція є тотожною. Для цього спочатку звернемо увагу на те, що будь-який многочлен n-го степеня $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ завжди можна подати у вигляді

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_0=a(x-x_1)(x-x_2)...(x-x_{n-1})(x-x_n)+$$

$$+b(x-x_1)(x-x_2)...(x-x_{n-1})+....+k(x-x_1)(x-x_2)+l(x-x_1)+m \quad (5.2)$$

Прирівнюючи коефіцієнти при однакових степенях x в лівій і правій частинах цієї тотожності, можна знайти коефіцієнти $a, b, ..., k, l, m$ за коефіцієнтами $a_n, a_{n-1}, ..., a_0$ або навпаки.

Приклад. Подати многочлен $f(x)=x^3-2x^2+3x-7$ у формі (5.2), коли $x_1 = 2$, $x_2 = 3$, $x_3= 1$. Маємо

$$f(x)= x^3-2x^2+3x-7=a(x-2)(x-3)(x-1)+$$
$$+b(x-2)(x-3)+c(x-2)+d.$$

Порівнювання коефіцієнтів дає результати: $a=1$, $b=4$, $c=12$, $d=-1$, тобто

$$x^3-2x^2+3x-7=(x-2)(x-3)(x-1)+4(x-2)(x-3)+12(x-2)-1.$$

Теорема. *Якщо конгруенція n-го степеня* $f(x)=a_nx^n+a_{n-1}x_{n-1}+...+a_0 \equiv 0 \pmod p$ *має* $n+1$ *розв'язків, то всі її коефіцієнти кратні модулю, тобто ця конгруенція тотожна.*

Квадратичні лишки і нелишки

Розглянемо, як найпростіші, двочленні конгруенції степеня $n>1$ виду

$$x^n \equiv a \pmod p \qquad (5.3),$$

де p – просте число і НСД $(a, p) = 1$.

Якщо така конгруенція має розв'язок, то число a називається *лишком степеня n за простим модулем p,* якщо ні, то *нелишком степеня n за модулем p.* Якщо $n=2$ лишки і нелишки називаються *квадратичними,* $n=3$ – *кубічними,* $n = 4$ – *біквадратними.*

Зробимо кілька зауважень відносно конгруенції (5.3). Перш за все зауважимо, що конгруенція розглядається за умови НСД$(a, p) = 1$, тому нуль не належить ні до лишків, ні до нелишків. Це пояснюється тим, що конгруенція виду $x^n \equiv 0 \pmod p$ має єдиний розв'язок $x \equiv 0 \pmod p$ і внаслідок тривіальності цього факту такий випадок виключається під час розгляду конгруенції (5.3).

У конгруенції (5.3) достатньо вважати, що число a задовольняє умову $1 \le a < p$, бо будь-яка конгруенція $x^n \equiv b \pmod p$, де $b > p$, завжди зводиться до конгруенції з невід'ємними коефіцієнтами, меншими за p.

Якщо в конгруенції модуль $p = 2$, то фактично розглядається також тривіальний випадок: $a=0$, або $a=1$. Отже, конгруенцію $x^n \equiv a \pmod p$ задовольняє або клас непарних чисел $K_1^{(2)}$, якщо a – непарне число, або клас всіх парних чисел $K_0^{(2)}$, якщо a – парне число. Тому вважатимемо далі, що $p > 2$, і перейдемо до розгляду найпростішої квадратної двочленної конгруенції $x^2 \equiv a \pmod p$, НСД $(a,p)=1$, $p>1$.

Приклад. Знайдемо всі квадратичні лишки і нелишки за модулем $p=17$. Множина чисел

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$$

є ЗСЛ за модулем $p=17$. Якщо ж цю множину чисел розглядати з точки зору можливості існування розв'язків квадратної конгруенції, то частина чисел множини є квадратичними лишками, а частина їх – квадратичними нелишками. Враховуючи, що

$$1^2 \equiv 1(mod\ 17), 2^2 \equiv 4(mod\ 17), 3^2 \equiv 9(mod\ 17),$$

$$4^2 \equiv 16(mod\ 17), 5^2 \equiv 8(mod\ 17), 6^2 \equiv 2(mod\ 17),$$

$$7^2 \equiv 15(mod\ 17), 8^2 \equiv 13(mod\ 17), 9^2 \equiv 13(mod\ 17)$$

$$10^2 \equiv 15(mod\ 17), 11^2 \equiv 2(mod\ 17), 12^2 \equiv 8(mod\ 17),$$

$$13^2 \equiv 16(mod\ 17), 14^2 \equiv 9(mod\ 17), 15^2 \equiv 4(mod\ 17)$$

$$16^2 \equiv 1\ (mod 17),$$

бачимо, що квадратичними лишками за модулем 17 є: 1, 2, 4, 8, 9, 13, 15, 16.

Квадратичними нелишками за модулем 17 є: 3, 5, 6, 7, 10, 11,12,14.

Відповідно до сказаного, конгруенцію

$$x^2 \equiv 2 \pmod{17}$$

задовольняють числа $x = 6$ і $x = 11$, і тому вона має два розв'язки: $K_6^{(17)}, K_{11}^{(17)}$. Мають по два розв'язки і конгруенції $x^2 \equiv 15\ (mod\ 17)$, $x^2 \equiv 8\ (mod\ 17)$ та інші.

А конгруенції

$$x^2 \equiv 3\ (mod\ 17), x^2 \equiv 7\ (mod\ 17),\ x^2 \equiv 11(mod\ 17)$$

та інші, в правій частині яких стоять квадратичні нелишки за модулем 17, розв'язків не мають.

Проведений аналіз свідчить про те, що квадратні конгруенції за модулем 17 або мають два розв'язки, або не мають їх зовсім. І половина лишків ЗСЛ за модулем p=17 є квадратичними лишками, а половина – квадратичними нелишками.

Теорема. *Якщо a – квадратичний лишок за модулем p,* НСД(a, p)=1, p>2, *то квадратна конгруенція* $x^2 \equiv a\ (mod\ p)$ *має два розв'язки.*

Теорема*. Для будь-якого простого числа p*>2 *половина лишків* ЗСЛ є *квадратичними лишками, а половина – квадратичними нелишками.*

Критерій Ейлера

За досить великих модулів p множина ЗСЛ налічує велику кількість членів, і тоді процес підстановки цих чисел у конгруенцію для знаходження її розв'язків стає громіздким. Тому перед розв'язуванням конгруенції важливо наперед встановити, чи є число a квадратичним лишком. Відповідь на це запитання дають *критерій Ейлера* і *символ Лежандра.*

Теорема **(*критерій Ейлера*).** *Якщо p*>2 є *простим, то число a є квадратичним лишком за модулем p тоді і тільки тоді, коли*

$$a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$$

і квадратичним нелишком тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$.

Наприклад. Встановимо, чи має розв'язки квадратна конгруенція $x^2 \equiv 13\ (mod\ 17)$.

За критерієм Ейлера знаходимо число $13^{\frac{17-1}{2}}$ і встановлюємо, що за модулем 17

$$13^{\frac{17-1}{2}} = 13^8 = (-4)^8 = 16^4 = (-1)^4 \equiv 1\ (mod\ 17).$$

Отже, задана конгруенція має розв'язки.

Символ Лежандра

За великих p і a користуватися критерієм Ейлера практично майже неможливо.

Значно ефективнішим є спосіб, який ґрунтується на так званому символі Лежандра $\left(\frac{a}{p}\right)$. Читається символ так: «a відносно p».

***Означення**. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається для всіх цілих чисел a, які не діляться на просте число $p > 2$, рівністю*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{якщо } a \text{ є квадратичним лишком за модулем } p, \\ -1, & \text{якщо } a \text{ є квадратичним незалишком } p. \end{cases}$$

Використовуючи критерій Ейлера, очевидно, маємо

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\ p).$$

Властивості символу Лежандра:

1. *Якщо* $a \equiv a_1 (mod\ p)$, *то* $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.

Наприклад, $\left(\frac{400}{151}\right) = \left(\frac{2 \cdot 151 + 98}{151}\right) = \left(\frac{98}{151}\right)$.

2. $\left(\frac{a^2}{p}\right) = 1$.

3. $\left(\frac{1}{p}\right) = 1$.

4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Властивість 4 можна конкретизувати. Справді, просте число $p > 2$ є непарним числом. А будь-яке непарне число можна, наприклад, подати у вигляді $p=4m+1$ або $p=4m+3$.

Якщо $p=4m+1$, то на основі властивості 4

$$\left(\frac{-1}{p}\right)=\left(\frac{-1}{4m+1}\right)=(-1)^{\frac{(4m+1)-1}{2}}=1.$$

Якщо $p=4m+3$, то

$$\left(\frac{-1}{p}\right)=\left(\frac{-1}{4m+3}\right)=(-1)^{\frac{(4m+3)-1}{2}}=-1.$$

Отже, справедливим є таке твердження:

Число (-1) *є квадратичним лишком за модулем p, якщо p можна подати у вигляді* $p=4m+1$, *і квадратичним нелишком за модулем p, якщо p має вигляд* $p=4m+3$.

Наприклад, число $p=17$ має вигляд $17=4\cdot4+1$, тому мінус 1 є квадратичним лишком за модулем 17. А число $p=23$ має вигляд $23=5\cdot4+3$, тому (-1) є квадратичним нелишком за модулем 23.

$$5.\ \left(\frac{a_1\cdot a_2\cdot\ldots\cdot a_k}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\ldots\left(\frac{a_k}{p}\right).$$

Наслідок 1. $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)=\left(\frac{a}{p}\right)\cdot 1=\left(\frac{a}{p}\right)$.

Наслідок 2. $\left(\frac{a^n}{p}\right)=\left(\frac{a}{p}\right)^n$.

Наслідок 3. *Якщо число a не ділиться на просте число* $p>2$ *і в канонічному розкладі на добуток простих множників має вигляд*

$$a=q_1^{t_1}q_2^{t_2}\ldots q_k^{t_k},\ \text{то}$$

$$\left(\frac{q_1^{t_1}q_2^{t_2}\ldots q_k^{t_k}}{p}\right)=\left(\frac{q_1}{p}\right)^{t_1}\left(\frac{q_2}{p}\right)^{t_2}\ldots\left(\frac{q_k}{p}\right)^{t_k}.$$

Останній наслідок зводить питання обчислення символу Лежандра $\left(\frac{a}{p}\right)$ до обчислення символів Лежандра виду $\left(\frac{q}{p}\right)$, де обидва числа q і p є простими числами, більшими за 2.

За модулем 8 всі непарні числа можна подати як числа виду $8k+1$, $8k+3$, $8k+5$, $8k+7$, або $8k\pm1$, $8k\pm3$. Оскільки при $p=8k\pm1$ число $\frac{p^2-1}{8}$ є парним, а при $p=8k\pm3$ є непарним, то звідси випливає таке твердження:

6. *Число* 2 *є квадратичним лишком за простим модулем p, якщо p подано у вигляді суми p =* $8k \pm 1$, *і квадратичним нелишком за модулем p, якщо p подано у вигляді p =* $8k \pm 3$.

7. *Закон взаємності квадратичних лишків:*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Зазначимо що властивості 6-7 важливі і широко використовуються під час знаходження числового значення символу Лежандра $\left(\frac{p}{q}\right)$.

Розв'язування квадратичних конгруенцій

Критерій Ейлера і символ Лежандра дають можливість встановити, чи є число *a* квадратичним лишком за модулем *p,* тобто встановити, чи має розв'язки квадратна конгруенція $x^2 \equiv a \pmod p$.

Розв'язують цю конгруенцію *методом спроб,* підставляючи в неї замість *x* числа ЗСЛ за модулем *p,* або *за допомогою спеціальних таблиць.*

Для великих *p* метод розв'язування за допомогою спроб внаслідок своєї громіздкості стає явно непрактичним. Тільки в окремих випадках можна знайти розв'язки конгруенції в загальному вигляді.

Наприклад. Знайдемо розв'язки квадратної конгруенції $x^2 \equiv 10 \pmod{41}$. Насамперед, встановимо, чи має розв'язки ця конгруенція. Знаходимо

$$\left(\frac{10}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{5}{41}\right).$$

Для $a=2$, $p=41=8\cdot5+1=8k+1$, тоді за властивістю 6 (п.5) $a=2$ – є квадратичний лишок за модулем $p=41$, тобто $\left(\frac{2}{41}\right) = 1$. Тоді:

$$\left(\frac{10}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{5}{41}\right) = 1 \cdot \left(\frac{5}{41}\right) = (\text{за властивістю 7}) =$$
$$= (-1)^{\frac{5-1}{2}\cdot\frac{41-1}{2}}\left(\frac{41}{5}\right) = \left(\frac{41}{5}\right) =$$

$$= \left(\frac{5 \cdot 8 + 1}{5}\right) = (\text{за властивістю 1}) = \left(\frac{1}{5}\right) =$$
$$= (\text{за властивістю 3}) = 1.$$

Отже, $\left(\frac{10}{41}\right) = 1$ і тому задана конгруенція має розв'язки.

Запишемо ЗСЛ: {1, 2, 3,… 40}. Підставляючи в конгруенцію послідовно числа ЗСЛ, отримуємо, що її задовольняють числа x=16 і x=25. Отже, розв'язками заданої конгруенції є класи чисел $K_{16}^{(41)}$ і $K_{25}^{(41)}$.

Показники за модулем

Розглянемо множину цілих додатних степенів числа *a: a, a^2, a^3,...* з точки зору їх конгруентності за деяким модулем $m > 1$, вважаючи, що НСД (a, m) = 1. За теоремою Ейлера маємо: $a^{\varphi(m)} \equiv 1 (mod\ m)$, і, отже, $a^{\varphi(m)k} \equiv 1 (mod\ m)$ для будь-якого натурального *k.* Таким чином, серед степенів числа *a* знайдеться нескінченна кількість чисел, конгруентних з 1 за модулем *m.*

Найменше натуральне число δ, для якого правильна конгруенція $a^{\delta} \equiv 1 (mod\ m)$, *називається показником, до якого належить число a, за модулем m.* Інакше число δ позначають ще символом $P_m(a)$. Число $\delta \leq \varphi(m)$, бо може бути і меншим за значення $\varphi(m)$ функції Ейлера. У випадку, коли $\delta = \varphi(m)$, число *a* називається *первісним коренем* за модулем *m.*

Приклади.

1. Знайти P_m (a), якщо a =3, m = 8.

Для модуля m = 8 ЗСЛ={1, 3, 5, 7}, тому $\varphi(8)=4$. Отже, $3^4 \equiv 1 (mod\ 8)$. Проте, як виявляється, $\delta = P_8(3) < \varphi(8)$. Справді, аналізуючи числа ПСЛ, бачимо, що вже $3^2 \equiv 1\ (mod\ 8)$. Отже, P_8 (3) = 2, тобто число 3 належить до показника 2 за модулем 8.

2. Знайти P_m (a), якщо a = 3, m = 10. Для m=10 число $\varphi(10)=4$. Отже, $3^4 \equiv 1 (mod\ 10)$.

Аналізуючи степені чисел 3^1, 3^2, 3^3, бачимо, що вони не конгруентні 1 за модулем 10. Тому й $\delta = P_{10}(3) = 4$, тобто число 3 належить показнику 4 за модулем 10. Отже, число 3 є первісним коренем за модулем 10.

Зауважимо, що вимога НСД(a, m) = 1 є істотною. У випадку, коли числа a і m не є взаємно простими, конгруенція $a^{\delta} \equiv 1 (mod\ m)$ не виконується ні при яких δ.

***Теорема**. Якщо $a_1 \equiv a_2\ (mod\ m)$, то числа a_1 і a_2 належать до одного й того самого показника за цим модулем.*

$$a_1 \equiv a_2 (mod\ m)\ і\ a_2^{\delta_1} \equiv 1 (mod\ m) \rightarrow a_1^{\delta_1} \equiv 1 (mod\ m).$$

Наслідок. *Усі числа одного класу $K_a^{(m)}$ належать тому самому показнику δ за модулем m.*

Таким чином, говорять не про числа, а *про класи чисел, які належать до даного показника за модулем m.* У прикладі 1 до показника δ=2 належить клас $K_3^{(3)}$, а в прикладі 2 до показника δ = 4 належить клас $K_3^{(10)}$. При цьому клас $K_3^{(10)}$ є, очевидно, *класом первісних коренів за* модулем *m.*

Властивості показників за модулем

1. Якщо НСД(a, m) = 1 *і* δ *– показник, до якого належить число a за модулем m, то серед степенів* $1=a^0, a, a^2, a^3, ..., a^{\delta-1}$ *немає, чисел, конгруентних між собою за модулем m.*

Наслідок 1. *Якщо a – первісний корінь за модулем m, тобто* $\delta=\varphi(m)$, *то множина степенів*

1 $a^0, a, a^2, a^3 ... a^{\varphi(m)}$ *є* ЗСЛ *за модулем m.*

2. *Якщо* $\delta=P_m(a)$, *то:*

$$a^{k_1} \equiv a^{k_2} (mod\ m) \Leftrightarrow k_1 \equiv k_2 (mod\ \delta).$$

Наслідок 2. *Якщо число a належить до показника δ за модулем m, і* $a^k \equiv 1 (mod\ m)$, *то* $k \vdots \delta$.

Наслідок 3. *Показник δ, до якого належить число a за модулем m, є дільником числа* $\varphi(m)$.

Приклад. Знайти порядок P_{20} (7).

1) НСД (20, 7)=1.

2) P_{20} (7) є дільником числа $\varphi(20)$, що дорівнює кількості натуральних чисел, менших 20 та взаємопростих з ним. Такими є числа: 1, 3, 7, 9, 11, 13, 17, 19, їх кількість дорівнює 8, тому $\varphi(20)$=8. Тоді для знаходження δ необхідно дослідити тільки степені 7^1, 7^2, 7^4, 7^8, показники яких є дільниками числа 8.

3) Обираємо найменше з чисел, для якого виконується:

$7^k \equiv 1 (mod\ 20)$, k=1, 2, 4, 8.

$7^1 \equiv 7 (mod\ 20)$, $7^2 \equiv 9 (mod\ 20)$, $7^4 \equiv 1 (mod\ 20)$,

$7^8 \equiv 1 (mod\ 20)$.

Обираємо найменше з чисел 4 та 8, отже, $\delta = P_{20}(7) = 4$.

Добуток показників

Як буде показано далі, первісні корені за модулем m існують обов'язково за умови, коли $m = p$, де через p позначатимемо просте число; при цьому первісних коренів буде $\varphi(p-1)$ класів.

Теорема. *Якщо число a_1 належить до показника δ_1 за модулем m, а число a_2 – до показника δ_2 за модулем m і* НСД $(\delta_1, \delta_2) = 1$, *то добуток чисел $a_1 \cdot a_2$ належить до добутку показників $\delta_1 \cdot \delta_2$ за модулем m.*

Твердження теореми можна поширити на добуток n чисел.

Наслідок. *Якщо числа $a_1, a_2, ..., a_n$ належать за модулем m відповідно до показників $\delta_1, \delta_2, ..., \delta_n$, які попарно взаємно прості між собою, то показник, до якого належить добуток чисел $a_1 \cdot a_2 \dots a_n$ за модулем m, дорівнює добутку показників, до яких належать числа $a_1, a_2, ..., a_n$ за модулем m.*

Існування первісних коренів

У попередніх пунктах вже зазначалося, що конгруенції $a^\delta \equiv 1 (mod\ m)$, можуть не мати розв'язків. Це має місце, коли НСД $(a, m) = d > 1$. Якщо ж НСД $(a, m) = 1$, то існує таке натуральне число $\delta \le \varphi(m)$, при якому ця конгруенція істинна. При цьому постають питання про числові значення показника δ для різних чисел a за модулем m. Чи може, зокрема, бути випадок, коли для всіх a, взаємно простих з m, показник $\delta < \varphi(m)$? Іншими словами, чи може бути випадок, коли за даним модулем m не існує первісних коренів? Чи для всіх m існують первісні корені? Як їх знаходити?

Виявляється, що коли m – складене число, то первісні корені можуть і не існувати за цим модулем. *Наприклад*, якщо $m = 15$ (15 не є простим числом), то ПСЛ = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14}.

Очевидно, тут $\varphi(m)=\varphi(15)=8$, бо серед ПСЛ є 8 чисел, взаємно простих з *m:* 1, 2, 4, 7, 8, 11, 13, 14. Числа 3, 5, 6, 9, 10, 12 не взаємно прості з m і тому конгруенцію $a^{\delta}\equiv 1(mod\ m)$, задовольняти не можуть. Легко перевірити, що

$1^1 \equiv 1(mod\ 15)$, тобто δ=1; $8^4 \equiv 1(mod\ 15)$, тобто δ=4;
$2^4 \equiv 1(mod\ 15)$, тобто δ=4; $11^2 \equiv 1(mod\ 15)$, тобто δ=2;
$4^2 \equiv 1(mod\ 15)$, тобто δ=2; $13^4 \equiv 1(mod\ 15)$, тобто δ=4;
$7^4 \equiv 1(mod\ 15)$, тобто δ=4; $14^2 \equiv 1(mod\ 15)$, тобто δ=2.

Таким чином, число a=1 належить показнику δ=1 за модулем 15, числа a = 4, 11, 14 належать показнику δ=2, а числа a = 2, 7, 8, 13 – показнику δ=4 за модулем 15. Отже, всі показники $\delta<\varphi(m)$ і тому не існує первісних коренів за модулем 15.

Проте виявляється, що коли $m=p$ є простим числом, то первісні корені за цим модулем завжди існують.

Теорема. *За будь-яким простим модулем p існує хоча б один первісний корінь.*

Кількість класів первісних коренів

Теорема*. Якщо існує хоч одне число, яке належить до показника δ за модулем p, то всього класів таких чисел є $\varphi(\delta)$.*

Наслідок 1. *Первісних коренів за модулем p існує $\varphi(p\text{-}1)$.*

Наслідок 2. *Якщо a – первісний корінь за модулем p, то інші первісні корені слід шукати серед степенів a^2, a^3, ..., $a^{p\text{-}1}$ – вони мають вигляд a^k, де* НСД (k, p-1) = 1 і $k\le p$-1.

Зручного способу для знаходження первісних коренів практично не існує, їх знаходять за допомогою звичайних спроб. Щоб дещо полегшити процес обчислень, можна використати таку теорему.

Теорема*. Якщо* $p-1=q_1^{k_1}\cdot q_2^{k_2}\cdot\ldots\cdot q_s^{k_s}$ *– канонічний розклад числа p*-1, *то для того, щоб число a було первісним коренем за модулем p, достатньо, щоб виконувалась умова*: $a^{\frac{p-1}{q_i}} \not\equiv 1(mod\ p)$ *для всіх i* = 1, 2, ..., *s*.

Наприклад. Знайти первісні корені за модулем p=13. Первісних коренів є $\varphi(p\text{-}1)=\varphi(12)=4$. Шукати їх слід серед чисел ЗСЛ за модулем 13:

ЗСЛ={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}.
$2^1 \equiv 2\ (mod\ 13);\ 2^2 \equiv 4\ (mod\ 13);\ 2^3 \equiv 8\ (mod\ 13);$
$2^4 \equiv 3\ (mod\ 13);\ 2^5 \equiv 6\ (mod\ 13);\ 2^6 \equiv -1\ (mod\ 13);$
$2^7 \equiv -2\ (mod\ 13);\ 2^8 \equiv -4\ (mod\ 13);\ 2^9 \equiv -8\ (mod\ 13);$
$2^{10} \equiv -3\ (mod\ 13);\ 2^{11} \equiv -6\ (mod\ 13);\ 2^{12} \equiv 1\ (mod\ 13).$

Отже, 2 належить показнику $12=\varphi(13)$, тобто 2 є первісним коренем за модулем 13. Проте для встановлення цього факту краще скористатися попередньою теоремою. Число p-1=12 в канонічному розкладі має вигляд $p\text{-}1= 2^2 \cdot 3$. Побудуємо числа виду

$$\frac{p-1}{2} = \frac{12}{2} = 6; \frac{p-1}{3} = \frac{12}{3} = 4.$$

Досліджуючи конгруентність степенів 2^6 і 2^4 за модулем 13, бачимо, що

$$2^6 = 64 \equiv -1(mod13);\ 2^4 = 16 \equiv 3(mod13).$$

Отже, в обох випадках

$$2^6 \neq 1(mod13);\ 2^4 \neq 1(mod13)$$

і тому за теоремою число 2 є первісним коренем за модулем 13.

За наслідком 2 з теореми, інші первісні корені є числами виду 2^k, де НСД (k, p-1)=НСД (k, 12)=1 і $0<k\leq 12$. Ці умови задовольняють такі значення: k = 5, 7, 11. Отже, іншими первісними коренями за модулем 13 є числа 2^5, 2^7, 2^{11}. Враховуючи, що

$$2^5 \equiv 6\ (mod\ 13);\ 2^7 \equiv 11\ (mod\ 13),\ 2^{11} \equiv 7\ (mod\ 13),$$

встановлюємо, що первісними коренями за модулем 13 є числа 2, 6, 7, 11.

Індекси за простим модулем

ЗСЛ за модулем p можна подати сукупністю чисел –

найменших невід'ємних лишків 1, 2, 3, 4,..., p-1. Разом з тим, ЗСЛ може бути поданою й інакше – за допомогою степенів якогось первісного кореня за модулем p. Якщо q – є первісний корінь за модулем p (нагадуємо, що p і q взаємно прості), то степені $q, q^2, q^3,...,q^{p-1}$ є також сукупністю p-1 чисел, неконгруентних між собою за модулем p. Тому ці числа є також представниками різних класів лишків за модулем p і утворюють ЗСЛ за модулем p. Кожний клас лишків ЗСЛ за модулем p можна подати якимось числом виду q^γ. Тим самим кожному класу лишків $K_a^{(p)}$ ЗСЛ можна поставити у відповідність показник степеня γ числа q^γ, який і називається індексом класу $K_a^{(p)}$ з основою q.

***Означення**. Індексом числа a за модулем p* (або класу $K_a^{(p)}$) *при основі q називається таке ціле невід'ємне число* γ, *що* $q^\gamma \equiv a (mod\ p)$.

Позначають індекс $\gamma = ind_q\ a$ за модулем p.

Зауважимо, що для класу $K_0^{(p)}$ чисел, кратних модулю p, поняття індексу не вводять, бо при умові НСД (p, q)=1 конгруенція виду $kp \equiv q^\gamma (mod\ p)$ неможлива.

Приклад. Нехай p=7. Можна встановити, що первісними коренями за модулем 7 є числа 3 і 5. Візьмемо за q менший первісний корінь 3. Очевидно, $3^1 \equiv 3 (\text{mod } 7)$, $3^2 \equiv 2 (mod\ 7)$, $3^3 \equiv 6 (mod\ 7)$, $3^4 \equiv 4 (mod\ 7)$, $3^5 \equiv 5 (mod\ 7)$, $3^6 \equiv 1 (mod\ 7)$. У правих частинах конгруенцій стоять числа ЗСЛ.

Перепишем конгруенції інакше:

$1 \equiv 3^6 (mod\ 7)$, $2 \equiv 3^2 (mod\ 7)$, $3 \equiv 3^1 (mod\ 7)$,
$4 \equiv 3^4 (mod\ 7)$, $5 \equiv 3^5 (mod\ 7)$, $6 \equiv 3^3 (mod\ 7)$.

Кожному з чисел 1, 2, 3, 4, 5, 6 або, що те саме, кожному із класів лишків за модулем 7

$$K_1^{(7)}, K_2^{(7)}, K_3^{(7)}, K_4^{(7)}, K_5^{(7)}, K_6^{(7)}$$

поставимо у відповідність індекс γ – показник степеня первісного кореня 3. Цю відповідність можна подати у вигляді таблиці 5.1.

Таблиця 5.1.

Число	1	2	3	4	5	6
Індекс	6	2	1	4	5	3

Таким чином, поняття індексів у теорії конгруенцій аналогічне поняттю логарифмів чисел. Ми далі побачимо, що й роль їх аналогічна: операції з числами в конгруенціях можна замінити певними операціями над індексами. На практиці користуються таблицями індексів, аналогічними побудованій (їх можна знайти, наприклад, у [7]). Для зручності користування будують і другу таблицю (5.2), де упорядкована множина індексів.

Таблиця 5.2

Індекс	1	2	3	4	5	6
Число	3	2	6	4	5	1

Основні властивості індексів

1. *Числа $\gamma' \geq 0$ є індексами числа a за модулем p при основі q тоді і тільки тоді, коли*

$$\gamma' \equiv \gamma (mod\ p-1), \text{ де } \gamma = ind_q a \text{ за модулем p.}$$

2. *Для того щоб $a \equiv b\ (mod\ p)$ необхідно і достатньо, щоб виконувалася конгруенція*

$$ind_q a \equiv ind_q b (mod\ p-1).$$

За даними властивостями можна встановити, що кожному класу лишків $K_a^{(p)}$, де a входить до ЗСЛ за модулем p, взаємно однозначно відповідає клас лишків $K_\gamma^{(p-1)}$, де γ входить до ПСЛ за модулем p-1.

У зв'язку з цим повніше передостанню таблицю можна записати так:

Класи за модулем 7	$K_1^{(7)}$	$K_2^{(7)}$	$K_3^{(7)}$	$K_4^{(7)}$	$K_5^{(7)}$	$K_6^{(7)}$
Класи індексів (класи за модулем 6)	$K_6^{(6)}$	$K_2^{(6)}$	$K_1^{(6)}$	$K_4^{(6)}$	$K_5^{(6)}$	$K_3^{(6)}$

3. $ind_q 1 = 0\ (mod\ p-1)$.

4. $ind_q\, q$=1 (*mod p*-1).
5. *Індекс добутку чисел за модулем p при основі q конгруентний за модулем p*-1 *сумі індексів окремих множників при основі q, тобто*

$$ind_q(a_1a_2...a_n)=ind_qa_1+ind_qa_2+...+ind_qa_n.$$

6. $ind_q a^n \equiv n\ ind_q a(mod\ p-1)$.
7. Якщо $a \vdots b$, то $ind_q \frac{a}{b} \equiv ind_q a - ind_q b(mod\ p-1)$.

Останні властивості є наслідком властивості 5. Зауважимо, що перехід від конгруенції між числами до конгруенції їх індексів називається *індексацією,* а зворотний перехід – *потенціюванням.*

Розв'язування двочленних конгруенцій *n*- го степеня за допомогою індексів

З двочленними конгруенціями *n*-го степеня за простим модулем ми вже зустрічалися. У загальному вигляді двочленні конгруенції можна записати так: $ax^n \equiv b$ (*mod p*), де НСД(*a, p*)= 1 і *n* – натуральне число.

Якщо провести індексацію цієї конгруенції при однаковій основі, то отримуємо конгруенцію

ind (ax^n)≡ *ind b*(*mod p*-1), або, що те ж саме,
ind a+n indx≡*ind b*(*mod p*-1).

Ці конгруенції еквівалентні. Якщо позначити *ind b*- *ind a=c, ind x=y,* то конгруенція *ind a+n indx*≡*ind b* (*mod p*-1) має вигляд *ny* ≡*c* (*mod p*-1).

Тим самим від конгруенції *n*-го степеня за допомогою індексації ми прийшли до конгруенції першого степеня. Розв'язавши її і взявши величину *y=ind x,* знайдемо *x* за відповідними таблицями.

Приклад. Розв'язати конгруенцію

$$3x^3 \equiv 4\ (mod\ 7).$$

Проводячи індексацію при деякій основі *q* (як правило, це найменший первісний корінь за модулем *p*), отримуємо: *ind* 3+3*ind x*≡*ind* 4 (*mod* 6).

За таблицею індексів маємо *ind* 3= 1, *ind* 4 = 4 і тому маємо 1+3*indx*≡4 (*mod* 6), 3*indx*≡ 3 (*mod* 6).

Розв'язками цієї лінійної конгруенції є числа *ind x*=1, 3, 5 з ПСЛ за модулем 6. З таблиці 5.2 отримуємо відповідні три значення невідомого *x: x*=3, 6, 5 (*mod* 7).

Отже, задана конгруенція має три розв'язки.

За допомогою індексів дуже легко знайти показники за модулем. Справді, нехай треба знайти $P_7(6)$. Маємо конгруенцію $6^x \equiv 1 (mod\ 7)$. Виконавши індексацію, отримуємо конгруенцію 1-го степеня $x\ ind\ 6 \equiv ind\ 1 (mod\ 6)$. За таблицею індексів далі маємо $x \cdot 3 \equiv 0 (mod\ 6)$, або, скоротивши на 3 обидві частини і модуль конгруенції, маємо $x \equiv 0\ (mod\ 2)$. Вибираючи найменше натуральне число з класу $K_0^{(2)}$ знаходимо, що $x = 2$, тобто $P_7(6) = 2$.

Приклади розв'язування типових завдань

№1. *За допомогою критерію Ейлера встановити, чи має розв'язок конгруенція* $x^2 \equiv 7\ (mod\ 13)$.

Розв'язання. За критерієм Ейлера знаходимо число $7^{\frac{13-1}{2}}$ і встановлюємо, що за модулем 13

$$7^{\frac{13-1}{2}} = 7^6 = (49)^3 \equiv (-3)^3 \equiv -1\ (mod\ 13).$$

Відповідь: не має розв'язків.

№2. *За допомогою символу Лежандра встановити чи має розв'язок конгруенція* $x^2 \equiv 404\ (mod\ 523)$.

Розв'язання. Знаходимо символ Лежандра $\left(\frac{404}{523}\right)$. Скористаємося наслідком 1 властивості 5 $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$: $\left(\frac{404}{523}\right) = \left(\frac{101 \cdot 2^2}{523}\right) = \left(\frac{101}{523}\right)$;

далі використаємо властивість 7 $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)$: $\left(\frac{101}{523}\right) = (-1)^{\frac{523-1}{2} \cdot \frac{101-1}{2}} \left(\frac{523}{101}\right) = \left(\frac{523}{101}\right)$.

За властивістю 1, якщо $a \equiv b\ (mod\ p)$ то:

$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, отже, $\left(\frac{523}{101}\right) = \left(\frac{18}{101}\right)$.

Знову використаємо наслідок 1 властивості 5 $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{18}{101}\right) = \left(\frac{3^2\cdot 2}{101}\right) = \left(\frac{2}{101}\right)$.

За властивістю 6: $\left(\frac{2}{101}\right) = \left(\frac{2}{13\cdot 8-3}\right) = -1$.

Відповідь: немає розв'язків.

№3. *Знайти розв'язок конгруенцій найпростішим способом* $x^2 \equiv 19$ (*mod* 31).

Розв'язання. До правої частини конгруенції додамо число 62, кратне модулю: $x^2 \equiv 81$ (*mod* 31).

Отже, $x \equiv 9$ (*mod* 31), $x \equiv -9 \equiv 22$ (*mod* 31).

Відповідь: $x \equiv 9$ (*mod* 31), $x \equiv 22$ (*mod* 31).

№4. *Замінити дану конгруенцію рівносильною їй конгруенцією, степінь якої нижче модуля:*

$x^7 - 3x^6 + x^5 + 4x^2 - 4x + 2 \equiv 0$ (*mod* 5).

Розв'язання. Щоб дану конгруенцію замінити на їй еквівалентну, степінь якої менше модуля конгруенції, необхідно многочлен

$$x^7 - 3x^6 + x^5 + 4x^2 - 4x + 2$$

поділити на $x^5 - x$; в остачі отримаємо многочлен

$$x^2 - 3x + 2.$$

Ділення многочлена $f(x)$ на $x^p - x$ можна не виконувати, а використати деякі прості конгруенції.

$x^n \equiv x^{(p-1)k+m} \equiv x^{(p-1)k}x^m \equiv 1\cdot x^m$ (*mod* p)

$x^7 \equiv x^{(5-1)k+m} \equiv x^{4\cdot 1+3} \equiv x^3$ (*mod* 5)

$x^6 \equiv x^{(5-1)k+m} \equiv x^{4\cdot 1+2} \equiv x^2$ (*mod* 5)

$x^5 \equiv x^{(5-1)k+m} \equiv x^{4\cdot 1+1} \equiv x$ (*mod* 5)

$$x^7 - 3x^6 + x^5 + 4x^2 - 4x + 2 \equiv x^3 - 3x^2 + x + 4x^2 - 4x + 2 \equiv$$
$$\equiv x^3 + x^2 - 3x + 2$$

Отже, дана конгруенція еквівалентна конгруенції

$$x^3 + x^2 - 3x + 2 \equiv 0 \text{ (mod } 5).$$

Відповідь: $x^3 + x^2 - 3x + 2 \equiv 0 \ (mod\ 5)$.

№5. *Конгруенцію* $7x^4 - 9x^3 + 8x^2 + 10x - 6 \equiv 0 \ (mod\ 11)$ *замінити рівносильною їй конгруенцією зі старшим коефіцієнтом, рівним одиниці.*

Розв'язання. Оскільки старший коефіцієнт даної конгруенції дорівнює 7 і НСД (7, 11) = 1, то знаходимо єдиний розв'язок конгруенції $7a \equiv 1 \ (mod\ 11)$ у вигляді $a \equiv 8 \ (mod\ 11)$.

Враховуючи, що НСД (8, 11) = 1, помножимо обидві частини даної конгруенції на число 8, не змінюючи модуль конгруенції:

$$56x^4 - 72x^3 + 64x^2 + 80x - 48 \equiv 0 \ (mod\ 11).$$

Після ряду спрощень прийдемо до конгруенції

$x^4 + 5x^3 - 2x^2 + 3x - 4 \equiv 0 \ (mod\ 11)$, яка рівносильна даній.

Відповідь: $x^4 + 5x^3 - 2x^2 + 3x - 4 \equiv 0 \ (mod\ 11)$

№6. *Знайти порядок* $P_m\ (a)$*, числа a за модулем m, якщо:*

а) $a = 2, m = 15$; б) $a = 3, m = 15$.

Розв'язання. Щоб знайти порядок $P_m\ (a)$, числа a за модулем m, слід забезпечити виконання таких вимог:

1. НСД$(a, m) = 1$.
2. $P_m\ (a)$ – дільник числа $\varphi(m)$.
3. $P_m\ (a)$ – найменше з тих натуральних чисел δ, для яких виконується конгруенція $a^{\delta} \equiv 1 (mod\ m)$.

а) Маємо (2, 15) = 1. $\varphi(15) = 8$, отже $P_{15}\ (2)$ міститься серед чисел 1, 2, 4, 8.

$2^1 \equiv 2 \ (mod\ 15)$,

$2^2 \equiv 4 \ (mod\ 15)$,

$2^4 \equiv 16 \equiv 1 \ (mod\ 15)$.

Отже, $P_{15}\ (2) = 4$.

б) Оскільки НСД(3, 15) = 3 ≠1, то для числа a=3 за модулем $m = 15$ порядку не існує.

Відповідь: а) $P_{15}\ (2) = 4$, б) $P_{15}\ (3)$ не існує.

№7. *Скласти таблиці індексів та антиіндексів за модулем* 23*.*

Розв'язання. Знайдемо один із первісних коренів за модулем 23.

$$\varphi(23)=22,\ 5^2 \neq 1(mod\ 23),\ 5^{11} \neq 1(mod\ 23),$$
$$5^{22} \equiv 1(mod\ 23).$$

Отже, 5 є первісним коренем за модулем 23. Візьмемо його за основу таблиці індексів і знайдемо найменші невід'ємні лишки степенів $5^0, 5^1, \ldots, 5^{22}$:

$5^0 \equiv 1\ (mod\ 23);$ $5^8 \equiv 16\ (mod\ 23);$ $5^{16} \equiv 3\ (mod\ 23);$
$5^1 \equiv 5\ (mod\ 23);$ $5^9 \equiv 11\ (mod\ 23);$ $5^{17} \equiv 15\ (mod\ 23);$
$5^2 \equiv 2\ (mod\ 23);$ $5^{10} \equiv 9\ (mod\ 23);$ $5^{18} \equiv 6\ (mod\ 23);$
$5^3 \equiv 10\ (mod\ 23);$ $5^{11} \equiv 22\ (mod\ 23);$ $5^{19} \equiv 7\ (mod\ 23);$
$5^4 \equiv 4\ (mod\ 23);$ $5^{12} \equiv 18\ (mod\ 23);$ $5^{20} \equiv 12\ (mod\ 23);$
$5^5 \equiv 20\ (mod\ 23);$ $5^{13} \equiv 21\ (mod\ 23);$ $5^{21} \equiv 14\ (mod\ 23).$
$5^6 \equiv 8\ (mod\ 23);$ $5^{14} \equiv 13\ (mod\ 23);$
$5^7 \equiv 17\ (mod\ 23);$ $5^{15} \equiv 19\ (mod\ 23);$

Отже, $ind_5 1=0$, $ind_5 2=2$, …, $ind_5 22=11$. Складемо таблицю індексів. У рядку поставимо цифри, що позначатимуть десяток, у стовпчик – одиниці. На перетині ставимо індекс. Маємо таблицю 5.3.

Таблиця 5.3.

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

Побудуємо таблицю антиіндексів (таблиця 5.4)

Таблиця 5.4.

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

№8. *Розв'язати конгруенцію* $17x^{18} \equiv 22\ (mod 23)$.

Розв'язання. Беремо індекси від обох частин конгруенції

$$ind\ 17+18ind\ x \equiv ind\ 22\ (mod\ 22).$$

За таблицею 5.3 маємо: *ind* 17=7, *ind* 22=11 і

тому: $7+18ind\ x\equiv 11\ (mod\ 22)$, $18ind\ x\equiv 4\ (mod\ 22)$. Оскільки $(18, 22)=2$ і $4:2$, то конгруенція має два розв'язки. Скоротимо спочатку конгруенцію на 2:

$9ind\ x\equiv 2\ (mod\ 11)$, додамо до правої частини -11: $9ind\ x\equiv -9\ (mod\ 11)$, скоротимо на 9: $ind\ x\equiv -1\ (mod\ 11)$, отже, $ind\ x\equiv 10\ (mod\ 22)$ або $ind\ x\equiv 21\ (mod\ 22)$. За таблицею 5.4. знаходимо відповідні значення невідомої: $x\equiv 9\ (mod\ 23)$, $x\equiv 14\ (mod\ 23)$.

Відповідь: $x\equiv 9\ (mod\ 23)$, $x\equiv 14\ (mod\ 23)$.

Завдання для аудиторного заняття

№1. За допомогою критерію Ейлера встановити, чи мають розв'язки конгруенції:

а) $x^2 \equiv 3\ (mod\ 7)$; б) $x^2 \equiv 5\ (mod\ 11)$; в) $x^2 \equiv 6\ (mod\ 13)$.

№2. За допомогою символу Лежандра встановити, чи мають розв'язки конгруенції:

а) $x^2 \equiv 22\ (mod\ 13)$; б) $x^2 \equiv 99\ (mod\ 601)$;

в) $x^2 \equiv 219\ (mod\ 383)$; г) $x^2 \equiv 47\ (mod\ 73)$;

д) $x^2 \equiv 231\ (mod\ 101)$.

№3. Знайти розв'язок конгруенцій найпростішим способом:

а) $x^2 \equiv 4\ (mod\ 7)$; б) $x^2 \equiv 20\ (mod\ 101)$;

в) $x^2 \equiv 6\ (mod\ 47)$; г) $x^2 \equiv 12\ (mod\ 23)$.

№4. Замінити дані конгруенції рівносильними їм конгруенціями, степені яких нижче модуля:

а) $x^8 - 3x^7 + 2x^6 + 3x^4 - 2x^2 - 1 \equiv 0\ (mod\ 5)$;

б) $x^{13} - x^3 + x - 3 \equiv 0\ (mod\ 11)$;

в) $x^8 - 2x^7 + 3x^6 + x^5 - 2x^2 - x - 3 \equiv 0\ (mod\ 5)$.

№5. Розв'язати конгруенції:

а) $x^8 - x^6 + x^5 - x^4 + 2x^2 - x + 3 \equiv 0\ (mod\ 5)$;

б) $x^9 - x^3 + x - 5 \equiv 0\ (mod\ 7)$;

в) $x^{14} - 4x^{13} - x + 6 \equiv 0\ (mod\ 13)$.

№6. Замінити дані конгруенції рівносильними зі старшим коефіцієнтом рівним одиниці:

а) $7x^5 - 2x^4 + 5x^3 - x^2 + 3x - 2 \equiv 0\ (mod\ 11)$;

б) $11x^3 - 6x^2 + 2x - 5 \equiv 0\ (mod\ 15)$;

в) $27x^3 + 14x^2 - 10x + 13 \equiv 0\ (mod\ 59)$.

№7. Знайти порядок $P_m(a)$, числа a за модулем m, якщо:

а) $a = 2$, $m = 5$; б) $a = 4$, $m = 5$;

в) $a = 5, m = 8$; г) $a = 10, m = 13$;

д) $a = 7, m = 22$.

№8. Скласти таблиці індексів за модулем p з основою g, якщо:

а) $p=5, g=3$; б) $p=11, g=5$.

№9. Розв'язати конгруенцію, використовуючи результати №8:

а) $17x^{18} \equiv 22(mod 5)$; б) $3x^{20} \equiv 2(mod 11)$.

Відповіді: ***№1***. а) немає розв'язків; б) має розв'язки; в) немає розв'язків. ***№2***. а) має розв'язки; б) немає розв'язків; в) має розв'язки; г) немає розв'язків; д) немає розв'язків. ***№3***. а) $x \equiv 2 \pmod 7$, $x \equiv 5 \pmod 7$; б) $x \equiv 11 \pmod{101}$, $x \equiv 90 \pmod{101}$; в) $x \equiv 10 \pmod{47}$, $x \equiv 37 \pmod{47}$, г) $x \equiv 9 \pmod{23}$, $x \equiv 14 \pmod{23}$. ***№4***. а) $4x^4 - 3x^3 - 1 \equiv 0 \pmod 5$; б) $-x^3+x^2+x - 3 \equiv 0 \pmod{11}$; в) $x^3 + x^2 + 2x - 2 \equiv 0 \pmod 5$. ***№5***. а) немає розв'язків; б) $x \equiv 5 \pmod 7$; в) $x \equiv 2 \pmod{13}$, $x \equiv 3 \pmod{13}$. ***№6***. а) $x^5 - 5x^4 + 7x^3 - 8x^2 + 2x - 5 \equiv 0 \pmod{11}$; б) $x^3 - 6x^2 + 7x - 10 \equiv 0 \pmod{15}$; в) $x^3 + 18x^2 - 55x + 42 \equiv 0 \pmod{59}$. ***№7***. а) 4; б) 2; в) 2; г) 6; д) 10.

Завдання для самостійного розв'язування

№1. За допомогою критерію Ейлера встановити, чи мають розв'язки конгруенції:

а) $x^2 \equiv 5 \pmod 7$; б) $x^2 \equiv 7 \pmod{11}$; в) $x^2 \equiv 12 \pmod{13}$.

№2. За допомогою символу Лежандра встановити, чи мають розв'язки конгруенції:

а) $x^2 \equiv 33 \pmod{179}$; б) $x^2 \equiv 65 \pmod{193}$;

в) $x^2 \equiv 26 \pmod{241}$; г) $x^2 \equiv 30 \pmod{269}$;

д) $x^2 \equiv 42 \pmod{251}$.

№3. Знайти розв'язок конгруенцій найпростішим способом:

а) $x^2 \equiv 20 \pmod{31}$; б) $x^2 \equiv 7 \pmod{59}$;

в) $x^2 \equiv 7 \pmod{31}$.

№4. Замінити дані конгруенції рівносильними їм конгруенціями, степені яких нижче модуля:

а) $x^9 - 3x^4 + 2x^3 - x + 3 \equiv 0 \pmod 7$;

б) $x^{10} + 3x^5 - 4x^3 + x^2 - 3 \equiv 0 \pmod 7$;

в) $x^{14} - x^{12} + 3x^5 - 6x^2 + x + 1 \equiv 0 \pmod{11}$.

№5. Розв'язати конгруенції:

а) $x^8 - x^4 + 2x - 3 \equiv 0 \pmod 5$;

б) $x^{12} + 2x^{11} - 2x - 1 \equiv 0 \ (mod\ 11)$.

№6. Замінити дані конгруенції рівносильними зі старшим коефіцієнтом рівним одиниці:

а) $2x^5 - 4x^4 + 3x^3 - 2x + 3 \equiv 0 \ (mod\ 13)$;

б) $3x^6 - 2x^5 + 3x^3 + 2x^2 - 3 \equiv 0 \ (mod\ 7)$;

в) $5x^4 - 3x^3 + 2x^2 - x + 5 \equiv 0 \ (mod\ 11)$.

№7. Знайти порядок $P_m\ (a)$, числа a за модулем m, якщо:

а) $a = 4, m = 15$; б) $a = 2, m = 15$;

в) $a = 2, m = 17$; г) $a = 7, m = 20$;

д) $a = 6, m = 39$.

№8. Скласти таблиці індексів за модулем p з основою g, якщо:

а) p=29, g=2; б) p=13, g=2.

№9. Розв'язати конгруенцію, використовуючи результати №8:

а) $5x^{11} \equiv -19 \ (mod\ 29)$; б) $2x^8 \equiv 5 \ (mod\ 13)$.

Відповіді: ***№1.*** а) немає розв'язків; б) немає розв'язків; в) має розв'язки. ***№2.*** а) немає розв'язків; б) немає розв'язків; в) немає розв'язків. ***№3.*** а) $x \equiv 12 \ (mod\ 31)$, $x \equiv 19 \ (mod\ 31)$; б) $x \equiv 19 \ (mod\ 59)$, $x \equiv 40 \ (mod\ 59)$; в) $x \equiv 5 \ (mod\ 31)$, $x \equiv 26 \ (mod\ 31)$. ***№4.*** а) $-3x^4 + 3x^3 - x + 3 \equiv 0 \ (mod\ 7)$. ***№5***. а) $x \equiv 4 \ (mod\ 5)$; б) $x \equiv 1 \ (mod\ 11)$, $x \equiv 10 \ (mod\ 11)$. ***№6.*** а) $x^5 - 2x^4 + 8x^3 - x + 8 \equiv 0 \ (mod\ 13)$; б) $x^6 - 3x^5 + x^3 + 3x^2 - 1 \equiv 0 \ (mod\ 7)$. №7. а) 2; б) 4; в) 8; г) 4; д) не існує.

Тема шоста
МНОГОЧЛЕНИ ВІД ОДНІЄЇ ЗМІННОЇ. КІЛЬЦЕ МНОГОЧЛЕНІВ НАД ОБЛАСТЮ ЦІЛІСНОСТІ

Попередні зауваження

Поняття многочлена не є новим для читача. З цим поняттям зустрічалися як у середній школі, так і під час вивчення математичного аналізу. З курсу математичного аналізу відомо, що многочленом від однієї змінної є ціла раціональна функція виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ...+a_1 x+a_0 \qquad (6.1)$$

задана на всій дійсній осі, де коефіцієнти a_n, a_{n-1} ..., a_1, a_0 – довільні задані дійсні числа. В аналізі вивчались деякі властивості многочленів від дійсної змінної, зокрема їх неперервність, вирази для похідних різного порядку тощо. Найпростіші типи многочленів (зокрема лінійну функцію $f(x)= ax + b$ та квадратну функцію $f(x)=ax^2+bx + c$) досить детально вивчають ще в середній школі.

З другого боку, в алгебрі многочлени зустрічались у зв'язку з розв'язуванням алгебраїчних рівнянь вищих степенів з одним невідомим, тобто рівнянь виду

$$a_n x^n + a_{n-1}x^{n-1} + ... +a_1 x + a_0 = 0,$$

ліва частина яких є многочлен від однієї змінної. На відміну від аналізу, в алгебрі многочлени вважаються цілими раціональними функціями *комплексної* змінної, тобто виразами, в яких коефіцієнти a_n, a_{n-1}, ..., a_1, a_0 є комплексні числа, а змінна x може набувати довільних комплексних значень. Хоч трактування многочленів як функцій комплексної змінної достатнє для потреб дослідження і розв'язування алгебраїчних рівнянь з числовими коефіцієнтами, ми все ж таки покладемо в основу дальшого викладу ще більш загальний погляд на многочлен. Адже ми тепер знайомі не лише з числовими, а й з абстрактними алгебраїчними структурами (кільцями, полями, лінійними

просторами, алгебрами та ін.), і природно ставити питання про існування, кількість та способи знаходження розв'язків рівнянь, в яких коефіцієнти та невідоме є елементи деякої абстрактної алгебраїчної структури, причому дії додавання і множення, за допомогою яких утворено многочлен, є операції цієї структури, а 0 – її нульовий елемент.

Звичайно, абстрактне означення многочленів повинно бути таким, щоб їх властивості узагальнювали важливі з теоретичного і практичного погляду властивості многочленів з числовими коефіцієнтами.

Означення многочлена

Вираз виду (6.1) повністю визначається коефіцієнтами $a_n, a_{n-1}, ..., a_1, a_0$. Але ці коефіцієнти не можуть бути цілком довільними об'єктами. Для можливості виконання операцій додавання та множення многочленів за тими самими правилами, що й в елементарній математиці, коефіцієнти розглядуваних многочленів повинні належати деякому комутативному кільцю R. Крім того, кільце R не повинно мати дільників нуля, тобто, щоб $ab = 0 \leftrightarrow a = 0$ або $b = 0$, для довільних $a, b \in R$ (0 – нульовий елемент кільця).

Комутативне кільце, в якому не існує дільників нуля, називається *областю цілісності*. Отже, коефіцієнти многочленів, які ми розглядаємо, належать деякій області цілісності R.

Означення. *Многочленом* (поліномом) *від однієї змінної над областю цілісності R називається вираз виду* (6.1), *де n – довільне ціле невід'ємне число,* $a_n, a_{n-1}, ..., a_1, a_0$ – елементи R, *а* x (або x^1), x^2, ... x^{n-1}, x^n – деякі символи; x^k *називається k-м степенем змінної* x (або невідомого x), *а* a_k *– k-м коефіцієнтом многочлена* (6.1) *або коефіцієнтом при* x^k ($k = 0, 1, ..., n$).

Многочлен повністю визначається своїми коефіцієнтами $a_n, a_{n-1}, ..., a_1, a_0$, а символи $x^n, x^{n-1}, ..., x$ відіграють поки що, так би мовити, роль «розділових знаків», що відокремлюють коефіцієнти один від одного та упорядковують їх. Зауважимо також, що знак «+» у символічному записі (6.1) поки що не є позначенням якоїсь операції, вираз $a_k x^k$ не є добутком a_k на x^k, а x^k не є добутком k

множників x. По суті, многочлен (6.1) можна було б записати просто як упорядковану сукупність коефіцієнтів або як (n+1)-вимірний вектор (a_n, a_{n-1}, ..., a_1, a_0). Проте, як виявиться далі, запис у формі (6.1) має переваги над векторним записом.

Многочлени від змінної x позначатимемо малими латинськими буквами: $f(x)$, $g(x)$, $q(x)$, $s(x)$ тощо, сукупність усіх многочленів від x над областю цілісності R – символом $R[x]$.

***Означення**. Вираз a_kx^k (k = 1, ..., n-1, n) називається k-м членом або членом k-го степеня многочлена $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, a_0 – нульовим або вільним членом, причому записи a_0 і a_0x^0 рівнозначні. Якщо $a_k = 0$ (тобто є нульовим елементом області цілісності R), то кажуть, що k-й член многочлена $f(x)$ дорівнює нулю або його немає.*

Відповідно до означень різні члени многочлена від однієї змінної є завжди членами різних степенів. Зауважимо, що *k-й* коефіцієнт a_k многочлена іноді називають коефіцієнтом його *k*-го члена.

У виразі для многочлена (6.1) члени, які дорівнюють нулю, можна не писати. Так, многочлен

$$f(x) = 0x^5 + 2x^4 + 0x^3 + 0x^2 + 0x + 4,$$

розглядуваний як многочлен над кільцем усіх парних цілих чисел (це кільце, як відомо, є областю цілісності), можна записати коротше:

$$f(x) = 2x^4 + 4.$$

Обидва записи містять ту саму інформацію про многочлен: нульовий коефіцієнт його дорівнює 4, четвертий – 2, решта коефіцієнтів дорівнюють нулю. Роль «розділових символів» x^k у записі многочлена, як бачимо, саме в тому і полягає, щоб цю інформацію зробити незалежною від способу запису. Єдина незручність, яка при цьому залишається, полягає у тому, що ми не можемо однозначно сказати, що розуміємо під «рештою коефіцієнтів». Зрозуміло, що в цю решту напевно входять a_1, a_2, a_3.

***Означення**. Відмінний від нуля член многочлена $f(x)$, степінь якого більший за степінь усіх інших відмінних від нуля членів цього многочлена, називається старшим*

членом, його коефіцієнт – старшим коефіцієнтом, а його степінь – степенем многочлена $f(x)$.

Степінь многочлена $f(x)$ позначають ***deg f.***

Домовимось тепер, що будь-який многочлен $f(x)$ записуватимемо так, щоб запис починався із старшого члена, тобто, не включати у запис рівних нулю членів, степінь яких більший за *deg f.* Згідно з цією домовленістю будь-який многочлен *n-го* степеня подаватимемо, як правило, у вигляді (6.1), причому $a_n \neq 0$, а з решти коефіцієнтів частина або всі можуть бути рівні нулю. Цей запис характеризується тим, що члени упорядковано за спаданням степеня x^k . Таку форму запису називають *канонічною.* Вживають також назву *«многочлен стандартного виду».* Ми переважно користуватимемося канонічною формою запису многочленів, хоч в окремих випадках будуть зручні інші форми (наприклад, розміщення членів у порядку зростання степенів).

Зокрема, довільний многочлен першого степеня над областю цілісності R можна записати так: $f(x)=a_1x+a_0$ (a_1, $a_0 \in R$, $a_0 \neq 0$); такі многочлени називають також *лінійними двочленами.*

Будь-якому многочлену нульового степеня можна надати вигляду $f(x)=a_0$ ($a_0 \in R$, $a_0 \neq 0$). Многочлени нульового степеня називають також *константами*. Очевидно, будь-який елемент $a \in R$, відмінний від нульового, можна розглядати як многочлен нульового степеня над R. Елемент $0 \in R$ ми також вважатимемо константою і многочленом над R; цей многочлен називатимемо *нуль-многочленом* і позначатимемо $\theta(x)$, тобто $\theta(x)=0$. Нуль-многочлену не приписують жодного степеня. Все ж нам буде зручно вважати, що канонічна форма охоплює і випадок нуль-многочлена, тобто допускати у цій формі при $n=0$ випадок $a_n = 0$.

Слід, отже, мати на увазі, що завжди істинна імплікація $[\deg f = n] \rightarrow [a_n \neq 0]$, але якщо в канонічній формі $n=0$, то a_n може бути будь-яким елементом області цілісності R (хоч при $a_0 = 0$ не вважаємо $n = 0$ степенем многочлена).

У дальшому викладі ми іноді припускатимемо деяку мовну вільність і тлумачитимемо висловлення «степінь многочлена $f(x)$ менший (не більший) за n» так: «$f(x)=\theta(x)$

або deg $f < n$ (deg $f \le n$)». Зокрема, усі константи можна вважати многочленами, степінь яких не більший від нуля (або, як кажуть, многочленами не вище від нульового степеня).

Дії над многочленами

Многочлени, як і вектори, становлять інтерес не самі по собі, а як об'єкти деяких алгебраїчних операцій.

Нехай дано два многочлени над областю цілісності *R.*

$$f(x)= a_n x^n+a_{n-1}x_{n-1} +...+a_1x+a_0 \ (a_i \in R, i=0,\ 1, \dots , n), \qquad (6.1)$$

$$g(x)= b_m x^m+b_{m-1}x^{m-1}+...+b_1x+b_0 \ (b_j \in R, j=0,\ 1, ..., m). \qquad (6.2)$$

***Означення**. Многочлени $f(x)$ і $g(x)$ називають рівними між собою і записують $f(x)=g(x)$, якщо канонічні форми цих многочленів збігаються, тобто*

$$f(x) = g(x) \rightarrow n=m \text{ і } a_k=b_k .$$

Якщо $f(x)$ і $g(x)$ відмінні від $\theta(x)$, то останню рівність можна переписати у вигляді

$$f(x) = g(x) \rightarrow deg\, f = deg\, g \text{ і } a_k= b_k,$$

а для випадку нуль-многочлена можна записати

$$f(x) = \theta(x) \rightarrow (deg\, f = 0) \text{ і } a_0 = 0.$$

Нерівність deg $f \le 0$ тут означає, що $f(x)$ не має членів ненульового степеня.

З означення безпосередньо випливає, що рівність многочленів має властивості рефлексивності, симетричності та транзитивності, тобто є відношенням еквівалентності на множині $R[x]$. Природно рівні між собою многочлени вважати тим самим многочленом. Так само природно вживати означення $f(x) \neq g(x)$ для висловлення $\overline{f(x) = g(x)}$, тобто заперечення рівності многочленів $f(x)$ і $g(x)$.

Означимо тепер суму многочленів. Без обмеження загальності можна вважати, що $n \ge m \ge 0$.

***Означення**. Сумою многочленів $f(x)$ і $g(x)$ називається многочлен*

$$s(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_{m+1}x^{m+1} + (a_m + b_m)x^m + \\ +(a_{m-1} + b_{m-1})x^{m-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

Те, що $s(x)$ є сумою многочленів $f(x)$ і $g(x)$, записують так: $s(x)= f(x) + g(x)$.

З цього означення випливають наслідки.

Наслідок 1. *Якщо $f(x) \in R[x]$, $g(x) \in R[x]$, то й $f(x)+g(x) \in R[x]$.*

Наслідок 2. *Степінь суми двох многочленів не перевищує більшого з степенів даних многочленів: $deg\,(f+g) \le \max\{deg\,f, deg\,g\}$.*

Наслідок 3. *Для довільного многочлена $f(x) \in R[x]$ і $\theta(x) \in R[x]$: $f(x)+ \theta(x)= f(x)$.*

***Означення**. Добутком многочленів $f(x)$ і $g(x)$ називається многочлен*

$$p(x) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \ldots + c_1x + c_0\,,$$

де

$c_k = a_kb_0 + a_{k-1}b_1 + \ldots + a_1b_{k-1} + a_0b_k$, $k=0, 1,\ldots, n+m$, $a_{k-j}=0$ $(j=0,1,\ldots,k)$ *при* $k - j>n$, $b_j=0$ *при* $j>m$.

Те, що $p(x)$ є добуток многочленів $f(x)$ і $g(x)$, записують так: $p(x)=f(x)g(x)$ або $p(x) = f(x)\cdot g(x)$.

Зауважимо що, якщо $f(x)$ – будь-який многочлен над R, a_i – його коефіцієнти, $n = deg\,f$, то символ a_i при $i > n$ означає нульовий елемент кільця R.

Наслідок 4. *Якщо $f(x) \in R[x]$, $g(x) \in R[x]$, то й $f(x)\cdot g(x) \in R[x]$.*

Наслідок 5. *Якщо $f(x)$ і $g(x)$ не є нуль-многочлени, то $deg\,(fg)=deg\,f+deg\,g$.*

Справді, нехай $deg\,f\,(x) = n$, $deg\,g = m$. Оскільки $f(x)\ne\theta(x)$, $g(x)\ne\theta(x)$, *то* $a_n\ne0$, $b_m\ne0$. Але тоді $c_{n+m}=a_nb_m\ne0$, бо R є область цілісності і тому в R не існує дільників нуля, що неможливо. Звідси випливає істинність наслідку 5.

Зауважимо, що саме під час доведення наслідку 5 ми вперше використали те, що R – не просто кільце, а область цілісності.

Наслідок 6. *$f(x)=\theta(x)$ або $g(x)=\theta(x)$, то $f(x)\cdot g(x) = \theta(x)$, тобто при множенні двох многочленів, з яких хоча б один є нуль-многочленом, отримуємо нуль-многочлен.*

В п. 2 ми домовились розглядати елементи $a \in R$ як многочлени не вище нульового степеня над R. Після того як введено означення рівності між многочленами та дій над ними, потрібно переконатись, що в застосуванні до елементів кільця R як до многочленів не вище нульового степеня, ці означення збігаються з означеннями рівності та відповідних операцій у кільці R.

Але це справді так, бо якщо $f(x) = a_0$, $g(x) = b_0$ – многочлени не вище нульового степеня над R (зокрема, це можуть бути і нуль-многочлени), то

$$f(x)=g(x) \rightarrow a_0=b_0, f(x)+g(x)=a_0+b_0, f(x)\, g(x)=a_0b_0,$$

тобто рівність цих многочленів рівносильна рівності відповідних елементів кільця R, а сума (добуток) цих многочленів є сумою (добутком) відповідних елементів R (у розумінні операцій в кільці R).

Тим самим перевірено коректність розгляду елементів області цілісності R як многочленів над R не вище нульового степеня. Точніше, показано ізоморфізм між сукупністю усіх многочленів не вище нульового степеня над R і самим кільцем R. Саме це і дає право ототожнювати многочлен не вище нульового степеня з відповідним елементом кільця R.

Зокрема, нуль-многочлен $G(x)$ можна розглядати як нульовий елемент кільця R, в зв'язку з чим ми у більшості випадків замість $\theta(x)$ писатимемо 0.

Кільце многочленів над областю цілісності

Нехай, як і раніше, R – область цілісності, $R[x]$ – сукупність усіх многочленів над R. Звичайно, властивості $R[x]$ визначаються властивостями області цілісності R і можуть бути істотно різними для різних областей цілісності R. Наприклад, многочлен $f(x)=x^4+1$ з числовими коефіцієнтами $a_4=4$, $a_3=a_2=a_1=0$, $a_0=1$ можна розглядати і як многочлен над кільцем усіх цілих чисел, і як многочлен над полями Q, R, C усіх раціональних, дійсних та комплексних чисел відповідно (всі ці структури є областями цілісності). Але $f(x)$, як елемент різних із цих сукупностей, має різні властивості. Так, у $C[x]$ многочлен $f(x)$ розкладається на

лінійні множники, тобто може бути поданий як добуток двох лінійних двочленів з $C[x]$:

$$f(x)=4x^2+1=(2x+i)(2x-i)=g(x)h(x),\ g(x)h(x)\in C[x].$$

Той же час у множинах $Z[x]$, $Q[x]$, $R[x]$ таких двочленів не існує, і вказаний розклад неможливий. Отже, властивість $f(x)$ розкладатись на лінійні множники залежить від того, над якою областю цілісності розглядаємо цей многочлен.

Проте існують властивості сукупності $R[x]$ многочленів над областю цілісності R, які не залежать від специфічних особливостей R, а лише від того, що R є областю цілісності. Саме такі спільні для усіх $R[x]$ властивості ми тут і розглянемо.

***Теорема**. Сукупність $R[x]$ усіх многочленів над областю цілісності R є область цілісності відносно операцій додавання та множення многочленів.*

***Теорема**. $R[x]$ є кільце з одиницею тоді і тільки тоді, коли R є кільце з одиницею.*

Справді, якщо в R існує одиниця 1, то вона, розглядувана як многочлен нульового степеня, є одиницею і в кільці $R[x]$, бо $f(x)\cdot 1=f(x)$. Навпаки, нехай $\boldsymbol{e}(x)$ – одиниця кільця многочленів, тобто для довільного $f(x)\in R[x]$, $f(x)\cdot\boldsymbol{e}(x)=f(x)$.

Зрозуміло, що $\boldsymbol{e}(x)$ відмінний від нуль-многочлена і є многочлен нульового степеня (бо $deg\ f+deg\ \boldsymbol{e}=deg\ f \rightarrow deg\ \boldsymbol{e}=0$), тобто ненульовий елемент кільця R. Далі, з рівності $f(x)\cdot\boldsymbol{e}(x)=f(x)$ випливає $a_0\boldsymbol{e}=a_0$, *де* a_0 *- довільний* член многочлена $f(x)$. Оскільки $f(x)$ – довільний многочлен з $R[x]$, то a_0 – довільний елемент з R. Тому $a_0\boldsymbol{e}=a_0 \rightarrow \boldsymbol{e}=1$, тобто $\boldsymbol{e}$ – одиниця кільця R. Цим наше твердження доведено.

Оскільки $R[x]$ є кільце, можна розглядати різницю будь-яких многочленів як дію обернену до додавання.

У зв’язку з тим, що всі елементи $a\in R$ можна розглядати як многочлени над R, то в $R[x]$ означено не тільки дії додавання і множення, а й операцію *множення на елементи з* R. Ураховуючи це, можна показати, що $R[x]$ є лінійний простір і алгебра над R.

Функціональне тлумачення многочлена

Нехай $f(x)=a_nx^n+a_{n-1}x_{n-1}$ + ... + a_1x+a_0 – многочлен над областю цілісності R, а C – деяке комутативне кільце, що є розширенням R. Якщо α – будь-який елемент з C, то має сенс такий вираз:

$$a_n\alpha^n + a_{n-1}\alpha_{n-1} + ... + a_1\alpha+a_0, \qquad (6.3)$$

бо в C визначено дії множення і додавання над елементами a_i, α.

Вираз (6.3) *утворений з* $f(x)$ *заміною символа* x *елементом* α. *У зв'язку з цим його позначають* $f(\alpha)$ *і називають значенням многочлена* $f(x)$ *при* $x = \alpha$ *(або* «в *точці* α»). *Очевидно*, $f(\alpha)$ є елементом C. Кожному $\alpha \in C$ відповідає за цим *правилом єдиний цілком певний* елемент $f(\alpha) \in C$. Пригадуючи загальне означення функції (відображення), можемо висловити таке твердження.

Теорема. *Якщо* $f(x)$ *– будь-який многочлен над областю цілісності* R, *а* C *– деяке комутативне кільце, яке є розширенням* R, *то, поставивши кожному елементу* $\alpha \in C$ *у відповідність елемент* $f(\alpha) \in C$, отримуємо функцію $\varphi_f: C\to C$; $\varphi_f(\alpha)=f(\alpha)$.

Іншими словами, *многочлен* $f(x)=R[x]$ *визначає відображення* φf *будь-якого комутативного розширення* C *кільця* R *у себе.*

Нагадаємо, що сумою (добутком) двох функцій $\varphi: X\to Y$, $\psi: X\to Y$, називається функція $\chi: X\to Y$ така, що

$$\chi(x)=\varphi(x)+\psi(x),\ \chi(x)=\varphi(x)\psi(x),\ \text{для будь-якого } x \in X.$$

Звичайно, це означення передбачає, що у множині Y означено операцію додавання (множення) елементів.

Нехай тепер $f(x)$, $g(x)$ – многочлени над R і $s(x)= = f(x)+g(x)$; $p(x)=f(x)g(x)$ – сума і добуток цих многочленів у розумінні п.3. Як відомо, $s(x) \in R[x]$ і $p(x) \in R[x]$.

Якщо C – деяке комутативне розширення кільця R, то можна розглянути функції $f: C\to C$, $g: C\to C$, $s: C\to C$, $p: C\to C$. Щоб функцію s можна було розглядати як суму, а функцію p – як добуток функцій f і g слід скористатися теоремою.

Теорема. *Нехай*

$$f(x) = \sum_{k=0}^{n} a_k x^k,\ g(x) = \sum_{k=0}^{m} b_k x^k$$

– многочлени над областю цілісності R, $s(x) = f(x)+g(x)$; $p(x) = f(x)g(x)$ *а C – будь-яке комутативне розширення кільця R. Тоді для будь-якого* $\alpha \in C$: $s(\alpha)=f(\alpha)+g(\alpha)$, $p(\alpha)=f(\alpha)g(\alpha)$, *тобто*

$$\varphi_s=\varphi_f+\varphi_g,\ \varphi_p=\varphi_f\cdot\varphi_g.$$

Отже, введені в п.3 означення суми і добутку многочленів узгоджені з загальними поняттями суми і добутку функцій.

Зауваження. Ми вимагали, щоб *C* було комутативним розширенням кільця *R.* Проте для того, щоб сказане про функціональний сенс многочлена було *справедливим, досить, щоб C було кільцем, усі елементи якого комутують з будь-яким елементом комутативного підкільця R.*

Спираючись на це зауваження, можна, зокрема, розглядати многочлени як функції від матриць. Точніше, нехай *R* – будь-яка область цілісності, а M_n – кільце квадратних матриць *n*-го порядку, елементи яких належать *R.* Як відомо M_n можна розглядати як розширення кільця *R,* ототожнюючи кожний елемент $a \in R$ з діагональною матрицею

$$a = \begin{pmatrix} \alpha & 0 & \dots & 0 \\ 0 & \alpha & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha \end{pmatrix} \in M_n,$$

оскільки $a \to \alpha$ є ізоморфізм. При цьому будь-який елемент $\beta \in M_n$, переставний з будь-яким елементом $\alpha \in R$ (адже діагональні матриці переставні з довільними матрицями з M_n). Саме ж кільце M_n, як відомо, не є комутативним.

Отже, якщо $f(x) = \sum_{k=0}^{n} a_k x^k$ - многочлен над *R,* а *A* – будь-яка матриця з M_n, то $f(A)=a_nA^n+\dots+a_1A+a_0$ також є матрицею з M_n і $f(x)$ можна розглядати як функцію $\phi_f: M_n \to M_n$.

Функції (зокрема, многочлени) від матриць широко використовують у математиці. Все ж у дальшому викладі, якщо не зазначене супротивне, ми завжди вважатимемо C комутативним розширенням R.

Перейдемо тепер до розгляду питання про рівність многочленів. Згідно з означенням п.3, для многочленів

$$f(x)=\sum_{k=0}^{n} a_k x^k \ , g(x)=\sum_{k=0}^{m} b_k x^k$$

$$f(x)=g(x)\equiv m=n \wedge [a_k=b_k],\ k=0, 1,\ldots, n.$$

З другого боку, дві функції $\varphi: X\to Y$, $\psi: X\to Y$, вважають рівними між собою, якщо значення цих функцій рівні між собою при всіх $x \in X$ (або, як кажуть, якщо ці функції тотожно рівні на X).

Отже, рівносильність алгебраїчного і функціонального означень рівності многочленів $f(x)$ і $g(x)$ означає, що є істинною еквіваленції: для будь-якого $\alpha \in C$:

$$f(\alpha)=g(\alpha)\leftrightarrow m=n \wedge [a_k=b_k]\ k=0, 1,\ldots, n, \qquad (6.4)$$

де C – будь-яке комутативне розширення кільця R. Зрозуміло, що рівність буде істинне для довільного C, якщо буде істинне для $C = R$.

Слід відразу зауважити, що у випадку довільної області цілісності R правильність (6.4) стверджувати не можна. Проте можна навести умови, які досить накласти на область цілісності R, щоб справджувалась еквіваленція (6.4).

***Теорема**. Якщо R – область цілісності характеристики* 0, *то многочлен* $q(x)\in R[x]$ *є нуль-многочленом тоді і тільки тоді, коли його значення в усіх точках області R дорівнюють нулю* (або $q(x)$ дорівнює нулю тотожно на R).

Наслідок. *Якщо R – область цілісності характеристики* 0, *то многочлени* $f(x), g(x) \in R[x]$ *рівні між собою тоді і тільки тоді, коли їх значення в довільній точці області R рівні між собою.*

Приклади розв'язування типових завдань

№1. *Скласти многочлен за даними його коефіцієнтами:* 1, 0, 0, 4, 0, 2, 0, 3, -1, *якщо вони розміщені в порядку спадання степенів.*

Розв'язання. Задано дев'ять коефіцієнтів, тому заданий многочлен є 8 степеня, оскільки многочлен необхідно записувати у стандартному вигляді, то a_8=1, a_7=a_6=a_4=a_2=0, a_5=4, a_3=2, a_1=3, a_0= -1. Отже, нехай маємо многочлен $f(x)$, тоді $f(x)=x^8+4x^5+2x^3+3x-1$.

№2. *Виконати додавання, віднімання, множення многочленів:*

а) $f(x) = x^5 - 3x^4 + 2x^2 + 3x - 10,$

$g(x) = x^5 + 4x^3 - 6x^2 + x - 2;$

б) $f(x) = \bar{2}x^3 + \bar{3}x^2 + x - \bar{1},$

$g(x) = \bar{2}x^2 + \bar{4}x + \bar{3}$ у кільці $Z_5[x]$.

Зауваження. Запис $\bar{a}$ означає, що дане число записане не у десятковій системі числення, а в іншій, указаній в умові. У нашому випадку, ці числа записані у п'ятирічній системі числення.

Розв'язання.

а) $f(x) + g(x) = (x^5 - 3x^4 + 2x^2 + 3x - 10) +$
$+(x^5 + 4x^3 - 6x^2 + x - 2) = 2x^5 - 3x^4 + 4x^3 - 4x^2 + 4x -$
$-12;$

$f(x) - g(x) = (x^5 - 3x^4 + 2x^2 + 3x - 10) -$
$-(x^5 + 4x^3 - 6x^2 + x - 2) = -3x^4 - 4x^3 + 8x^2 + 2x - 8;$

$f(x) \cdot g(x) = (x^5 - 3x^4 + 2x^2 + 3x - 10) * (x^5 + 4x^3 -$
$- 6x^2 + x - 2) = x^{10} + 4x^8 - 6x^7 + x^6 - 2x^5 - 3x^9 -$
$- 12x^7 + 18x^6 - 3x^5 + 6x^4 + 2x^7 + 8x^5 - 12x^4 + 2x^3 -$
$- 4x^2 + 3x^6 + 12x^4 - 18x^3 + 3x^2 + 20 - 10x^5 - 40x^3 +$
$+ 60x^2 - 10x + 20 = x^{10} - 3x^9 + 4x^8 - 16x^7 + 22x^6 -$
$- 7x^5 + 6x^4 - 56x^3 + 59x^2 - 10x + 20;$

б) $f(x) + g(x)=(\bar{2}x^3 + \bar{3}x^2 + x - \bar{1}) + (\bar{0}x^3 + \bar{2}x^2 + \bar{4}x +$
$+\overline{3}) = (\bar{2} + \bar{0})x^3 + (\bar{3} + \bar{2})x^2 + (\bar{1} + \bar{4})x + (-\bar{1} + \bar{3}) =$
$= \bar{2}x^3 + \bar{0}x^2 + \bar{0}x + \bar{2} = \bar{2}x^3 + \bar{2};$

$f(x)-g(x)=(\bar{2}x^3+\bar{3}x^2+x-\bar{1})-(\bar{0}x^3+\bar{2}x^2+\bar{4}x+$
$+\overline{3})=(\bar{2}-\bar{0})x^3+(\bar{3}-\bar{2})x^2+(\bar{1}-\bar{4})x+(-\bar{1}-\bar{3})=\bar{2}x^3+$
$+\bar{1}x^2-\bar{3}x-\bar{4}=\bar{2}x^3+x^2-\bar{3}x-\bar{4};$

$f(x)\cdot g(x)=(\bar{2}x^3+\bar{3}x^2+x-\bar{1})\cdot(\bar{2}x^2+\bar{4}x+\bar{3})=$
$=(\bar{2}\cdot\bar{2})x^5+(\bar{2}\cdot\bar{4}+\bar{3}\cdot\bar{2})x^4+(\bar{2}\cdot\bar{3}+\bar{3}\cdot\bar{4}+\bar{1}\cdot\bar{2})x^3+$
$+(\bar{3}\cdot\bar{3}+\bar{1}\cdot\bar{4}+(-\bar{1})\cdot\bar{2})x^2+(\bar{1}\cdot\bar{3}+(-\bar{1})\cdot\bar{4})x+(-\bar{1})\cdot$
$\cdot\bar{3}=\bar{4}x^5+\bar{4}x^4+\bar{0}x^3+x^2-x-\bar{3}=-x^5-x^4+x^2-$
$-x-\bar{3}.$

Відповідь: а) $f(x)+g(x)=2x^5-3x^4+4x^3-4x^2+$
$+4x-12;\ \ f(x)-g(x)=-3x^4-4x^3+8x^2+2x-8;$

$f(x)\cdot g(x)=x^{10}-3x^9+4x^8-16x^7+22x^6-7x^5+$
$+6x^4-56x^3+59x^2-10x+20;$

б) $f(x)+g(x)=\bar{2}x^3+\bar{2};$

$f(x)-g(x)=\bar{2}x^3+x^2-\bar{3}x-\bar{4};$

$f(x)\cdot g(x)=-x^5-x^4+x^2-x-\bar{3}.$

№3. *Записати у стандартному вигляді многочлен та визначити його степінь:*

а) $f(x)=x^2+4x^4+2x^3+3x^2-1+5x^8-4x^6+2x^8+3x-x^8+4x^5+2x^3+3x;$

б) $f(x)=\bar{2}x^5+\bar{3}x^2+\bar{4}x^3+x-\bar{3}x^4+\bar{2}x^2-\bar{1}x^3-\bar{1}$, у кільці $Z_5[x]$.

Розв'язання. У многочлені стандартного вигляду члени розташовані за спаданням степеня змінної. Зведемо подібні доданки.

а) $f(x)=x^2+4x^4+2x^3+3x^2-1+5x^8-4x^6+2x^8+3x-$
$-x^8+4x^5+2x^3+3x=6x^8-4x^6+4x^5+4x^4+4x^3+4x^2+3x-1,$
$deg\ f(x)=8;$

б) $f(x)=\bar{2}x^5+\bar{3}x^2+\bar{4}x^3+\bar{1}x-\bar{3}x^4+\bar{2}x^2-\bar{1}x^3+-\bar{1}+$
$+\bar{2}x^4-\overline{4}=\bar{2}x^5+\left(-\bar{3}+\overline{2}\right)x^4+\overline{(4-1)}x^3+\left(\bar{3}+\overline{2}\right)x^2+$
$+\overline{1}x-\left(\overline{1}+\overline{4}\right)=\bar{2}x^5+\overline{4}x^4+\bar{3}x^3+\overline{1}x,$

$deg\ f(x)=5.$

№4. *Знайти всі цілі числа a, b, при яких многочлен* $f(x)=x^4+ax^3+bx^2-8x+4$ *є квадратом деякого многочлена* $g(x)$ *з кільця* $Z[x]$*, та записати многочлен* $g(x)$*.*

Розв'язання. Многочлен $f(x)$ має степінь 4. Тому степінь шуканого многочлена $g(x)$ (якщо він існує) дорівнює 2. Нехай $g(x)=mx^2+nx+p,\ m\neq 0,$ і многочлен $f(x)$ та $(g(x))^2$

дорівнюють один одному. Запишемо многочлен $(g(x))^2$ у канонічній формі:

$(g(x))^2 = (mx^2+nx+p)^2 = m^2x^4+2mnx^3+(2mp+n^2)x^2+ +2npx+p^2.$

З умови рівності многочленів маємо систему рівнянь:

$$\begin{cases} m^2 = 1 \\ 2mn = a \\ 2mp + n^2 = b. \\ 2np = -8 \\ p^2 = 4 \end{cases}$$

З першого рівняння системи знаходимо, що $m \in \{1, -1\}$, а з останнього $p \in \{2, -2\}$. Це означає, що дана система рівнянь рівносильна сукупності чотирьох систем:

$$\begin{cases} m = 1 \\ p = 2 \\ n = -2; \\ a = -4 \\ b = 8 \end{cases} \quad \begin{cases} m = 1 \\ p = -2 \\ n = 2 \ ; \\ a = 4 \\ b = 0 \end{cases} \quad \begin{cases} m = -1 \\ p = 2 \\ n = -2 \, ; \\ a = 4 \\ b = 0 \end{cases} \quad \begin{cases} m = -1 \\ p = -2 \\ n = 2 \ . \\ a = -4 \\ b = 8 \end{cases}$$

Таким чином, якщо a = -4, b = 8, то існують два многочлени $g_1(x)=-x^2+2x-2$, $g_2(x)=x^2+2x+2$, які задовольняють умову задачі.

Якщо $a=4$, $b=0$, то існують два многочлени $g_1(x)=x^2+2x-2$, $g_2(x)=-x^2-2x+2$, які задовольняють умову задачі. Цим вичерпуються всі можливі випадки шуканого зображення многочлена $f(x)$.

Завдання для аудиторного заняття

№1. Скласти многочлен за даними його коефіцієнтами: 1, 0, 2, -4, 0, 1, 3, 5, *якщо вони розміщені в порядку спадання степенів.*

№2. Виконати додавання, віднімання, множення многочленів та вказати степінь отриманого многочлена:

а) $f(x) = x^4 - 3x^3 + 2x^2 + 3x - 6,$
$g(x) = x^5 + 6x^3 - 7x^2 + x - 1;$

б) $f(x) = 4x^4 - 8x^3 + 3x^2 - 8x + 4,$
$g(x) = x^4 - 2x^3 - 18x^2 - 6x + 9;$

в) $f(x) = 4x^4 - 4x^3 - 19x^2 + 106x,$
$g(x) = x^3 + 6x^2 + 30x + 25;$

г) $f(x) = \bar{2}x^4 + \bar{3}x^3 + \bar{4}x^2 + \bar{1}x - \bar{3},$
$g(x) = \bar{3}x^5 + \bar{2}x^3 - \bar{1}x^2 + \bar{2}x -$ в кільці $Z_5[x];$

д) $f(x) = \bar{3}x^5 + \bar{3}x^3 + \bar{4}x^2 + \bar{1}x - \bar{3},$
$g(x) = \bar{3}x^5 + \bar{2}x^3 + \bar{2}x^2 + \bar{2}x -$ в кільці $Z_6[x].$

№3. Визначити, які серед даних многочленів рівні:

$f(x) = sin\frac{\pi}{6} * x^3 - \sqrt{4 + 2\sqrt{3}}x^2 - x + arctg1 - \frac{\pi}{4} + 5^0,$

$g(x) = cos\frac{\pi}{2} * x^2 - (4 - (-2)^2)x - (3 - 9^{0,5}),$

$q(x) = 0{,}5x^3 - \left(1 + \sqrt{3}\right)x^2 + tg\frac{\pi}{4} - x,$ *s(x)=0.*

№4. При яких значеннях *a, b* наступні многочлени з кільця $Z[x]$ рівні між собою:
$f(x)=ax^2(x+1)+b(x^2+1)(x-6)+cx(x^2+1)$ та $g(x)=x^2+5x+6$?

№5. Знайти всі значення числа *a,* при яких многочлен $f(x)$ *є* квадратом деякого многочлена $g(x)$ з того самого кільця, та записати многочлен *g(x):*
а) $f(x)=x^4+6x^3+11x^2+ax+1$ з кільця $Z[x];$
б) $f(x) = \bar{4}x^4 + \bar{a}x^2 - \bar{1} -$ в кільці $Z_5[x].$

№6. Знайти всі цілі числа *a, b,* при яких многочлен $f(x)=x^3+ax^2+12x+b$ є кубом деякого многочлена $g(x)$ з кільця $Z[x].$

Відповіді: ***№1.*** $f(x)=x^7+2x^5-4x^4+x^2+3x+5.$ ***№2.*** а) $f(x) + g(x) = x^5 + x^4 + 3x^3 - 5x^2 + 4x - 7;$ $\deg q(x) = 5;$ $f(x) - g(x) = -x^5 + x^4 - 9x^3 + 9x^2 + 2x - 5;$ $\deg q(x) = 5;$ $f(x) \cdot g(x) = x^9 - 3x^8 + 8x^7 - 22x^6 + 28x^5 - 52x^3 + 43x^2 - 9x + 6;$ $\deg q(x) = 9;$ б) $f(x) + g(x) = 5x^4 - 10x^3 - 15x^2 - 14x + 13;$ $f(x) - g(x) = 3x^4 - 6x^3 + 21x^2 - 2x - 5;$ $f(x) \cdot g(x) = 4x^8 - 16x^7 - 53x^6 - 38x^5 + 194x^4 + 46x^3 + 3x^2 - 96x + 36;$
в) $f(x) + g(x) = 4x^4 - 3x^3 - 13x^2 + 136x + 25;$ $f(x) - g(x) = 4x^4 - 5x^3 - 25x^2 + 76x - 25;$ $f(x) \cdot g(x) = 4x^7 + 20x^6 + 77x^5 - 28x^4 + 479x^3 + 2705x^2 + 2650x.$

Завдання для самостійного розв'язування

№1. Скласти многочлен за даними його коефіцієнтами: 1, 2, -7, 6, 1, 3, 5, *якщо вони розміщені в порядку спадання степенів.*

№2. Виконати додавання, віднімання, множення многочленів:

а) $f(x) = 2x^4 - 7x^3 + 3x^2 + 3x - 4,$
$g(x) = 3x^5 - 6x^3 - 3x^2 + x - 2;$

б) $f(x) = 9x^4 - 8x^3 + 7x^2 - x + 3,$
$g(x) = x^4 - 3x^3 - 8x^2 - 7x + 4;$

в) $f(x) = 5x^4 + x^3 - 11x^2 + 10x - 6,$
$g(x) = 2x^3 + 4x^2 - 3x + 5;$

г) $f(x) = \bar{2}x^5 + \bar{3}x^3 + \bar{1}x^2 + \overline{1}x - \bar{3},$
$g(x) = \bar{3}x^5 + \bar{2}x^3 - \bar{1}x^2 + \bar{2}x -$ в кільці $Z_4[x]$.

№3. У кільці многочленів $Z_5[x]$ дано многочлени $f(x) = x^2 + \bar{3}x + \bar{2}, g(x) = \bar{4}x^2 + \bar{2}x + \bar{3}, h(x) = x^2 + + \bar{2}x + \bar{2}$. Перевірити, що $f(x) + g(x) = \bar{0}$, звідки $f(x) = -g(x)$; $f(x) \cdot h(x) = x^4 - \bar{1}$.

№4. При яких значеннях *a, b* наступні многочлени з кільця $Z[x]$ рівні між собою:

$f(x)=ax(x^2+3)+bx(x-1)+c(x+1)$ та $g(x)=2x^3+5x^2+8x+7$?

№5. Знайти всі значення числа *a,* при яких многочлен $f(x)=9x^4-12x^3+16x^2-8x+a$ є квадратом деякого многочлена $g(x)$ з того самого кільця $Z[x]$, та записати многочлен $g(x)$.

Відповіді: ***№1.*** $f(x)=x^6+2x^5-7x^4+6x^3+x^2+3x+5$ ***№2***. а) $f(x)\,g(x) = = 6x^9 - 21x^8 - 3x^7 + 45x^6 - 9x^5 - 36x^4 + 32x^3 + 9x^2 - 10x + + 8$; б) $f(x)\,g(x) = 9x^8 - 35x^7 - 41x^6 - 21x^5 + 42x^4 - 82x^3 + + 11x^2 - 25x + 12$; в) $f(x)\,g(x) = 10x^7 + 22x^6 - 33x^5 - 2x^4 + + 66x^3 - 109x^2 + 68x - 30$.

Тема сьома
ТЕОРІЯ ПОДІЛЬНОСТІ МНОГОЧЛЕНІВ

Многочлени над полем

Досі ми розглядали кільце многочленів над *областю* цілісності *R.* Хоч означення кільця многочленів $R[x]$ було дано для довільної області цілісності *R,* для деяких змістових результатів, слід додатково вимагати, щоб в *R* існувала одиниця і щоб кільце *R* було кільцем характеристики нуль. Тепер ми вимагатимемо, щоб область цілісності *R* була полем, тобто, щоб в *R* для довільного елемента $a\neq0$ існував обернений елемент a^{-1} або щоб для будь-яких *a* і *b,* що належать *R,* $a\neq0$, *випливає, що існує* $c \in R: c=a^{-1}b=b/a.$

Отже, в подальшому викладі розглядатимемо *многочлени над полем P.* Оскільки будь-яке поле є областю цілісності з одиницею, то все, розглянуте у темі шість, залишається істинним для цих многочленів. Зокрема, *сукупність усіх многочленів над полем P є область цілісності з одиницею* $P[x]$ *відносно додавання і множення многочленів.*

Особливо важливу роль в шкільному курсі алгебри, в аналізі та теорії функцій, а також у практичних застосуваннях математики відіграють многочлени над числовими полями, тобто многочлени над полем комплексних чисел або його підполями (*R*, *Q* та ін.). Як зазначалося у попередній темі, оскільки числові поля мають характеристику нуль, то *для многочленів над числовими полями алгебраїчне означення многочленів рівносильне функціональному.* Це полегшує вивчення їх і дає змогу встановити низку важливих спеціальних властивостей.

Було б помилкою думати, що у випадку, коли кільце, над яким розглядаються многочлени, є полем *P*, то й кільце многочленів $P[x]$ виявиться полем. Більше того: *для жодного многочлена ненульового степеня з* $P[x]$ *не існує оберненого елемента.* Справді, для довільного $f(x) \in P[x]$ такого, що $deg\ f \geq 1$, рівність $f(x)g(x)=1$ неможлива ні при якому $g(x) \in P[x]$, адже $g(x)$ не може бути нуль-многочленом і тому $deg\ (f\cdot g) = deg\ f + deg\ g \geq 1$, звідки $f(x)g(x)\neq1$.

Що ж до многочленів нульового степеня, які є елементами поля P, то для кожного з них обернений елемент в $P[x]$ існує і є також многочленом нульового степеня. Іншими словами, *дільниками одиниці в області цілісності* $P[x]$ *є многочлени нульового степеня* (відмінні від нуля константи) *і тільки вони.*

Як бачимо, не тільки все кільце $P[x]$ не є полем, а й будь-яке підкільце, яке містить хоч один многочлен ненульового степеня, не є полем.

Із сказаного зрозуміло, що два різні многочлени з $P[x]$, як правило, не діляться один на одного. Все ж для $P[x]$ може бути побудована теорія подільності, цілком аналогічна теорії подільності цілих чисел, якщо операцію ділення многочленів (обернену до операції множення з $P[x]$) замінити більш загальною операцією *ділення з остачею.*

Кільце многочленів як евклідове кільце

Щоб довести, що кільце $P[x]$ многочленів над полем P є евклідовим, потрібно, згідно з означенням евклідового кільця, показати, що

1. $P[x]$ *є область цілісності*;
2. *існує відображення*:

$\varphi: P[x]\setminus\{0\}\to N^0=NU\{0\}$

таке, *що має місце ділення з остачею, тобто для* $f(x)$, $g(x) \in P[x]$, *існують* $s(x)$, $r(x) \in P[x]$, *такі, що* $f(x)=g(x)s(x)+ + r(x)$, $g(x)\neq 0$, $r(x)=0$ або $\varphi(r(x))< \varphi(g(x))$.

Відображення $\varphi: P[x]\setminus\{0\}\to N^0$ побудуємо в такий спосіб. Кожному многочлену $f(x) \in P[x]$ відмінному від нуля, поставимо у відповідність його степінь, тобто $\varphi(f(x))=deg\ f \in N^0$.

Необхідно показати, що *для довільних многочленів* $f(x)$ *і* $g(x)$ *з кільця* $P[x]$ *існують многочлени* $s(x)$ *і* $r(x)$ *такі, що* $f(x)$ *можна подати у вигляді*

$$f(x) = g(x)s(x)+r(x) \qquad (7.1)$$

де $r(x)=0$ або $deg\ r<deg\ g$.

Під час ділення з остачею многочленів вживають ту саму термінологію, що й для цілих чисел: $f(x)$ – *ділене,* $g(x)$ – *дільник,* $s(x)$ – *частка,* $r(x)$ – *остача.* Умова для чисел, щоб остача була менша за модуль дільника, у випадку

многочленів замінюється умовою, щоб степінь остачі був менший від степеня дільника.

***Теорема**. Довільний многочлен $f(x)$ з кільця $P[x]$ ділиться з остачею на будь-який многочлен $g(x)$ з цього кільця, відмінний від нуль-многочлена; при цьому частка й остача також належать до $P[x]$ і визначаються однозначно.*

***Теорема**. Кільце $P[x]$ многочленів над полем P є евклідове кільце.*

Зауважимо, що у кільці $R[x]$, де R – область цілісності, але не поле, ділення з остачею, взагалі кажучи, нездійсненне. Так, у кільці $Z[x]$ для многочленів $f(x) = x^2+1$, $g(x) = 3x-1$ не можна знайти многочленів $s(x)$ і r ($deg\ r<1$) таких, щоб

$$x^2+1=(3x-1)s(x)+r.$$

Техніка ділення з остачею. Схема Горнера

Ділення з остачею для двох заданих многочленів (тобто знаходження частки та остачі) виконується наступним чином. Спочатку від діленого $f(x)$ віднімають $\frac{a_n}{b_m}x^{n-m}g(x)$, де $g(x)$ – дільник, a_n і b_m – старші коефіцієнти $f(x)$ і $g(x)$ відповідно. З многочленом-різницею діють так само, як з $f(x)$, а саме: якщо старший член цього многочлена $c_l x^l$, $l \geq m$, то від нього віднімають $\frac{c_l}{b_m}x^{l-m}g(x)$ і т. д. Цей процес продовжують доти, поки не отримують многочлен, степінь якого менший від m. Такий момент обов'язково настане, бо степінь діленого щоразу зменшується щонайменше на одиницю. Знайдений таким способом многочлен і буде $m(x)$, а $s(x)$ буде сумою множників $\frac{a_n}{b_m}x^{n-m}$, $\frac{c_l}{b_m}x^{l-m}$ при $g(x)$, які будувалися в процесі цього віднімання.

Наприклад. Нехай $f(x)=x^4 - 2x^3+x - 1$, а $g(x) = x^2 - 2$. Знайдемо $g_1(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$

У цьому разі

$$g_1(x)=(x^4 - 2x^3+x - 1) - x^2(x^2 - 2)= -2x^3+2x^2+x - 1.$$

Далі, з $g_1(x)$ діємо так само, як і з $f(x)$:

$$g_2(x)=(-2x^3+2x^2+x-1)-(-2x)(x^2-2)=2x^2-3x-1.$$

Аналогічно

$$g_3(x)=2x^2-3x-1-2(x^2-2)=-3x+3.$$

Як бачимо, степінь $g_3(x)$ вже менший від степеня $g(x)$. Отже, $r(x)=g_3(x)=-3x+3$, $s(x)=x^2-2x+2$,

$$x^4-2x^3+x-1=(x^4-2)(x^2-2x+2)+(-3x+3).$$

Це саме ділення з остачею можна подати у звичайній формі:

$$\begin{array}{l} x^4-2x^3+x-1 \,|\, \underline{x^2-2} \\ -(\underline{x^4\quad -2x^2}) \quad |\, x^2-2x+2 \\ \quad -2x^3+2x^2+x-1 \\ \quad -(\underline{-2x^3\quad +4x}) \\ \quad\quad 2x^2-3x-1 \\ \quad\quad -(\underline{-2x^2\quad -4}) \\ \quad\quad\quad\quad -3x+3 \end{array}$$

Оскільки за теоремою частка $s(x)$ і остача $r(x)$ визначаються однозначно, для знаходження їх можна користуватися і методом невизначених коефіцієнтів.

Пояснимо цей метод на тому самому прикладі. Нам відомо, що існують такі многочлени $s(x)$ і $r(x)$, для яких справджується рівність $x^4-2x^3+x-1=(x^2-2)s(x)+r(x)$, причому степінь $s(x)$ не може перевищувати $n-m$, тобто в цьому разі двох, а степінь $r(x)$ менший від m, тобто в цьому разі не перевищує одиницю. Це означає, що $s(x)$ і $r(x)$ можна подати в канонічній формі так:

$$s(x)=A_2x^2+A_1x+A_0,\ r(x)=B_1x+B_0,$$

де A_0, A_1, A_2, B_0, B_1 – поки що невідомі коефіцієнти. Підставляючи ці вирази у останню рівність, маємо

$$x^4-2x^3+x-1=(x^2-2)(A_2x^2+A_1x+A_0)+(B_1x+B_0).$$
$$x^4-2x^3+x-1=x^4A_2+x^3A_1+x^2(A_0-2A_2)+x(-2A_1+B_1)+$$
$$+(-2A_0+B_0).$$

За означенням рівності многочленів коефіцієнти при однакових степенях x рівні між собою. Звідси маємо систему рівнянь:

$$A_2=1, A_1= -2,\ A_0 - 2A_2=0, -2A_1+B_1=1, -2A_0+B_0= -1.$$

Розв'язавши цю систему, матимемо

$$A_0 = 2, A_1= -2, A_2=1, B_0=3, B_1=-3.$$

Тобто

$$s(x)= x^2-2x+2, r(x)=-3x+3.$$

У загальному випадку $s(x)$ шукають у вигляді многочлена з невизначеними коефіцієнтами степеня $n - m$, а $r(x)$ – степеня $m - 1$.

Застосуємо такий перехід до окремого, але важливого для дальшого викладу випадку, коли $g(x)=x- \alpha$, тобто коли многочлен-дільник є лінійний двочлен. Використовуючи метод невизначених коефіцієнтів, одержимо

$$a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0=(x- \alpha)(A_{n-1}x^{n-1}+ +A_{n-2}x^{n-2}+...+A_1x+A_0)+r. \qquad (7.2)$$

Звернемо увагу на те, що остача в цьому разі є многочлен, не вище нульового степеня, тобто константа (елемент поля P). Прирівнюючи коефіцієнти у рівності (7.2), отримуємо:

$$a_n=A_{n-1},\ a_{n-1}=A_{n-2}-\alpha A_{n-1},\ ...,\ a_1=A_0-\alpha A_1,\ a_0=r\ -\ \alpha A_0.$$

Звідси:

$$A_{n-1}=a_n,\ A_{n-2}= a_{n-1} + \alpha A_{n-1},\ ...,$$
$$A_0=a_1+ \alpha A_1,\ r= a_0+ \alpha A_0 \qquad (7.3)$$

Формули (7.3) показують, що поділити многочлен *на* $(x-\alpha)$ можна за такою схемою, яка називається *схемою Горнера*

	a_n	a_{n-1}	a_{n-2}	...	a_1	a_0
α	$a_n=A_{n-1}$	$\alpha A_{n-1}+a_{n-1}= =A_{n-2}$	$\alpha A_{n-2}+a_{n-2}= =A_{n-3}$	...	$\alpha A_1+a_1=A_0$	$\alpha A_0 + a_0 = =r$

Виконуючи ділення за цією схемою, кожний наступний коефіцієнт A_{k-1} частки й остачу r дістають множенням

щойно обчисленого коефіцієнта A_k на α і додаванням до знайденого добутку відповідного коефіцієнта a_k даного многочлена.

Зауважимо, що ділення з остачею многочлена $f(x)$ на лінійний двочлен виду $x-\alpha$ здійснене і в кільці многочленів над будь-якою областю цілісності R (що не є полем), хоч, як було зазначено в попередньому пункті, для довільних многочленів $f(x) \in R[x]$, $g(x) \in R[x]$, частка $s(x)$ і остача $r(x)$ можуть в $R[x]$ не існувати. У випадку ж $g(x)=x-\alpha$ коефіцієнти частки й остача, як показують формули (7.3), належать області цілісності R.

Схему Горнера особливо доцільно використовувати тоді, коли знайдену частку треба знову ділити на який-небудь лінійний множник. Під час застосування схеми Горнера для послідовного ділення не потрібно щоразу наново виписувати коефіцієнти часток: закінчення одного з процесів ділення є в той же час початком наступного.

Остача при діленні $f(x)$ на $x-\alpha$ дорівнює значенню многочлена при $x=\alpha$, тобто $f(\alpha)$.

***Теорема* (*Безу*).** *Для будь-якого елемента α з поля P остача при діленні многочлена $f(x) \in P[x]$ на $x-\alpha$ дорівнює $f(\alpha)$.*

Як було зазначено, за схемою Горнера зручно багаторазово ділити многочлен на лінійний двочлен. За допомогою такого ділення легко отримати розклад довільного многочлена $f(x)$ за степенями $(x-\alpha)$, який широко використовується в алгебрі та аналізі.

Приклад. Знайдемо розклад многочлена

$$f(x)=x^5-3x^3+x^2-2x+1$$

за степенями двочлена $x-1$. Складемо таку таблицю:

	1	0	-3	1	-2	1
1	1	1	-2	-1	-3	-2
1	1	2	0	-1	-4	
1	1	3	3	2		
1	1	4	7			
1	1	5				
1	1					

У першому рядку цієї таблиці стоять коефіцієнти даного многочлена $f(x)$; у другому рядку, починаючи з другого стовпчика, стоять коефіцієнти частки $f_1(x)$ і остача $r_0 = -2$; у третьому рядку, починаючи з другого стовпчика, маємо вже результат ділення $f_1(x)$ на x-1 і остачу $r_1 = -4$, що утворилась при цьому діленні, і т. д.

Отже, останні у кожному рядку таблиці числа є шукані коефіцієнти $r_5=1$, $r_4 = 5$, $r_3= 7$, $r_2 = 2$, $r_1 = -4$, $r_0 =- 2$, а розклад многочлена $f(x)$ за степенями x-1 матиме вигляд**:**

$$f(x)=(x-1)^5+5(x-1)^4+7(x-1)^3+2(x-1)^2-4(x-1)-2.$$

Подільність многочленів. Ідеали кільця $P[x]$

Ми пересвідчились у тому, що будь-який многочлен $f(x) \in P[x]$ ділиться на довільний ненульовий многочлен $g(x) \in P[x]$ з остачею. Проте нас особливо цікавитиме той окремий випадок, коли це ділення відбувається «без остачі», або, як кажуть, «націло». У цьому випадку говорять, що $f(x)$ *ділиться* на $g(x)$.

Вважатимемо, що многочлен $f(x) \in P[x]$ ділиться на многочлен $g(x) \in P[x]$ і записуватимемо $f(x) \vdots g(x)$, якщо остача $r(x)$ при діленні $f(x)$ на $g(x)$ дорівнює нулю, тобто якщо існує многочлен $s(x) \in P[x]$ такий, що

$$f(x)=g(x)s(x). \qquad (7.4)$$

Якщо $f(x)$ ділиться на $g(x)$, то кажуть також, що $g(x)$ *ділить* $f(x)$ або є *дільником* $f(x)$, і записують $g(x)/f(x)$.

Частка $s(x)$ визначається однозначно.

Зауважимо, що нуль-многочлен ділиться на довільний многочлен, відмінний від нуля; при цьому частка також є нуль-многочлен. Це дає змогу далі в цьому пункті вважати всі розглядувані многочлени відмінними від нуля.

Оскільки $P[x]$ не є поле, то многочлени з $P[x]$, взагалі кажучи, не діляться один на одного. Але це не виключає того, що в окремих випадках таке ділення «націло» можливе (як і в кільці цілих чисел).

Властивості подільності многочленів у кільці $P[x]$ одержимо безпосередньо з властивостей подільності в довільній області цілісності. При цьому слід урахувати, що

дільниками одиниці в кільці $P[x]$ є всі відмінні від нуля константи і тільки вони.

Властивості: для будь-яких $f(x)$, $g(x)$, $h(x)$ з $P[x]$, $c \in P$, $c \neq 0$.

1. $f(x) \vdots g(x) \wedge g(x) \vdots h(x) \rightarrow f(x) \vdots h(x)$.
2. $f(x) \vdots h(x) \wedge g(x) \vdots h(x) \rightarrow (f(x) + g(x)) \vdots h(x) \wedge (f(x) - g(x)) \vdots h(x)$.
3. $f(x) \vdots h(x) \rightarrow f(x)g(x) \vdots h(x)$.
4. $f_1(x) \vdots h(x) \wedge f_2(x) \vdots h(x) \wedge \ldots \wedge f_m(x) \vdots h(x) \rightarrow (f_1(x)g_1(x) + \cdots + f_m(x)g_m(x)) \vdots h(x)$.
5. $f(x) \vdots c$.
6. $f(x) \vdots g(x) \rightarrow f(x) \vdots cg(x)$.

Як відомо, два елементи області цілісності з одиницею називаються *асоційованими*, якщо вони діляться один на одного, або, що те саме, відрізняються лише множником, що є дільником одиниці. Зокрема, у кільці $P[x]$ многочлени $f(x)$, $g(x)$ *асоційовані*, якщо вони відрізняються лише множником, який є відмінною від нуля константою c:

$$f(x)=cg(x) \text{ або } g(x)=f(x)/c=c' f(x).$$

Відношення між многочленами *«бути асоційованими»* рефлексивне, симетричне і транзитивне, тобто є відношенням *еквівалентності.*

Якщо не вважати різними асоційовані многочлени (тобто розглядати класи асоційованих многочленів), то відношення подільності $f(x) \vdots g(x)$ можна тлумачити як відношення порядку (нестрогого), адже це відношення рефлексивне ($f(x) \vdots c\, f(x)$), транзитивне (властивість 1), антисиметричне.

Тобто *якщо $f(x)$ і $g(x)$ або асоційовані з ними многочлени взаємно діляться один на одного, то $f(x)$ і $g(x)$ збігаються з точністю до асоційованості.*

Розглянемо тепер питання про будову ідеалів кільця $P[x]$.

Згідно з загальним означенням ідеалу комутативного кільця, непорожня сукупність многочленів $f(x) \in P[x]$ є ідеалом кільця $P[x]$, якщо вона є групою відносно додавання і якщо добуток многочленів $f(x) \in I$, $g(x) \in P[x]$ належить I.

Серед ідеалів кільця особливу роль відіграють *головні ідеали*, кожний з яких породжений деяким елементом кільця. У кільці з одиницею головний ідеал, породжений елементом f, складається з усіх елементів кільця, кратних f, і позначається (f). Якщо в області цілісності з одиницею усі ідеали – головні, то її називають *кільцем головних ідеалів*. Такі кільця мають ряд спільних властивостей, на які спирається теорія подільності.

Теорема. *Кільце $P[x]$ многочленів над довільним полем P є кільце головних ідеалів.*

Найбільший спільний дільник. Алгоритм Евкліда

Означення. *Якщо многочлен $d(x)$ є дільником многочлена $f(x)$ і многочлена $g(x)$, то він називається спільним дільником многочленів $f(x)$ і $g(x)$.*

Означення*. Спільний дільник многочленів $f(x)$ і $g(x)$, який ділиться на кожний інший спільний дільник цих многочленів, називається найбільшим спільним дільником многочленів $f(x)$ і $g(x)$ і позначається через (f, g)*, або НСД (f, g).

Ці означення природно узагальнюються на випадок m ($m>2$) многочленів.

Звичайно, будь-які два многочлени мають тривіальні спільні дільники, а саме – дільники одиниці кільця $P[x]$; такими дільниками є усі відмінні від нуля константи (елементи поля P) (див. властивість 5 подільності). Очевидно також, що НСД двох многочленів не визначається цілком однозначно. Якщо $d(x)$ – найбільший спільний дільник, то й кожний многочлен $cd(x)$, де c – елемент поля P, відмінний від нуля, також є НСД цих многочленів. Проте з *точністю до сталого множника найбільший спільний дільник визначається однозначно.* Справді, якщо $d(x)$ і $d_1(x)$ – найбільші спільні дільники даних двох многочленів, то $d(x)$ повинен ділитися на $d_1(x)$ (бо $d(x)$ – найбільший спільний дільник), а $d_1(x)$ повинен ділитися на $d(x)$ (бо $d_1(x)$ – найбільший спільний дільник). Тоді $d(x)$ і $d_1(x)$ асоційовані, тобто $d_1(x)=cd(x)$, де c – константа, відмінна від нуля. Розглядаючи спільні дільники двох многочленів, ми не братимемо до уваги тривіальні дільники і вважатимемо,

що многочлени взаємно прості, якщо в них немає спільних дільників, відмінних від многочленів нульового степеня.

***Означення**. Многочлени $f(x)$ і $g(x) \in P[x]$ називаються взаємно простими, якщо кожний їхній спільний дільник є многочленом нульового степеня* (відмінною від нуля константою).

Зрозуміло, що многочлени $f(x)$, $g(x)$ взаємно прості тоді і тільки тоді, коли НСД $(f, g) = 1$ (адже ця умова рівнозначна тому, що кожний спільний дільник многочленів є дільником одиниці).

Основне твердження відносно НСД многочленів, яким ми постійно користуватимемось, можна сформулювати так:

***Теорема.** Для будь-яких двох многочленів $f(x)$, $g(x) \in P[x]$ існує найбільший спільний дільник $d(x)$, причому $d(x)$ можна подати у вигляді $d(x)=f(x)u(x)+g(x)v(x)$, де $u(x)$, $v(x)$ – деякі многочлени* з $P[x]$.

Наслідок. *Многочлени $f(x)$, $g(x) \in P[x]$ взаємно прості тоді і тільки тоді, коли існують многочлени $u(x)$, $v(x) \in P[x]$ такі, що $f(x)u(x)+g(x)v(x)=1$.*

З цього наслідку випливає ряд простих, але важливих властивостей взаємно простих многочленів. Сформулюємо деякі з них: для будь-яких $f(x)$, $g(x)$, $h(x)$ з $P[x]$:

1. $(f, g) = 1 \wedge (f, h) = 1 \rightarrow (f, gh) = 1$.
2. $f(x)g(x) \vdots h(x) \wedge (f, h) = 1 \rightarrow g(x) \vdots h(x)$.
3. $f(x) \vdots g(x) \wedge f(x) \vdots h(x) \wedge (g, h) = 1 \rightarrow f(x) \vdots g(x)\,h(x)$.

Маємо *спосіб знаходження* найбільшого дільника двох многочленів. $P[x]$ є евклідове кільце, у ньому застосовна процедура знаходження НСД за допомогою послідовного ділення з остачею або Евкліда. Цей алгоритм у загальному вигляді було описано в третій темі. Тут ми розглянемо алгоритм Евкліда стосовно НСД двох многочленів.

Нехай дано два многочлени $f(x)$ і $g(x)$, причому степінь $f(x)$ не менший від степеня $g(x)$. Виконаємо послідовне ділення з остачею, яке можна записати за допомогою такої системи рівностей:

$$
\begin{aligned}
&f(x)= g(x)\, s_1(x)+ r_1(x),\\
&g(x)= r_1\,(x)\, s_2\,(x)+ r_2(x),\\
&r_1\,(x)= r_2\,(x)\, s_3(x)+ r_3(x),\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&r_{n-2}\,(x)= r_{n-1}\,(x)\, s_n(x)+ r_n(x),\\
&r_{n-1}\,(x)= r_n\,(x)\, s_{n+1}\,(x).
\end{aligned}
\qquad (7.4)
$$

Ми тут виходимо з того, що після скінченної кількості ділень остача $r_{n+1}(x)$ дорівнюватиме 0. Справді, з самого означення остачі зрозуміло, що степінь многочлена $r_1\,(x)$ менший від степеня $g\,(x)$; степінь $g_2\,(x)$ менший від степеня $g_1\,(x)$ і взагалі степінь $r_k\,(x)$ менший від степеня $r_{k-1}\,(x)$. Але це означає, що або якась з остач $r_k(x)$ дорівнюватиме нулю, або степінь остачі, зменшуючись при кожному діленні принаймні на одиницю, дорівнюватиме нулю. Якщо $deg\ r_n=0$, то $r_{n+1}=0$, бо будь-який многочлен ділиться на многочлен нульового степеня. Алгоритм Евкліда для многочленів зводиться до скінченної кількості ділень з остачею. Оскільки степінь $r_1(x)$ не більший за m-1, де m – степінь $g(x)$, то кількість кроків у попередній схемі не може перевищувати m.

Наприклад. Нехай $f(x) = x^3 - 3x^2 +3x - 1$, $g(x)= x^3 - 1$. Знайти НСД.

Застосовуючи алгоритм Евкліда до цих многочленів, отримуємо такі рівності:

$x^3-3x^2+3x-1=(x^3-1)\cdot 1+(-3x^2+3x)$	$s_1(x)=1,$ $r_1(x)= -3x^2+3x$
$x^3-1=(-3x^2+3x)(-1/3\ x-1/3)+(x-1)$	$s_2(x)= -1/3\ x-1/3$ $r_2(x)= x-1$
$-3x^2+3x=(x-1)(-3x)$	$s_3(x)= x-1$ $r_3(x)=0$

Відповідно до загальної теорії остання відмінна від нуля остача $r_n(x)$ у системі рівностей (7.4) і є НСД многочленів $f(x)$ і $g(x)$. Тобто, НСД$(f, g)= r_2(x) = x-1$.

Наприклад. Знайдемо найбільший спільний дільник многочленів:

$$f(x)= x^4+ x^3 + x^2 + 1,\ g(x) = 4x^3 + 3x^2 + 2x + 1.$$

Ділимо $x^4+ x^3 + x^2 + 1$ на $4x^3 + 3x^2 + 2x + 1$.

При цьому, щоб уникнути дробових коефіцієнтів, перший з цих многочленів домножимо на 4. Зрозуміло, що при цьому частка й остача також помножаться на 4, що не має істотного значення, бо всі многочлени ми визначаємо з точністю до сталого множника.

Маємо:

$$x^4 + x^3 + x^2 + x + 1 \,|\, \underline{4x^3 + 3x^2 + 2x + 1}$$
(помножимо на 4) $\quad | \, x$
$$4x^4 + 4x^3 + 4x^2 + 4x + 4$$
$$\underline{4x^4 + 3x^3 + 2x^2 + x}$$
$$x^3 + 2x^2 + 3x + 4$$

Перш ніж ділити далі, помножимо знайдену різницю знову на 4. При цьому частку отримуємо неправильну, бо її перший коефіцієнт у 4 рази, а другий – у 16 раз більший за той, який повинен бути. Що ж до остачі, то вона збільшиться в 16 раз. Оскільки нас цікавить не частка, а остача і оскільки цю остачу можна визначити з точністю до сталого множника, то такий процес «порушеного ділення» веде нас до мети.

Помножимо на 4, маємо далі:

$$x^4 + x^3 + x^2 + x + 1 \,|\, \underline{4x^3 + 3x^2 + 2x + 1}$$
(домножимо на 4) $\quad | \, x+1$
$$4x^4 + 4x^3 + 4x^2 + 4x + 4$$
$$-(\underline{4x^4 + 3x^3 + 2x^2 + x\ )}$$
$$x^3 + 2x^2 + 3x + 4 \qquad \text{домножимо на 4}$$
$$4x^3 + 8x^2 + 12x + 16$$
$$-(\ \underline{4x^3 + 3x^2 + 2x + 1})$$
$$5x^2 + 10x + 15 \ \text{поділимо на 5}$$
$$x^2 + 2x + 3 \ \ r_1(x)$$

Таким чином, $r_1(x) = x^2 + 2x + 3$. Ділимо далі:

$$4x^3 + 3x^2 + 2x + 1 \,|\, \underline{x^2 + 2x + 3}$$
$$-\ (\underline{4x^3 + 8x^2 + 12x}) \ | \ 4x\text{-}5$$
$$-5x^2 - 10x + 1$$
$$-\ (\underline{-5x^2 - 10x - 15})$$
$$16 \quad \text{ділимо на 16}$$
$$1 \quad r_2(x)$$

Отже, $r_2(x)= 1$. Далі ділити не потрібно, бо видно, що $r_3(x) = 0$ і тому НСД $(f, g) = r_2 (x) = 1$. Найбільший спільний дільник дорівнює 1, тобто многочлени $f(x) = x^4+ x^3 + x^2+1$, $g(x) = 4x^3 + 3x^2 + 2x + 1$ взаємно прості.

Іноді доводиться шукати НСД не двох, а більшої кількості многочленів, скажімо, $f_1(x)$, …, $f_n(x)$. У цьому випадку спочатку знаходимо $d_1(x)$=НСД($f_1(x)$, $f_2(x)$); потім шукаємо $d_2(x)$=НСД($d_1(x)$, $f_3(x)$); $d_3(x)$=НСД($d_2(x)$,$f_4(x)$); …; $d_k(x)$=НСД($d_{k-1}(x)$, $f_{k+1}(x)$);…; $d_{n-1}(x)$=НСД($d_{n-2}(x)$, $f_n(x)$). $d_{n-1}(x)$ і буде НСД усіх многочленів.

Справді, $f_k (x)$ ділиться на $d_{k-1} (x)$; $d_{k-1}(x)$ ділиться на $d_k (x)$; і т. д., нарешті, $d_{n-2} (x)$ ділиться на $d_{n-1}(x)$. Якщо тепер $d(x)$ – будь-який спільний дільник для $f_1 (x)$, $f_2(x)$, ..., $f_n (x)$, то він є також дільником для $d_1(x)$, $d_2(x)$, ..., $d_{n-1}(x)$, як це випливає з означень цих многочленів. Отже, $d_{n-1}(x)$ – найбільший спільний дільник многочленів $f_1(x)$, …, $f_n(x)$.

Зрозуміло, що коли які-небудь два з многочленів $f_1(x)$, $f_2(x)$, ... , $f_n(x)$ взаємно прості, то НСД усіх многочленів дорівнює одиниці. За допомогою алгоритму Евкліда можна також знайти для заданих многочленів $f(x)$, $g(x) \in P[x]$ многочлени $u (x)$ і $v (x)$ з $P[x]$ такі, що істинною є рівність $d(x)=f(x)u(x)+g(x)v(x)$.

Оскільки $d(x)=r(x)$, то з рівностей (7.4) отримуємо (для спрощення записів позначатимемо многочлени скорочено, опускаючи букву x):

$$d=r_{n-2} - r_{n-1} s_n.$$

У свою чергу,

$r_{n-1}= r_{n-3} - r_{n-2} s_{n-1}$,

$r_{n-2}= r_{n-4} - r_{n-3} s_{n-2}$ і т. д.

У загальному випадку:

$$r_{n-k}= r_{n-k-2} - r_{n-k-1} s_{n-k},$$

де k=1, 2, ..., n-1, причому під r_1 слід розуміти многочлен f, а під r_0 – многочлен g.

Підставимо тепер у $d=r_{n-2} - r_{n-1} s_n$ вираз для r_{n-1}. Отримуємо:

$$d=r_{n-2} – [r_{n-3} - r_{n-2} s_{n-1}] s_n= - r_{n-3} s_n+ r_{n-2} (1+ s_n s_{n-1}).$$

Отже,

$$d= - r_{n-3} s_n + r_{n-2} (1+ s_n s_{n-1}).$$

З цього виразу можна аналогічно виключити r_{n-2} , підставивши замість нього відповідний вираз. Виключаючи далі r_{n-3}, r_{n-4}, ..., ми щоразу діставатимемо вираз d через r_{k-1} і r_k, в якому множники при них утворені з часток s_i за допомогою додавання і множення. Процес поступового виключення r_k припиниться тоді, коли в правій частині рівності з'являться $r_1=f$ і $r_0=g$.

Отже, ми отримуємо, що $d=fu+gv$, де u і v – деякі многочлени, утворені з часток s_n, s_{n-1} .... s_1. З самого способу побудови $u(x)$ і $v(x)$ бачимо, що ці многочлени належать до того самого кільця $P[x]$, що й $f(x)$, $g(x)$.

У кільці $P[x]$ многочленів над полем P можна означити і *найменше спільне кратне* елементів.

***Означення**. Спільним кратним многочленів $f(x)$, $g(x) \in P[x]$ називається будь-який многочлен $s(x) \in P[x]$ такий, що $s(x) \vdots f(x)$ і $s(x) \vdots g(x)$. Найменшим спільним кратним* (НСК) *многочленів $f(x)$, $g(x)$ називається спільне кратне $f(x)$, $g(x)$, яке ділить будь-яке інше спільне кратне цих многочленів;* НСК *многочленів $f(x)$, $g(x)$ позначають* НСК $[f, g]$ або $[f, g]$.

***Теорема**. Для будь-яких відмінних від нуля многочленів $f(x)$, $g(x)$ найменше спільне кратне існує і визначається однозначно з точністю до сталого множника.*

Можна, аналогічно до НСД, розглядати НСК довільної кількості многочленів.

Незвідні многочлени

Розглянемо тепер, які з елементів області цілісності $P[x]$ є *нерозкладними або простими*. Згідно з загальним означенням, елемент області цілісності нерозкладний або простий, якщо він *не є дільником одиниці і не має нетривіальних дільників.* Переформулюємо це означення стосовно кільця многочленів над полем P, увівши для простого многочлена спеціальний термін – *незвідний.*

***Означення**. Многочлен $f(x) \in P[x]$ називається незвідним у полі P, якщо він не є константа і не має дільників, відмінних від константи і від многочленів виду $cf(x)$, де c – константа.*

Іншими словами, $f(x)$ є $P[x]$ – незвідний у полі P, якщо $deg\ f \geq 1$ і якщо з рівності $f(x)=g(x)s(x)$, $g(x)$, $s(x) \in P[x]$ випливає $deg\ g=0$ і $deg\ s=0$.

Складені елементи області цілісності $P[x]$ називатимемо *звідними многочленами у полі.*

***Означення**. Многочлен $f(x) \in P[x]$ називається звідним у полі P, коли $deg\ f \geq 1$ і коли існують такі многочлени $g(x)$, $s(x) \in P[x]$, що $f(x)=g(x)s(x)$, причому $0 \leq deg\ g < deg\ f$ і $0 \leq deg\ s < deg\ f$, $deg\ f = deg\ g + deg\ s$.*

Отже, будь-який многочлен, вищий від нульового степеня, є або звідним, або незвідним у даному полі.

Підкреслимо, що звідність чи незвідність многочлена є поняття *відносне* і залежить від поля P, над яким многочлен розглядається. Як відомо, будь-який многочлен $f(x) \in P[x]$ можна вважати також многочленом над полем Δ – довільне розширення поля P.

Якщо $f(x)$ звідний у полі P, то він звідний і в будь-якому розширенні цього поля. Але цілком можливо, що многочлен $f(x)$, незвідний у полі P, виявиться звідним у деякому розширенні Δ поля P.

Наприклад. Многочлен x^2+1 незвідний у полі раціональних чисел і в полі дійсних чисел. Цей многочлен звідний у полі комплексних чисел. Для доведення незвідності у полі дійсних чисел припустимо супротивне, тобто що $x^2+1=(ax+b)(cx+d)$, *де a, b, c, d – дійсні числа* $a \neq 0$, $c \neq 0$. Нехай $x = -\frac{b}{a}$; тоді $\left(-\frac{b}{a}\right)^2 + 1 = 0$, тобто $a^2+b^2=0$, що неможливо, бо $a \neq 0$.

До многочленів нульового степеня поняття звідності і незвідності не застосовується. Що ж до многочленів першого степеня, то має місце така теорема.

***Теорема**. Многочлен першого степеня над довільним полем P незвідний у цьому полі.*

Це твердження очевидне, коли врахувати, що степінь добутку многочленів дорівнює сумі степенів співмножників.

Зауважимо, що кожний многочлен $f(x)$ першого степеня з раціональними коефіцієнтами незвідний у будь-якому числовому полі P, бо це поле можна розглядати як розширення поля раціональних чисел, і тому $f(x) \in P[x]$.

Сформулюємо деякі властивості незвідних многочленів, які є конкретизацією для випадку кільця $P[x]$ загальних властивостей простих елементів у будь-якій області цілісності з одиницею.

1. *Якщо* $p(x)$ *– многочлен, незвідний у даному полі, то і многочлен* $cp(x)$*, де* c *– довільна відмінна від нуля константа, незвідний у цьому полі.*
2. *Якщо* $p(x)$ *– незвідний у даному полі многочлен, а* $f(x)$ *– довільний многочлен над цим полем, то або* $f(x)$ *ділиться на* $p(x)$*, або ці многочлени взаємно прості.*
3. *Якщо незвідний у даному полі многочлен* $p(x)$ *ділиться на інший незвідний у цьому полі многочлен* $q(x)$*, то ці многочлени збігаються з точністю до сталого множника.*

Ми бачили, що звідність чи незвідність многочлена істотно залежить від того, над яким полем цей многочлен розглядається. На відміну від цього, *взаємна простота* двох многочленів і, більше того, їх НСД повністю визначається даними многочленами *незалежно* від того, до якого кільця ми їх відносимо. Це пояснюється тим, що найбільший спільний дільник визначається за допомогою раціональних дій над даними многочленами і, отже, його коефіцієнти залежать тільки від коефіцієнтів даних многочленів і належать до того самого поля. З цих самих міркувань зрозуміло, що подільність чи неподільність многочлена $f(x)$ на многочлен $g(x)$ також не залежить від того, над яким полем вони розглядаються.

Канонічний розклад многочлена

Фундаментальну роль у теорії подільності цілих чисел відіграє теорема про можливість і єдиність розкладу довільного цілого числа (відмінного від 0, 1 і мінус 1) у добуток простих множників. Це твердження називають *основною теоремою арифметики.* Виявляється, що для многочленів істинне цілком аналогічне твердження про можливість і однозначність розкладу довільного многочлена над полем P у добуток незвідних у цьому полі многочленів.

Теорема*. Кожний многочлен* $f(x)$ *ненульового степеня над полем P можна подати у вигляді*

$$F(x)=p_1(x)p_2(x)\ldots p_l(x), \qquad (7.5)$$

де всі $p_k(x)$ *є незвідними многочленами у полі P. Зображення* (7.5) *єдине з точністю до сталих множників і до порядку нумерації многочленів* $p_k(x)$.

Зображення (7.5) називають *розкладом многочлена* $f(x)$ *на незвідні множники* (або у добуток незвідних множників) *у полі P.*

Наслідок. *Довільний многочлен ненульового степеня над полем P можна подати и вигляді*

$$f(x) = [p_1(x)]^{k_1}[p_2(x)]^{k_2}\ldots[p_m(x)]^{k_m}, \qquad (7.6)$$

де $p_1(x)$, $p_2(x)$, ..., $p_m(x)$ – *попарно різні* (неасоційовані) *многочлени, незвідні у полі P. Це зображення єдине з точністю до сталих множників* (і нумерації співмножників).

Зображення (7.6) називатимемо *канонічним розкладом многочлена* $f(x)$ *у полі P.*

Розклад (7.6) відразу випливає з зображення (7.5), коли врахувати те, що деякі з незвідних множників $p_1(x)$, $p_2(x)$, ..., $p_m(x)$ у формулі (7.5) можуть бути однакові.

Означення. *Якщо многочлен* $p_j(x)$ *входить у канонічний розклад* (7.6) *у степені з показником* k_j, *кажуть, що* $p_j(x)$ *є множником кратності* k_j *многочлена* $f(x)$. *Множники, кратність яких більша за одиницю, називаються кратними множниками многочлена.*

Іншими словами, *незвідний многочлен* $p_j(x)$ *є множником* k_j*-ї кратності многочлена* $f(x)$, *якщо* $f(x)$ *ділиться на* $[p_i(x)]^{k_j}$, *але не ділиться на* $[p_i(x)]^{k_j+1}$.

Покажемо тепер, що до многочленів можна застосувати метод знаходження НСД, подібний до методу розкладання на прості множники в арифметиці.

При цьому будемо користуватись тим очевидним фактом, що *кожний спільний дільник двох многочленів* $f(x)$ *і* $g(x)$ *над полем P може мати тільки такі незвідні множники в цьому полі, які є незвідними множниками як многочлена* $f(x)$, *так і многочлена* $g(x)$.

Теорема. *Якщо многочлени* $f(x)$ *і* $g(x)$ *розкладені на незвідні множники, то* НСД (f, g) *дорівнює добутку всіх незвідних множників, які входять у розклад як* $f(x)$, *так і*

$g(x)$. *Якщо таких спільних незвідних множників немає, то* НСД (f, g) = 1.

Звичайно, теорему легко поширити на випадок більшої кількості заданих многочленів.

Приклад. Нехай $f(x)=x^3+x^2-5x+3$, $g(x)=x^3-3x^2+3x-1$. Розкладемо ці многочлени на незвідні множники у полі Q.

Легко перевірити, що $x=1$ є коренем многочлена $f(x)$: $f(1)=(1)^3+1^2-5+3=0$. Поділемо за схемою Горнера.

	1	1	-5	3
1	1	2	-3	0

$$f(x)=(x-1)(x^2+2x-3)=(x-1)^2(x+3),$$
$$g(x)=x^3-3x^2+3x-1=(x-1)^3.$$

Відповідно до теореми, НСД (f, g)=$(x-1)^2$, тобто НСД (f, g) = $x^2 - 2x + 1$.

Приклади розв'язування типових завдань

№1. *Виконати ділення з остачею многочлена*

$f(x) = 4x^5 - 3x^3 + 2x - 6$ на $g(x) = x^3 - 2x^2 + 1$.

Розв'язання.

1-ий спосіб (ділення стовпцем)

$$\begin{array}{l|l} 4x^5 - 3x^3 + 2x - 6 & x^3 - 2x^2 + 1 \\ \underline{-\,4x^5 - 8x^4 + 4x^2} & 4x^2+8x+13 \quad (\textit{частка } s(x)) \\ 8x^4 - 3x^3 - 4x^2 + 2x - 6 & \\ \underline{-\,8x^4 - 16x^3 + 8x} & \\ 13x^3 - 4x^2 - 6x - 6 & \\ \underline{-\,13x^3 - 26x^2 + 13} & \\ 22x^2 - 6x - 19 \quad (\textit{остача } r(x)) & \end{array}$$

***2-ий спосіб* (*метод невизначених коефіцієнтів*)**

$$f(x) = g(x) \cdot s(x) + r(x), \text{ де}$$
$$\text{частка } s(x) = Ax^2 + Bx + C;$$
$$\text{остача } r(x) == Mx^2 + Nx + P.$$
$$4x^5 - 3x^3 + 2x - 6 = (x^3 - 2x^2 + 1) \cdot$$
$$(Ax^2 + +Bx + C) + Mx^2 + Nx + P;$$
$$4x^5 - 3x^3 + 2x - 6 =$$
$$= Ax^5 + Bx^4 + Cx^3 - 2Ax^4 - 2Bx^3 - 2Cx^2 +$$
$$+Ax^2 + Bx + C + Mx^2 + Nx + P;$$

$$4x^5 - 3x^3 + 2x - 6=$$
$$= x^5 \cdot \text{A} + x^4 \cdot (\text{B} - 2\text{A}) + x^3(C - 2B) +$$
$$+x^2 \cdot (-2C + A + M) + x \cdot (B + N) + (C + P).$$

Прирівняємо коефіцієнти в лівій і правій частинах останнього рівняння. Складемо систему рівнянь та розв'яжемо її. Отримаємо:

$$\begin{cases} A = 4; \\ B - 2A = 0; \\ C - 2B = -3; \\ -2C + A + M = 0; \\ B + N = 2; \\ C + P = 6. \end{cases} \text{ звідси } \begin{array}{c} A = 4; \\ B = 8; \\ C = 13; \\ M = 22; \\ N = -6; \\ P = -19. \end{array}$$

Отже, $s(x) = 4x^2 + 8x + 13;$ $r(x) = 22x^2 - -6x - 19.$

***3-ій спосіб* (*застосування формул схеми Горнера*)**

$$g_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$
$$g_1(x) = 4x^5 - 3x^3 + 2x - 6 - 4x^{\mathbf{2}}(x^3 - 2x^2 + 1) =$$
$$= 4x^5 - 3x^3 + 2x - 6 - 4x^5 + 8x^4 - 4x^2 =$$
$$= 8x^4 - 3x^3 - 4x^2 + 2x + 6.$$
$$g_2(x) = g_1(x) - \frac{a_{n_1}}{b_m} x^{n_1-m} g(x)$$
$$g_2(x) = 8x^4 - 3x^3 - 4x^2 + 2x + 6 - \mathbf{8}\boldsymbol{x}(x^3 - 2x^2 + 1) =$$
$$= 8x^4 - 3x^3 - 4x^2 + 2x - 6 - 8x^4 +$$
$$+16x^3 - 8x = 13x^3 - 4x^2 - 6x - 6.$$
$$g_3(x) = g_2(x) - \frac{a_{n_2}}{b_m} x^{n_2-m} g(x)$$
$$g_3(x) = 13x^3 - 4x^2 - 6x - 6 - \mathbf{13}(x^3 - 2x^2 + 1) =$$
$$= 13x^3 - 4x^2 - 6x - 6 - 13x^3 + 26x^2 - 13 =$$
$$= 22x^2 - 6x - 19.$$

Частка $s(x) = \frac{a_n}{b_m} x^{n-m} + \frac{a_{n_1}}{b_m} x^{n_1-m} + \frac{a_{n_2}}{b_m} x^{n_2-m},$

тобто $s(x) = 4x^2 + 8x + 13.$

Остача $r(x) = 22x^2 - 6x - 19.$

Відповідь: $s(x) = 4x^2 + 8x + 13;$
$r(x) = 22x^2 - 6x - 19.$

№2. *Розкласти многочлен* $f(x) = 2x^5 - 3x^3 + 4x^2 - 7x + 5$ *із кільця* $\mathbb{Z}[x]$ *за степенями двочлена* $x - 1$.

Розв'язання. Застосуємо схему Горнера для знаходження коефіцієнтів шуканого розкладу.

В першому рядку таблиці виписуємо коефіцієнти многочлена $f(x)$. В другому рядку отримуємо коефіцієнти неповної частки $s_1 = 2x^4 + +2x^3 - x^2 + 3x - 4$ і остачу r_0=1. Саме числа цього рядка використовуються далі для відшукання коефіцієнтів неповної частки s_2 і остачі r_1 в 3-му рядку і т. д. Для зручності, в кожному рядку таблиці остачі обводимо.

	2	0	-3	4	-7	5
1	2	2	-1	3	-4	$\boxed{1} = r_0$
1	2	4	3	6	$\boxed{2} = r_1$	
1	2	6	9	$\boxed{15} = r_2$		
1	2	8	$\boxed{17} = r_3$			
1	2	$\boxed{10} = r_4$				
1	$\boxed{2} = r_5$					

Шуканий розклад многочлена f за степенями $x - 1$ має вигляд:

$$f(x) = 2(x-1)^5 + 10(x-1)^4 + 17(x-1)^3 + \\ +15(x-1)^2 + 2(x-1) + 1.$$

№3. *Розкласти многочлен* $f = \bar{3}x^6 + \bar{2}x^4 - \bar{3}x^3 + x - \overline{-1}$ *із кільця* $Z_5[x]$ *за степенями двочлена* $x - 2$.

Розв'язання. Застосуємо схему Горнера. Маємо: $a_6 = \bar{3}$, $a_5 = \bar{0}, a_4 = \bar{2}, a_3 = -\bar{3}, a_2 = \bar{0}, a_1 = \bar{1}, a_0 == -\bar{1}, c = \bar{2}$.

	$\bar{3}$	$\bar{0}$	$\bar{2}$	$-\bar{3}$	$\bar{0}$	$\bar{1}$	$-\bar{1}$
$\bar{2}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{1} = r_0$
$\bar{2}$	$\bar{3}$	$\bar{2}$	$\bar{3}$	$\bar{1}$	$\bar{2}$	$\bar{0} = r_1$	
$\bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{4}$	$\bar{0} = r_2$		
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{2}$	$\bar{3} = r_3$			
$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{2} = r_4$				
$\bar{2}$	$\bar{3}$	$\bar{1} = t_5$					
$\bar{2}$	$\bar{3} = r_6$						

Отже,

$$f(x) = \bar{3}(x-\bar{2})^6 + (x-\bar{2})^5 + \bar{2}(x-\bar{2})^4 + \bar{3}(x-\bar{2})^3 + \bar{1}.$$

Наведемо для прикладу таблиці додавання і множення класів за модулем 5:

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

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

№4. *Знайти значення многочлена* $f(x) = 31x^5 - 423x^4 + 2185x^3 - 5439x^2 + 6670x - 3293$ для *x*=2,1.

Розв'язання. Розкладемо многочлен $f(x)$ за степенями $x-2$.

	31	-423	2185	-5439	6670	-3293
2	31	-361	1463	-2513	1644	-5
2	31	-299	865	-783	78	
2	31	-237	391	-1		
2	31	-175	41			
2	31	-113				
2	31					

Таким чином,

$$f(x) = 31(x-2)^5 - 113(x-2)^4 + 41(x-2)^3 - -(x-2)^2 + 78(x-2) - 5,$$

$$f(2{,}1) = 31 \cdot (0{,}1)^5 - 113 \cdot (0{,}1)^4 + 41 \cdot (0{,}1)^3 - -(0{,}1)^2 + 78 \cdot (0{,}1) - 5 = \ 0{,}00031 - 0{,}0113 + +0{,}041 - 0{,}01 + 7{,}8 - 5 = 2{,}82001.$$

№5. *Знайти НСД та НСК многочленів:* $f(x) = x^4 + x^3 + 2x^2 + x + 1$, $g(x) = x^3 - 2x^2 + x - 2$.

Розв'язання. Для знаходження найбільшого спільного дільника (НСД) многочленів $f(x)$ і $g(x)$ скористаємось алгоритмом Евкліда:

$$\begin{array}{r|l} x^4 + x^3 + 2x^2 + x + 1 & x^3 - 2x^2 + x - 2 \\ \underline{-\,x^4 - 2x^3 + x^2 - 2x} & \hline x + 3 \\ 3x^3 + x^2 + 3x + 1 & \\ \underline{-\,3x^3 - 6x^2 + 3x - 6} & \\ 7x^2 + 7 & \end{array}$$

$$\begin{array}{r|l} x^3 - 2x^2 + x - 2 & 7x^2 + 7 \\ \underline{-\,x^3 + x} & \hline \frac{1}{7}x - \frac{2}{7} \\ -2x^2 - 2 & \\ \underline{-\,2x^2 - 2} & \\ 0 & \end{array}$$

Остання відмінна від нуля остача дорівнює $7x^2 + 7$, отже НСД $(f(x), g(x)) = 7x^2 + 7$.

НСК многочленів знайдемо за формулою:

$$\text{НСК}\,(f(x), g(x)) = \frac{f(x)\cdot g(x)}{\text{НСД}\,(f(x), g(x))}.$$

$$\text{НСК}\,(f(x), g(x)) = \frac{(x^4+x^3+2x^2+x+1)\cdot(x^3-2x^2+x-2)}{7x^2+7} =$$

$$= \frac{x^7 - x^6 + x^5 - 4x^4 - x^3 - 5x^2 - x - 2}{7x^2 + 7} =$$

$$= \frac{1}{7}x^5 - \frac{1}{7}x^4 - \frac{3}{7}x^2 - \frac{1}{7}x - \frac{2}{7}.$$

Відповідь: НСД $(f(x), g(x)) = 7x^2 + 7$;

$$\text{НСК}\,[f(x), g(x)] = \frac{1}{7}x^5 - \frac{1}{7}x^4 - \frac{3}{7}x^2 - \frac{1}{7}x - \frac{2}{7}.$$

№6. *Чи є звідним у полі Q многочлен* $f(x)=x^4+2x^3-3x^2 - 5x+2$?

Розв'язання. Припустимо, що многочлен є звідним у полі Q, тобто його можна розкласти в добуток не менше як двох многочленів ненульового степеня з кільця $Q[x]$. Використаємо метод невизначених коефіцієнтів. Можливі два випадки: 1) обидва множники мають степінь 2; 2) один

множник має степінь 1, а другий – 3.

Нехай $f(x)=(Ax^2+Bx+C)(Dx^2+Mx+N)$.

$$x^4+2x^3-3x^2-5x+2=ADx^4+(AM+BD)x^3+(AN+BM+CD)x^2+$$
$$+(BN+CM)x+CN.$$

Маємо:

$$\begin{cases} AD=1 \\ AM+BD=2 \\ AN+BM+CD=-3 \\ BN+CM=-5 \\ CN=2 \end{cases}$$

Розв'яжемо цю систему у цілих числах. З першого рівняння маємо: $A=D=1$ або $A=D=-1$. З останнього: $C=1$, $N=2$; $C=2$, $N=1$; $C=-1$, $N=-2$; $C=-2$, $N=$ $=-1$. Розглянемо кожен з восьми можливих варіантів.

Перший варіант.

$$\begin{cases} A=D=1 \\ M+B=2 \\ BM=-6 \\ 2B+M=-5 \\ C=1 \\ N=2 \end{cases}; \quad \begin{cases} A=D=1 \\ M=2-B \\ 2B-B^2+6=0 \\ 2B+2-B=-5 \\ C=1 \\ N=2 \end{cases}; \quad \begin{cases} A=D=1 \\ M=9 \\ -57\neq 0 \\ B=-7 \\ C=1 \\ N=2 \end{cases}$$ – несумісна.

Аналогічно переконуємося, що всі отримані системи є несумісними.

Це означає, що складена нами система рівнянь є несумісною, а отже, многочлен не розкладається в добуток двох многочленів другого степеня з цілими коефіцієнтами. Припустимо, що розклад виконується при дробових числах. Зведемо до найменшого спільного знаменника коефіцієнти многочленів $g_1(x)=Ax^2+Bx+C$, $g_2(x)=Dx^2+Mx+N$ та винесемо за дужки ці знаменники і найбільші спільні дільники чисельників обох многочленів. Маємо розклад:

$$f(x)=\frac{r}{s}(A_1x^2+B_1x+C_1)(D_1x^2+M_1x+N_1).$$

$$\text{НСД}\ (r, s)=\text{НСД}\ (A_1, B_1, C_1)=\text{НСД}\ (D_1, M_1, N_1)=1.$$

Оскільки коефіцієнти многочлена є цілими числами, то всі коефіцієнти многочлена

$$g(x)=(A_1x^2+B_1x+C_1)(D_1x^2+M_1x+N_1)$$

мають ділитися на число s, а тому й на кожен його простий дільник p. Разом з тим, серед кожної трійки чисел A_1, B_1, C_1 та D_1, M_1, N_1 знайдуться числа, які не діляться на p. Тому серед коефіцієнтів A_1D_1, $A_1M_1+B_1D_1$, $A_1N_1+B_1M_1+C_1D_1$, $B_1N_1+C_1M_1$, C_1N_1 многочлена $g(x)$ знайдеться такий, що не ділиться на p. Тому $s=1$ і ми отримуємо розклад з цілими коефіцієнтами, що, як доведено вище, неможливо.

Нехай $f(x)=(Ax+B)(Cx^3+Dx^2+Mx+N)$.

$$x^4+2x^3-3x^2-5x+2=Acx^4+(AD+BC)x^3+(AM+BD)x^2+$$
$$+(AN+BM)x+BN.$$

Маємо:

$$\begin{cases} AC=1 \\ AD+BC=2 \\ AM+BD=-3. \\ AN+BM=-5 \\ BN=2 \end{cases}$$

Одним із розв'язків системи є $A=C=N=1$, $B=2$, $D=0$, $M=-3$. Отже, $x^4+2x^3-3x^2-5x+2=(x+2)(x^3-3x+1)$. Тобто многочлен $f(x)$ є звідним у полі Q.

№7. *Довести, що многочлен* $f(x)=\overline{2}x^2+x+\overline{1}$ *незвідний у полі* Z_3.

Розв'язання. Якщо многочлен $f(x)$ є звідним у полі Z_3, то його можна подати у вигляді

$$f(x)=\left(\overline{A}x+\overline{B}\right)\left(\overline{C}x+\overline{D}\right), \text{ де } \overline{AC}\neq 0.$$

Звідси $f(x)=\overline{A}\left(x+\frac{\overline{B}}{\overline{A}}\right)\left(\overline{C}x+\overline{D}\right)$

і відповідно до теореми Безу многочлен $f(x)$ має коренем $x=-\frac{\overline{B}}{\overline{A}}$. Проте

$$f\left(\overline{0}\right)=\overline{1}, f\left(\overline{1}\right)=\overline{1}, f\left(\overline{2}\right)=\overline{2}.$$

Тобто многочлен $f(x)$ не має коренів в Z_3. Отже, многочлен $f(x)$ незвідний у полі Z_3.

Завдання для аудиторного заняття

№1. Виконати ділення з остачею многочлена $f(x)$ на $g(x)$ трьома різними способами:

а) $f(x) = x^4 - 3x^3 - 10x^2 + 2x + 5$,
$g(x) = x + 2$;

б) $f(x) = x^5 + 4x^4 - 2x^3 - 7x^2 + 3x + 5$,
$g(x) = x^3 - 2x$;

в) $f(x) = 4x^5 + 10x^4 + 8x^3 + 5x^2 + 2x + 3$,
$g(x) = 2x^3 + 3x^2 - x$;

г) $f(x) = \bar{4}x^6 + \bar{3}x^5 - x^4 - \bar{2}x^3 - \bar{2}x^2 + x - \overline{1}$,
$g(x) = x^2 + \overline{1}$ в кільці $Z_5[x]$.

№2. Користуючись схемою Горнера розкласти за степенями x_0:

а) $f(x)=x^4 - 8x^3+24x^2 - 50x+90$, $x_0 = 2$;

б) $f(x)=x^4+2ix^3-(1+i)x^2-3x+7+i$, $x_0 = -i$.

№3. Записати у вигляді лінійної комбінації
$f(x)u(x) + g(x)v(x) = d(x)$, де $d(x)$ – НСД $f(x)$ і $g(x)$:

а) $f(x) = x^4 + 2x^3 - x^2 - 6x - 4$, $g(x) = x^3 - 2x - 1$;

б) $f(x) = x^5 + x^4 - 6x^3 + 2x^2 + 7x + 3$,
$g(x) = x^4 - 7x^2 + 7x + 3$;

в) $f(x) = x^5 - 2x^4 + 4x^3 - 4x^2 + 2x - 1$,
$g(x) = x^4 - x^3 + 2x^2 - x - 1$;

г) $f(x) = x^3 - 4x^2 - 4x - 5$, $g(x) = x^3 - 6x^2 - 6x - 1$;

д) $f(x) = 3x^5 - 2x^4 - 2x^3 + 4x^2 - x - 2$,
$g(x) = x^4 - x^3 + x - 12$;

е) $f(x) = x^5 - \bar{2}x^3 + \bar{2}x^2 - \bar{2}x + \bar{2}$, $g(x) = x^3 - \bar{3}x + \bar{2}$
в кільці $Z_7[x]$;

є) $(x) = x^6 - x^5 - 10x^2 + 9x - 3$,
$h(x) = x^4 + x^3 + +2x^2 + 3x - 3$;

к) $f(x) = 3x^6 - 8x^5 + 5x^4 - 11x^3 - 10x^2 - 21x + 31$,
$h(x) = x^5 - 2x^4 - -4x^2 - 7x - 13$;

л) $f(x) = x^5 - 2x^4 - 3x^3 + 5x^2 - 4x - 2$,
$h(x) = x^4 - x^3 - 4x^2 - 3$.

№4. Знайти НСД та НСК многочленів:

а) $f(x) = x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$,
$g(x) = x^5 + x^2 - x + 1$ в кільці $Q[x]$;

б) $f(x) = x^5 + 3x^4 - 12x^3 - 52x^2 - 52x - 12$,
$g(x) = x^4 + 3x^3 - 6x^2 - 22x - 12$ в кільці $Q[x]$;

в) $f(x) = x^5 + x^4 + 3x^3 + 4x^2 + 4x + 2$,

$g(x) = x^5 + 2x^4 + 3x^3 + 6x^2 + 6x + 2$ в кільці $Q[x]$;

г) $f(x) = x^4 - 9x^3 + 25x^2 - 24x + 16$,
$g(x) = 2x^3 - x^2 + x + 1$ в кільці $\mathbb{Q}[x]$;

д) $f(x) = x^4 - 4x^3 + 4x^2 - 5x - 2$,
$g(x) = x^2 - x + 2$ в кільці $\mathbb{Q}[x]$;

е) $f(x) = \bar{2}x^4 + x^3 + x^2 + x - \bar{1}$,
$g(x) = \bar{2}x^4 + x^3 - x^2 - \bar{1}$ в кільці $\mathbb{Z}_5[x]$;

є) $f(x) = (x-1)^5(x^2+1)^2(x^4+x^2+1)^3$,
$h(x) = (x^2-1)^2(x^2+2x++1)(x^4-1)$;

ж) $f(x) = \left(x - \sqrt{3}\right)^2\left(3x + \sqrt{2}\right)^3$,
$h(x) = (2x+1)^2(x^2+1)(x^2-3)$;

з) $f(x) = (2x^2 - 3x + 9)(x-3)^3$,
$h(x) = (3x-4)^2(2x-1)$;

к) $f(x) = (x-3)^3(x-1+i)^3$,
$h(x) = \left(x - 1 - i\sqrt{2}\right)^2 x(x-1+i)^2$.

№5. Використовуючи схему Горнера, обчислити $f(a)$ і розкласти многочлен $f(a)$ за степенями $x - a$:

а) $f(x) = x^5 - 4x^4 + 7x^3 - 8x^2 + 12x - 1$, $a = 1$ в $Q[x]$;

б) $f(x) = 2x^4 + 8ix^3 - 14x^2 - 12ix + 4 + i$, $a = -i$ в $C[x]$;

в) $f(x) = \bar{4}x^4 - x^3 + \bar{3}x^2 - \bar{1}$, $a = \bar{4}$ в $Z_7[x]$;

г) $f(x) = x^5 + x - 5$, $a = -1$ в $Q[x]$;

д) $f(x) = x^4 + 8x^3 + 24x^2 + 29x + 12$, $a = -2$ в $Q[x]$;

е) $f(x) = -2x^5 - 20x^4 - 80x^3 - 16x^2 - 173x - 75$, $a = -2$ в $Q[x]$;

є) $f(x) = x^5 - 5x^4 + 9x^3 - 7x^2 + 4x - 4$, $a = 1$ в $Q[x]$;

ж) $f(x) = x^4 + 8x^2 + 12ix - 1$, $a = -i$ в $C[x]$;

з) $f(x) = x^3 - (1-3i)x^2 - (4+2i)x + 7 - 2i$, $a = 1 - i$ в $C[x]$;

и) $f(x) = x^5 - \bar{4}x^4 + \bar{2}x^3 - x^2 + x - \bar{4}$, $a = \bar{2}$ в $C[x]$;

і) $f(x) = x^4 - 4ix^3 - 7x^2 + 6ix + 2$, $a = i$ в $C[x]$;

й) $f(x) = \bar{2}x^5 - x^4 + x^3 - x^2 + x - \bar{4}$, $a = \bar{4}$ в $Z_5[x]$.

№6. Розкласти на незвідні множники в полі P многочлени:

а) $f(x) = x^4 - 2x^3 - 27x^2 - 44x + 7$ в Q;

б) $f(x) = 4x^4 + 4x^3 + 13x^2 + 6x + 9$ в Q;

в) $f(x) = x^2(x-3)^2 + 4x^2 - 12x + 4$ в R;

г) $f(x) = x^4 - 10x^2 + 169$ в R;

д) $f(x) = x^4 + 1$ в C;

е) $f(x) = x^5 - x$ в Z_5.

№7. Довести незвідність у кільці $Z[x]$*:*

а) $f(x) = x^5 - x^2 + 1$;

б) $f(x) = x^3 - x^2 + x + 1$.

№8. Спростити вираз:

а) $\frac{2x^5+11x^4+5x^3-2x^2-11x-5}{x^3+4x^2+4x+3}$;

б) $\frac{x^5+x^4+10x^2-6x+9}{x^6-x^5+3x^4+3x^3+4x^2+2x+21}$;

в) $\frac{x^5-6x^3+5x^2-9x+9}{2x^6+4x^5-9x^4-6x^3+14x^2+10x-15}$;

г) $\frac{2x^5+x^4-19x^3+29x^2-26x+8}{x^3+x^2-x+2}$.

Відповіді: ***№1.*** а) $x^3 - 5x^2 + 2 + \frac{1}{x+2}$; б) $x^2 + 4x + \frac{x^2+3x+5}{x^3-2x}$; в) $2x^2 + 2x + 2 + \frac{x^2+4x+3}{2x^3+3x^2-x}$; г) $\bar{4}x^4 + \bar{3}x^3 - 5x^2 - \bar{5}x + \bar{3} + \frac{x-\bar{4}}{x^2+\bar{1}}$. ***№2.*** а) $f(x-2)=(x-2)^4-18(x-2)+38$; б) $f(x+i)=(x+i)^4-2i(x+i)^3-(1+i)(x+i)^2--5(x+i)+7+5i$. ***№4.*** а) НСД $(f(x), g(x)) = x^3 - x + 1$; НСК $(f(x), g(x)) = x^8 + 3x^6 - 4x^5 - x^4 + 4x^3 - 6x^2 + 5x - 5$; б) НСД $(f(x), g(x)) = x + 3$; НСК $(f(x), g(x)) = x^8 + 3x^7 - 18x^6 - 74x^5 + 8x^4 + + 348x^3 + 520x^2 + 280x + 48$; д) НСД $(f(x), g(x)) = x^2 - x + 2$; НСК $(f(x), g(x)) = x^4 - 4x^3 + 4x^2 - 5x - 2$; е) НСД $(f(x), g(x)) = = \frac{x}{2} - \bar{1}$; НСК $(f(x), g(x)) = \bar{3}x^7 + \bar{4}x^6 + \bar{4}x^4 - \bar{5}x^3 - x^2 - \bar{2}x - \bar{1}$; ***№6.*** а) $f(x)=(x^2-7x+1)(x^2+5x+7)$; б) $f(x)=(2x^2+x+3)^2$; в) $f(x)=(x-1)^2(x-2)^2$; г) $f(x)=(x^2-18)(x^2+8)$; д) $f(x) = \left(x - \frac{\sqrt{2}-i\sqrt{2}}{2}\right)\left(x - \frac{\sqrt{2}+i\sqrt{2}}{2}\right)\left(x + \frac{\sqrt{2}+i\sqrt{2}}{2}\right)\left(x + \frac{\sqrt{2}-i\sqrt{2}}{2}\right)$; е) $f(x) = x(x-\bar{1})(x-\bar{2})(x-\bar{3})(x-\bar{4})$.

Завдання для самостійного розв'язування

№1. Виконати ділення з остачею многочлена $f(x)$ на $g(x)$ трьома різними способами:

а) $f(x) = x^4 - 2x^3 + 4x^2 - 6x + 8$,
$g(x) = x - 1$;

б) $f(x) = 3x^5 + 4x^4 - 6x^3 - 2x^2 + 4x - 2$,
$g(x) = 3x^3 - 2x^2 - 2x$;

в) $f(x) = 6x^5 + x^4 + 3x^3 + 3x^2 - x + 4$,
$g(x) = 3x^4 - x^3 + 2x^2$;

г) $f(x) = 6x^5 - 4x^4 + 2x^3 - 8x^2 + 6x - 2$,
$g(x) = 3x^3 + x^2 + 2x - 2$.

№2. Користуючись схемою Горнера розкласти за степенями x_0:

а) $f(x)=x^5$, $x_0=1$;

б) $f(x)=x^4+(3-8i)\,x^3-(21+18i)\,x^2-(33-20i)\,x+7+18i$,
$x_0=-1+2i$.

№3. Записати у вигляді лінійної комбінації $f(x)u(x)+g(x)v(x)=d(x)$, де $d(x)$ – НСД $f(x)$ і $g(x)$:

а) $f(x) = x^6 + x^5 - 3x^4 + 2x^3 + 4x - 2$,
$g(x) = x^5 + 3x^4 + x^3 + 6x^2 + 4x + 6$;

б) $f(x) = x^4 + 2x^3 - x^2 - 4x - 2$,
$g(x) = x^4 + x^3 - x^2 - 2x - 2$;

в) $f(x) = x^5 + 3x^4 + x^3 + x^2 + 3x + 1$,
$g(x) = x^4 + 2x^3 + x + 2$;

г) $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$,
$g(x) = x^4 - 3x^3 + 4x^2 - 3x + 3$;

д) $f(x) = 3x^5 - 2x^4 - 13x^3 + 8x^2 + 7x + 1$,
$g(x) = 3x^3 - 2x^2 + 2x + 1$;

е) $f(x) = \bar{2}x^5 - \bar{3}x^2 - \bar{3}x + \bar{2}$,
$g(x) = \bar{2}x^4 + \bar{3}x^3 - \bar{2}x - \bar{1}$ в кільці $Z_5[x]$;

є) $f(x) = \bar{2}x^2 + \bar{3}$,
$g(x) = x^4 + \bar{2}x^3 - \bar{3}x^2 + x + \bar{1}$ в кільці $Z_5[x]$;

ж) $f(x) = \bar{3}x^6 + \bar{3}x^4 - \bar{2}x^3 + \bar{3}x^2 - x + \bar{3}$,
$g(x) = \bar{3}x^5 + \bar{2}x^4 + \bar{3}x - \bar{3}$ в кільці $Z_5[x]$;

з) $f(x) = x^5 + 2x^4 - 8x^3 + x + 2$,
$g(x) = x^4 + 2x^3 - 6x^2 + x + 2$ в кільці $C[x]$.

№4. Знайти НСД та НСК многочленів:

а) $f(x) = x^5 + x^3 + x^2 + x - 1$,
$g(x) = x^4 + x^3 + x^2 + x + 1$ в кільці $Q[x]$;

б) $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$,
$g(x) = x^3 + 3x^2$ в кільці $Q[x]$;
в) $f(x) = x^4 + 5x^3 + 4x^2 + x + 4$,
$g(x) = x^3 + 3x^2 - 3x + 4$ в кільці $Q[x]$;
г) $f(x) = x^5 + 7x^4 + 13x^3 - x^2 - 7x - 13$,
$g(x) = x^4 + 8x^3 + 23x^2 + 34x + 39$ в кільці $Q[x]$;
д) $f(x) = x^5 - \bar{3}x^4 + \bar{2}x^3 + \bar{4}x^2 + x + \bar{2}$,
$g(x) = \bar{2}x^4 + \bar{3}x^3 + \bar{4}x^2 + \bar{4}x + 3$ в кільці $Z_5[x]$;
е) $f(x) = x^5 - \bar{6}x^4 + \bar{2}x^3 + \bar{2}x^2 + x + \bar{2}$,
$g(x) = \bar{3}x^5 + \bar{4}x^4 - \bar{4}x^3 + \bar{2}x^2 + \bar{4}x + \bar{1}$ в кільці $\mathbb{Z}_7[x]$;
є) $f(x) = x^4 - \bar{3}x^3 - x - \bar{4}$,
$g(x) = x^4 + \bar{2}x^3 + \bar{5}x^2 - \bar{5}x - \bar{3}$ в кільці $Z_7[x]$;
ж) $f(x) = x^3 - x^2 + 5x - 5$,
$g(x) = x^4 + 2x^3 + 2x - 1$ в кільці $R[x]$;
з) $f(x) = x^3 + 3x^2 + 4x - 1$,
$g(x) = x^3 + 2x^2 + x + 1$ в кільці $C[x]$;
и) $f(x) = x^6 + 8x^5 + 22x^4 + 43x^3 + 70x^2 + 57x + 39$,
$h(x) = x^4 + 7x^3 + +14x^2 + 21x + 33$;
і) $f(x) = 2x^7 + x^6 - x^5 + 9x^4 - 3x^3 - 8x - 7$,
$h(x) = 2x^6 - x^5 + 11x^3 - -10x^2 + x - 9$;
к) $f(x) = 6x^5 + x^4 + 12x^3 - 42x^2 + 30x + 25$,
$h(x) = 2x^4 - x^3 + 4x^2 - 17x + 20$.

№5. Використовуючи схему Горнера, обчислити $f(a)$ і розкласти многочлен $f(x)$ за степенями $x - a$:
а) $f(x) = 2x^4 - 10x^2 - 12x$, $a = -1$ в $Z[x]$;
б) $f(x) = x^4 - 8ix^3 - 25x^2 + (36i + 1)x + 24 - 2i$,
$a = 2i$ в $C[x]$;
в) $f(x) = \bar{2}x^4 - x^3 + x^2$, $a = \bar{2}$ в $Z_3[x]$;
г) $f(x) = x^5 + 11x^3 + 33x$, $a = i$ в $C[x]$;
д) $f(x) = -x^4 + \bar{3}x^3 - \bar{4}x^2 - x + \bar{6}$, $a = \bar{6}$ в $Z_7[x]$;
е) $f(x) = x^4 + x^3 - 5x^2 - 10x - 7$, $a = -1$ в $Q[x]$;
є) $f(x) = x^5 + 5x^4 + 10x^3 + 9x^2 + 4x - 2$,
$a = 1$ в $Q[x]$;
ж) $f(x) = x^3 + (5 + 3i)x^2 + (10i + 4)x + 7i - 2$,
$a = -1 - i$ в $C[x]$;
з) $f(x) = -x^5 - 5x^4 + 8x^3 + x + 1$, $a = -1$ в $Q[x]$;
и) $f(x) = -x^5 - \bar{3}x^4 - x^3 + \bar{2}x + \bar{4}$, $a = \bar{5}$ в $Z_7[x]$;
і) $f(x) = \bar{2}x^{11} - 3x^3 + \bar{3}x^2 - \bar{3}x + \bar{8}$, $a = \bar{1}$ в $Z_5[x]$;
й) $f(x) = \bar{4}x^4 + \bar{4}x^2 - \bar{3}x + \bar{3}$, $a = \bar{2}$ в $Z_5[x]$.

№6. Знайти за схемою Горнера неповну частку та остачу від ділення многочлена f на g, якщо:

а) $f = x^4 - 3x^3 + 6x^2 - 7,\ g = x + 4$ в $Z[x]$;

б) $f = \bar{2}x^5 - x^4 + \bar{3}x^2 - \bar{3}, g = x - \bar{3}$ в $Z_5[x]$;

в) $f = x^6 + (2 - 2i)x^5 + (1 + i)x^3 - (1 + i)x^2 + 2i$, $g = x + 1 - i$ в $C[x]$.

№7. Знайти лінійне представлення НСД многочленів $f = x^6 + x^5 - 3x^4 + 2x^3 + 4x - 2$; $g = x^5 + 3x^4 + x^3 + 6x^2 + 4x + 6$ із кільця $\mathbb{R}[x]$ за алгоритмом Евкліда.

№8. Для многочленів $f(x) = x^2 + (1 - i)x + +2i, g(x) = = ix^2 + x + 1 - 3i$ знайти їх суму, добуток, квадрати та куби многочленів.

№9. Розкласти на незвідні множники в полі Р многочлени:

а) $f(x) = x^4 - 6x^3 + 11x^2 - 6x + 1$ в R;

б) $f(x) = x^4 + x^2 + \overline{1}$ в Z_3;

в) $f(x) = x^9 - 1$ в Q.

№10. Довести незвідність у кільці $Z[x]$: $f(x) = x^3 - x^2 + + x + 1$.

Відповіді: ***№1.*** а) $x^3 + x^2 + 5x - 1 + \frac{7}{x-1}$; б) $x^2 + 2x + \frac{2x^2+4x-2}{3x^3-2x^2-2x}$; в) $2x + 1 + \frac{x^2-x+4}{3x^4-x^3+2x^2}$; г) $2x^2 - 2x + \frac{2x-2}{3x^3+x^2+2x-2}$. ***№2.*** а) $f(x- 1)= = (x- 1)^5+5(x+1)^4+10(x-1)^3+10(x+1)^2+5(x+1)+1$; б) $f(x+1-2i)=(x+1-2i)^4- - (x+1-2i)^3+2(x+1-2i)+1$. ***№4.*** а) НСД $(f(x), g(x)) = 1$; НСК $(f(x), g(x)) = x^9 + x^8 + 2x^7 + 3x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 1$; в) НСД $(f(x), g(x)) = -x - 4$; НСК $(f(x), g(x)) = -x^6 - 4x^5 - 2x^3 - 7x^2 + +3x - 4$; ***№9.*** а) $f(x) = \left(x - \frac{3-\sqrt{5}}{2}\right)^2 \left(x - \frac{3+\sqrt{5}}{2}\right)^2$; б) $f(x) = = \left(x + \overline{1}\right)^2 \left(x + \overline{2}\right)^2$; в) $f(x)=(x-1)(x^2+x+1)(x^6+x^3+1)$.

Тема восьма
ПОНЯТТЯ КОРЕНЯ МНОГОЧЛЕНА. КРАТНІ КОРЕНІ

Поняття кореня многочлена. Кратні корені

Нехай $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ – многочлен над полем P, а Δ – будь-яке розширення поля P (зокрема, може бути $\Delta = P$). Як відомо з теми шість, для довільного $\alpha \in \Delta$ можна обчислити *значення многочлена* $f(x)$ *при* $x = \alpha$ (або *в точці* α), тобто елемент

$$f(\alpha)=a_n \alpha^n+a_{n-1} \alpha^{n-1}+...+a_1 \alpha +a_0 \in \Delta.$$

Нас особливо цікавитимуть такі елементи $\alpha \in \Delta$, для яких значення $f(\alpha)$ є нулем поля P (або, що те саме, поля Δ).

Означення. *Коренем многочлена* $f(x) \in P[x]$ *називається елемент* α *будь-якого розширення* Δ *поля* P *такий, що* $f(\alpha) = 0$.

Корінь многочлена $f(x)$ називають також *нулем* многочлена.

Користуючись функціональною термінологією, можна сказати, що корені многочлена $f(x)$ – це *прообрази нульового елемента* при відображенні $f: \Delta \to \Delta$.

Поняття кореня многочлена має велике теоретичне і практичне значення. Адже розв'язування алгебраїчних рівнянь вищих степенів, тобто рівнянь виду

$$a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0=0$$

полягає в знаходженні всіх коренів многочлена, який утворює ліву частину рівняння.

Означення. *Елемент* $\alpha \in P$ *називається коренем многочлена* $f(x) \in P[x]$, *якщо* $f(x)$ *ділиться на* $x - \alpha$.

Теорема. *Елемент* $\alpha \in P$ *є коренем многочлена* $f(x) \in P[x]$ *тоді і тільки тоді, коли лінійний двочлен* $x-\alpha$ *є дільником многочлена* $f(x)$.

Теорема дає необхідну і достатню умову того, що $\alpha \in P$ є коренем многочлена $f(x)$.

Означення. *Елемент* $\alpha \in P$ *називається* k *- кратним коренем* (або коренем *k-ї* кратності) *многочлена* $f(x) \in P[x]$,

якщо f(*x*) *ділиться на* (*x*- α)^k*, але не ділиться на* (*x*- α)$^{k+1}$.

Іншими словами, кратність кореня α многочлена *f*(*x*) є найбільше з натуральних чисел *m* таких, що (*x* - α)^m є дільником *f*(α) у кільці *P*[*x*].

Корені кратності 1 називаються *простими*, корені кратності 2 і більше – *кратними*, причому двократні та трикратні корені іноді називають також *подвійними* та *потрійними* відповідно. Елементи поля *P,* які не є коренями *f* (*x*) ∈ *P*[*x*], іноді називають *нуль-кратними коренями f* (*x*).

Якщо *f* (*x*) – нуль-многочлен, то будь-який елемент α ∈ *P є* його коренем, причому кратність цього кореня не можна визначити, бо нуль-многочлен ділиться на (*x* - α)^m при довільному натуральному *m.* Якщо ж *f* (*x*) ≠0, то будь-який корінь α ∈ *P* має певну кратність *k* ≤ *deg f:* адже *f* (*x*) ділиться на *x*-α і не ділиться на (*x* -α)^m при *m* > *deg f.*

Очевидно, що α ∈ *P* є *k*-кратним коренем многочлена *f* (*x*) ∈ *P*[*x*] тоді і тільки тоді, коли

$$f(x)= (x -\alpha)^k g(x), \qquad (8.1)$$

де *g* (*x*) – многочлен над полем *P,* для якого α не є коренем: адже для того, щоб *f* (*x*) ділився на (*x* - α)^k і не ділився на (*x*-α)$^{k+1}$, необхідно і достатньо, щоб *g*(*x*) ∈ *P*[*x*] і не ділився на *x*-α. Зрозуміло, що *deg g=deg f- k* при *k=deg f* многочлен *g*(*x*) є константа.

Кількість коренів многочлена. Інтерполяційний многочлен

Нехай *f* (*x*) – многочлен *n*-го степеня над полем *P,* а Δ – будь-яке розширення поля *P.* Припустимо, що α ∈ Δ є коренем *f* (*x*) кратності k_1, α_2 є Δ – коренем *f* (*x*) кратності k_2, ..., a_m ∈ Δ – коренем *f* (*x*) кратності k_m, причому $\alpha_i \neq \alpha_j$ при *i* ≠ *j*. Тоді, згідно з (8.1), можна записати

$$f(x)= (x - \alpha_1)^{k_1} g_1(x) \qquad (8.2)$$

де $g_1(x)$ не ділиться на *x*-α_1. Оскільки *f* (*x*) має ділитись на $(x - \alpha_2)^{k_2}$ (але не на $(x - \alpha_2)^{k_2+1}$), а $(x - \alpha_2)^{k_1}$ взаємно простий з $(x - \alpha_2)^{k_2}$, то з (8.2), видно, що $g_1(x)$– ділиться на $(x - \alpha_2)^{k_2}$ (але не на $(x - \alpha_2)^{k_2+1}$), тоді згідно з (8.1), можна записати

$$f(x) = (x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} g_2(x),$$

де $g_2(x)$ – многочлен, який не має своїми коренями α_1 та α_2.

Продовжуючи міркувати в такий же спосіб (тобто, по суті, застосовуючи метод математичної індукції), отримуємо

$$f(x) = (x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \dots (x - \alpha_m)^{k_m} g_m(x), \qquad (8.3)$$

де $g_m(x)$ – многочлен, для якого жодний з елементів α_1, α_2, ..., α_m не є коренем. З (8.3) видно, що $\deg f = n = k_1 + k_2 + \dots + k_m + \deg g_m$, тобто $k_1 + \dots + k_m \le n$.

Отже, кількість коренів многочлена $f(x)$ у полі Δ не може перевищувати степеня цього многочлена, коли навіть кожний корінь ураховувати стільки разів, яка його кратність. Оскільки Δ – довільне розширення поля P, а будь-який корінь многочлена $f(x) \in P[x]$ лежить у якомусь розширенні поля P, то ми отримали такий результат.

Теорема. *Кількість усіх можливих коренів многочлена $f(x)$ над полем P не перевищує його степеня.*

Згідно з попереднім викладом, це твердження істинне, якщо під час підрахунку кількості коренів кожний з них рахуємо стільки разів, яка його кратність. Надалі постійно дотримуватимемося цієї домовленості.

Зауважимо, що ця теорема істинна і для многочленів нульового степеня (тобто для відмінних від нуля констант, які не мають жодного кореня). Вона істинна і у випадку, коли P є область цілісності з одиницею. Проте теорема неправильна для многочленів над кільцями, що мають дільники нуля.

Наслідок. *Якщо многочлен $f(x) \in P[x]$, степінь якого не перевищує n, має $n + 1$ різних коренів, то $f(x)$ є нуль-многочлен.*

Можна дати інше формулювання наведеному наслідку: *два многочлени $f(x)$, $g(x) \in P[x]$, степені яких не перевищують n і які приймають однакові значення в $n + 1$ різних точках з P, рівні між собою.*

Це означає, що серед многочленів не вище n-го степеня існує *не більше одного многочлена,* який приймає наперед

задані значення $\beta_j \in P$ в $n + 1$ різних точках $\alpha_1, \alpha_2, ..., \alpha_{n+1}$ поля *P.* Можна показати, що такий многочлен існує та він єдиний.

Теорема*. Існує один і тільки один многочлен $f(x) \in P[x]$ не вище n-го степеня, який приймає в $n + 1$ різних точках $\alpha_j \in P$ задані значення $\beta_j \in P$ ($j = 1, 2, ..., n+1$).*

Розглянемо многочлен

$$f(x) = \frac{(x-\alpha_2)(x-\alpha_3)\dots(x-\alpha_{n+1})}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\dots(\alpha_1-\alpha_{n+1})}\beta_1 +$$

$$+\frac{(x-\alpha_1)(x-\alpha_3)\dots(x-\alpha_{n+1})}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\dots(\alpha_2-\alpha_{n+1})}\beta_2 + \dots +$$

$$+\frac{(x-\alpha_1)\dots(x-\alpha_{j-1})(x-\alpha_{j+1})\dots(x-\alpha_{n+1})}{(\alpha_j-\alpha_1)\dots(\alpha_j-\alpha_{j-1})(\alpha_j-\alpha_{j+1})\dots(\alpha_j-\alpha_{n+1})}\beta_j +$$

$$+\dots+\frac{(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)}{(\alpha_{n+1}-\alpha_1)(\alpha_{n+1}-\alpha_2)\dots(\alpha_{n+1}-\alpha_n)}\beta_{n+1} \qquad (8.4)$$

Усі члени суми (8.4) є многочлени *n*-го степеня. При цьому *j*-й член побудований так, що при $x = \alpha_j$ він перетворюється в β_j, а при $x=\alpha_i$ ($i \neq j$) – перетворюється в 0. Отже, $f(x)$ є многочлен не вище *n-го* степеня і такий, що $f(\alpha_j) = \beta_j$ ($j = 1, 2, ..., n + 1$), тобто – шуканий многочлен. *Теорему доведено*.

Многочлен (8.4) називають *інтерполяційним многочленом Лагранжа*. Він розв'язує задачу *інтерполяції* многочлена, яка полягає в тому, щоб за певними $n+1$ значеннями многочлена не вище *n-го* степеня знайти всі його значення.

Приклад. Побудуємо многочлен не вище третього степеня над полем *Q*, який при $x = -1$, $x=0$, $x=1$, $x=2$ приймає значення 0, 1, 0, -1 відповідно.

За формулою (8.4) маємо:

$$f(x) = \frac{(x-0)(x-1)(x-2)}{(-1-0)(-1-1)(-1-2)}0 +$$

$$+\frac{(x+1)(x-1)(x-2)}{(0+1)(0-1)(0-2)}\cdot 1 +$$

$$+\frac{(x+1)(x-0)(x-2)}{(1+1)(1-0)(1-2)}\cdot 0+$$
$$+\frac{(x+1)(x-0)(x-1)}{(2+1)(2-0)(2-1)}\cdot(-1)=\frac{1}{3}x^3-x^2-\frac{1}{3}x+1.$$

Існування коренів многочлена. Поле розкладу

У попередньому пункті було з'ясовано, що кількість коренів многочлена не перевищує степеня цього многочлена.

***Теорема* (*Кронекера*).** *Якщо $f(x)$ – довільний многочлен над полем P, для якого $\deg f \geq 1$, то існує розширення K поля P, в якому є корінь $f(x)$.*

Одним з важливих наслідків теореми Кронекера є таке твердження:

***Теорема**. Для будь-якого многочлена $f(x) \in P[x]$ степеня $\deg f \geq 1$ існує таке розширення L поля P, в якому $f(x)$ розкладається на лінійні множники.*

Іншими словами, існує розширення L поля P, в якому степінь усіх незвідних множників многочлена $f(x)$ дорівнює 1.

***Означення**. Поле L, в якому многочлен $f(x)$ розкладається на лінійні множники, називають полем розкладу цього многочлена.*

Отже, остання теорема означає, що для будь-якого многочлена $f(x) \in P[x]$ ненульового степеня існує поле розкладу L, яке є розширенням поля P. Звичайно, може бути, що $L = P$.

Приклад. Многочлен $f(x) = x^4-2 \in Q[x]$ не можна розкласти на множники у полі Q раціональних чисел. У кільці многочленів над полем чисел виду $a + b\sqrt{2}$ (a, b раціональні) маємо розклад:

$$x^4-2=(x^2-\sqrt{2})(x^2+\sqrt{2}).$$

Дальше розкладання на множники у цьому кільці неможливе. Але в кільці $R[x]$ многочленів над полем дійсних чисел отримуємо:

$$x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2}).$$

Переходячи до ще більш широкого кільця многочленів $C[x]$, матимемо:

$$x^4 - 2 = \left(x - \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}i\right)\left(x - \sqrt[4]{2}i\right).$$

Оскільки всі множники тепер лінійні, робимо висновок, що C є поле розкладу многочлена $f(x)$.

***Означення**. Поле P називається алгебраїчно замкнутим, якщо воно є полем розкладу для будь-якого многочлена $f(x) \in P[x]$ ненульового степеня.*

Іншими словами, *P є алгебраїчно замкнуте поле, якщо усі корені будь-якого многочлена $f(x) \in P[x]$ належать цьому самому полю.*

Важливим прикладом алгебраїчно замкнутих полів є поле C комплексних чисел. Твердження про алгебраїчну замкнутість цього поля часто називають *основною теоремою теорії многочленів або основною теоремою алгебри*.

***Теорема.** Всякий, відмінний від константи, многочлен з однією змінною над полем комплексних чисел має щонайменше один комплексний корінь.*

***Теорема**. Поле комплексних чисел є алгебраїчно замкненим, тобто є полем розкладу будь-якого многочлена з комплексними коефіцієнтами.*

Розклад многочлена $f(x)$ на лінійні множники дає змогу отримати ряд важливих наслідків.

Наслідок 1. *Многочлен $f(x) \in P[x]$ n-го степеня має у полі розкладу n коренів.*

Оскільки $f(x)$ в жодному розширенні поля P не може мати більше за n коренів, то можна сказати, що *поле розкладу многочлена містить усі його корені.*

Наслідок 2. У *полі розкладу многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ має канонічний розклад виду*

$$f(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \ldots (x - \alpha_m)^{k_m},$$

($k_1+k_2+\ldots+k_m=n$), *де* $\alpha_1, \alpha_2, \ldots, \alpha_m$ *– різні корені многочлена* $f(x)$.

***Теорема (Вієта).** Якщо* $\alpha_1, \alpha_2, \ldots, \alpha_m$ *– корені многочлена*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in P[x], \text{ то}$$

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n},$$

$$\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_1\alpha_n+\alpha_2\alpha_3+\cdots+$$
$$+\alpha_2\alpha_n+\cdots+\alpha_{n-1}\alpha_n=\frac{a_{n-2}}{a_n},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\sum_{c_n^k}\alpha_{j_1}\alpha_{j_2}\ldots\alpha_{j_k}=(-1)^k\frac{a_{n-k}}{a_n},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\alpha_1\alpha_2\ldots\alpha_n=(-1)^n\frac{a_0}{a_n}. \qquad (8.5)$$

Символ $\sum_{C_n^k}$ слід тут розуміти так, що сума береться по всіх C_n^k комбінаціях з n індексів 1, 2, 3, ..., n по k. Співвідношення (8.5) називають *формулами Вієта*.

Похідна від многочлена

З курсу математичного аналізу відомо, що кожний многочлен n-го степеня з дійсними коефіцієнтами $f(x)=a_nx^n + \ldots + a_1x + a_0$, що розглядається як функція на множині всіх дійсних чисел, має в кожній точці x похідну $f'(x)$, яка також є многочленом, але вже $(n - 1)$-го степеня:

$$f'(x) = na_nx^{n-1} + (n-1)\,a_{n-1}x^{n-2} + \ldots + 2a_2x + a_1. \qquad (8.6)$$

У тих випадках, коли $f(x)$ є многочлен над іншим (взагалі кажучи, абстрактним) полем P, його можна розглядати як функцію, задану на деякому розширенні поля P (тема шість). Проте поняття границі, за допомогою якого вводять похідну в аналізі, застосовне не в усякому полі. Тому означимо поняття похідної від многочлена *формально,* домовившись вираз (8.6) завжди називати похідною від многочлена $f(x)=a_nx^n + \ldots + a_1x + a_0$ незалежно від того, до якого поля належать його коефіцієнти, і незалежно від множини його задання.

***Означення**. Похідною від многочлена*

$$f(x)=a_nx^n + \ldots + a_1x + a_0$$

називається многочлен

$$f'(x) = na_nx^{n-1} + (n-1)\,a_{n-1}x^{n-2} + \ldots + 2a_2x + a_1.$$

Похідну від многочлена нульового степеня, а також похідну від нуль-многочлена беруть рівною нулю.

Безпосередньо з означення випливає, що *похідна від многочлена над полем P є знову многочлен над полем P.*

У подальшому викладі завжди вважатимемо, що *P є поле характеристики* 0.

Для многочленів над полем дійсних чисел (як і для всіх диференційовних функцій) істинні такі правила диференціювання:

$[f(x)+g(x)]' = f'(x)+g'(x)$;
$[f(x)g(x)]' = f'(x)g(x)+f(x)g'(x)$;
$[cf(x)]' = cf'(x)$, де c – константа;
$[(f(x))^k]' = k[(f(x))^{k-1}]f'(x)$, k – натуральне число.

Ці рівності залишаються в силі для похідних від многочленів над довільним полем.

В алгебрі розглядають також другу, третю, ..., n- ну похідні від многочлена $f(x)$.

Відокремлення кратних множників

У попередній темі було показано, що всякий многочлен над полем P можна єдиним способом подати у вигляді добутку многочленів нижчих степенів, незвідних у цьому полі:

$$f(x) = [p_1(x)]^{k_1}[p_2(x)]^{k_2} \dots [p_m(x)]^{k_m} \qquad (8.7)$$

Отже, вивчати властивості многочленів і, зокрема, знаходити їх корені було б значно легше, якби для кожного многочлена був відомий канонічний розклад (8.7); але, виявляється, що в загальному випадку ця задача рівнозначна знаходженню коренів многочлена.

Проте ми покажемо, що в деяких випадках можна розробити загальний метод розкладання многочлена на множники, хоч цей розклад не буде таким повним, як зображення (8.7).

Виберемо у розкладі (8.7) ті незвідні множники $p_i(x)$, кратність яких k_i, дорівнює одиниці, і позначимо добуток цих множників через $\varphi_1(x)$:

$$\varphi_1(x) = p_{i_1}(x)p_{i_2}(x) \dots p_{i_s}(x).$$

Тепер утворимо добуток тих множників $p_j(x)$, кратність яких k_j, дорівнює 2, тобто тих, які входять у розклад (8.7) у другому степені:

$$\varphi_2(x) = p_{j_1}(x)p_{j_2}(x) \dots p_{j_r}(x).$$

Зауважимо, що $\varphi_2(x)$означає добуток самих незвідних множників кратності 2, а не їх квадратів, так що в розклад входить $[\varphi_2(x)]^2$. Продовжуючи аналогічно, розклад (8.7) можна записати у такому вигляді:

$$f(x) = \varphi_1(x)[\varphi_2(x)]^2[\varphi_3(x)]^3 \dots [\varphi_m(x)]^m. \qquad (8.8)$$

Якщо множників кратності $k < m$ в розкладі (8.7) немає, природно вважати $\varphi_k=1$.

Ми зараз викладемо загальний метод зображення многочленів у вигляді (8.8). Зрозуміло, що таке розкладання многочлена доцільне лише тоді, коли в зображенні (8.7) справді існують кратні множники. У противному разі $f(x)=\varphi_1(x)$, тобто ніякого розкладу на множники не буде.

Приклад. Нехай розклад многочлена $f(x)$ на незвідні множники в полі дійсних чисел має вигляд:

$$f(x) = x^{13} - 5x^{12} + 6x^{11} + 4x^{10} - 9x^9 + 5x^8 - 6x^7 - \\ -4x^6 + 8x^5 = x^5(x-2)^3(x^2+1)(x+1)^2(x-1).$$

Тут

$$\varphi_1(x) = (x^2+1)(x-1) = x^3 - x^2 + x - 1,$$
$$\varphi_2(x) = x+1,\ \varphi_3(x) = x-2, \varphi_4(x) = 1, \varphi_5(x) = x.$$
$$f(x) = \varphi_1(x)[\varphi_2(x)]^2[\varphi_3(x)]^3[\varphi_4(x)]^4[\varphi_5(x)]^5.$$

Як бачимо, $f(x)$ – многочлен 13-го степеня, а степінь многочленів $\varphi_k(x)$ не перевищує 3. Тому в цьому прикладі розклад многочлена $f(x)$ на множники $\varphi_k(x)$ дає змогу повністю знайти всі його корені, бо ми вміємо розв'язувати рівняння 1-3 степенів.

Задача зображення многочлена у вигляді (8.8) називається *відокремленням кратних множників.* До розгляду цієї задачі ми й переходимо.

Є досить простий спосіб, який дає змогу, користуючись похідною, визначати, чи має многочлен кратні множники.

***Теорема**. Якщо незвідний у даному полі P характеристики* 0 *многочлен $q(x)$ є множником кратності $k \geq 2$ для многочлена $f(x)$, то він є множником кратності k-1 для похідної $f'(x)$. Якщо $q(x)$ є множником першої кратності многочлена $f(x)$, то він не входить у розклад похідної $f'(x)$ на незвідні множники.*

Наслідок. *Для того, щоб многочлен $f(x)$ не мав кратних множників, необхідно і достатньо, щоб $f(x)$ був взаємно простим із своєю похідною.*

Справді, якщо всі незвідні множники многочлена $f(x)$ мають кратність 1, то в розкладі $f'(x)$ на незвідні множники не буде жодного множника, спільного з множниками многочлена $f(x)$. Тому, НСД $(f, f') = 1$. Якщо ж $f(x)$ має хоч один кратний множник $q(x)$, то НСД (f, f') ділиться на $q(x)$ і тому не може бути константою.

З наслідку, зокрема, випливає, що наявність чи відсутність кратних множників у даного многочлена залежить лише від його коефіцієнтів, а не від того поля, над яким його розглядають.

Як ми знаємо, кожний многочлен у даному полі можна подати у вигляді (8.8). Наше завдання полягає в тому, щоб, знаючи лише коефіцієнти многочлена $f(x)$, визначити многочлени $\varphi_1, \varphi_2, \ldots, \varphi_m$.

Оскільки $\varphi_1(x)$ є добутком незвідних множників многочлена $f(x)$, які мають кратність k=1, то в $f'(x)$ жодний з цих множників входити не буде. $\varphi_2(x)$ є добутком незвідних множників $f(x)$ кратності 2. У $f'(x)$ усі ці множники входять з кратністю одиниця, тобто $f'(x)$ має своїм множником добуток $\varphi_2(x)$ усіх цих незвідних множників, але вже у першому степені. Аналогічно, якщо $f(x)$ має множником $[\varphi_2(x)]^k$, то $f'(x)$ матиме множник $[\varphi_2(x)]^{k-1}$.

Таким чином, можемо записати:

$$f'(x) = \varphi_2(x)[\varphi_3(x)]^2 \ldots [\varphi_m(x)]^{m-1}\psi_1,$$

де – ψ_1 не ділиться на $\varphi_1, \ldots, \varphi_m$. Тоді спільний найбільший дільник (f, f') є добутком усіх множників, які входять у розклади як $f(x)$, так і $f'(x)$:

$$d_1 = \varphi_2(x)[\varphi_3(x)]^2 \ldots [\varphi_m(x)]^{m-1}.$$

Знайдемо тепер d_1':

$$d'_1 = \varphi_3(x)[\varphi_4(x)]^2 \dots [\varphi_m(x)]^{m-2}\psi_2,$$

де ψ_2 не ділиться на φ_i ($i = 2, \dots m$). Далі,

$$d_2 = (d_1, d'_1) = \varphi_3(x)[\varphi_4(x)]^2 \dots [\varphi_m(x)]^{m-2}.$$

Аналогічно можна обчислити $d_3, \dots, d_{m-1}=\varphi_m, d_m=1$.

$d_1, d_2, \dots, d_m$ вже не містять непотрібних нам множників ψ_j. Проте наша мета полягає в тому, щоб знайти кожний з множників φ_j окремо. Для цього поділимо f на d_1. Маємо

$$q_1 = \frac{f}{d_1} = \varphi_1\varphi_2 \dots \varphi_m .$$

Аналогічно:

$$q_2 = \frac{d_1}{d_2} = \varphi_2\varphi_3 \dots \varphi_m,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots,$$

$$q_{m-1} = \frac{d_{m-2}}{d_{m-1}} = \varphi_{m-1}\varphi_m,$$

$$q_m = \frac{d_{m-1}}{d_m} = \varphi_m.$$

З формул шукані множники φ_k отримуємо вже безпосередньо:

$$\varphi_1 = \frac{q_1}{q_2},\ \varphi_2 = \frac{q_2}{q_3}, \dots,\ \varphi_m = q_m.$$

Отже, ми приходимо до такого висновку:

У довільного многочлена над полем P можна відокремити кратні множники за допомогою скінченної кількості раціональних дій над деякими многочленами.

Оскільки, як нам відомо, похідні та найбільші спільні дільники не залежать від того, над яким полем розглядаються задані многочлени, то й результати обчислень за останніми формулами не залежать від цього поля, а лише від коефіцієнтів заданого многочлена.

Отже, розклад (8.8) многочлена над даним полем не залежить від того, до якого основного поля P відносимо коефіцієнти цього многочлена.

Наприклад. Відокремити кратні множники многочлена $f(x)= x^6- 6x^4 - 4x^3 + 9x^2 + 12x + 4.$

Знайдемо спочатку многочлени $d_i(x)$.

$d_1(x)$ – це НСД многочленів $f(x)$ і $f'(x)$.

$$f'(x) = 6x^5 - 24x^3 - 12x^2 + 18x + 12.$$

Застосувавши алгоритм Евкліда, маємо:

$$d_1(x) = x^4 + x^3 - 3x^2 - 5x - 2.$$

Далі маємо $d_1'(x) = 4x^3 + 3x^2 - 6x - 5$ і знаходимо $d_2(x)$ = НСД (d_1, d_1'). Одержимо

$$d_2(x) = x^2 + 2x + 1;\ d'_2(x) = 2x + 2.$$

Знаходимо $d_3(x)$ =НСД (d_2, d_2'). Маємо $d_3(x) = x + 1$, $d'_3(x) = 1$, тому й $d_4(x) = 1$.

Обчислимо тепер многочлени $q_j(x)$:

$$q_1(x) = \frac{f(x)}{d_1(x)} = \frac{x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4}{x^4 + x^3 - 3x^2 - 5x - 2} = x^2 - x - 2,$$

$$q_2(x) = \frac{d_1(x)}{d_2(x)} = x^2 - x - 2,$$

$$q_3(x) = \frac{d_2(x)}{d_3(x)} = x + 1,$$

$$q_4(x) = \frac{d_3(x)}{d_4(x)} = x + 1.$$

Тепер уже можна знайти множники $\varphi_1(x)$, $\varphi_2(x)$, $\varphi_3(x)$, $\varphi_4(x)$:

$$\varphi_1(x) = \frac{q_1(x)}{q_2(x)} = 1,\ \varphi_2(x) = \frac{q_2(x)}{q_3(x)} = x - 2,$$

$$\varphi_3(x) = \frac{q_3(x)}{q_4(x)} = 1,\ \varphi_4(x) = q_4(x) = x + 1.$$

Маємо остаточно: $f(x) = \varphi_1(x)\varphi_2^2(x)\varphi_3^3(x)\varphi_4^4(x)$, тобто $f(x) = (x-2)^2(x+1)^4$.

Отже, ми многочлен 6-го степеня звели до досить простої форми.

Відокремлення кратних множників не тільки спрощує дослідження і знаходження коренів многочленів, але й іноді, є передумовою для застосування деяких методів дослідження і розв'язування алгебраїчних рівнянь.

У таких випадках немає потреби знаходити кожний з множників $\varphi_i(x)$. Завдання полягає в тому, щоб позбутись кратних множників, побудувавши за многочленом $f(x)$ такий многочлен $q(x)$, який має всі ті незвідні множники, які має й $f(x)$, але вже першої кратності. Для цього досить поділити $f(x)$ на НСД многочлена $f(x)$ і його похідної $f'(x)$.

Відповідно до означення для визначення кратності кореня α досить послідовним діленням $f(x)$ на $x-\alpha$ знайти

таке k, щоб $f(x)$ ділився на $(x - \alpha)^k$, але не ділився на $(x- \alpha)^{k+1}$. Очевидно, k і буде кратністю кореня α.

Приклад. Многочлен $f(x)=x^6- 6x^4- 4x^3+9x^2+12x+4$ має в полі Q корінь $\alpha = 2$, як це можна встановити безпосередньою перевіркою. Послідовно ділитимемо $f(x)$ на $x - 2$, використовуючи схему Горнера:

	1	0	-6	-4	9	12	4
2	1	2	-2	-8	-7	-2	0
2	1	4	6	4	1	0	
2	1	6	18	40	81		

Многочлен $f(x)$ ділиться на $(x- 2)^2$, але не ділиться (остача рівна 81) на $(x - 2)^3$. Отже, кратність кореня 2 дорівнює двом.

У низці випадків буває зручно користуватись такою *ознакою кратності кореня*.

***Теорема**. Для того, щоб α був коренем кратності k многочлена $f(x)$, необхідно і достатньо, щоб $f(\alpha)= f'(\alpha)=...= = f^{(k-1)}(\alpha)=0, f^{(k)}(\alpha)\neq 0$.*

Приклад. Застосовуємо цю ознаку до многочлена $f(x)=x^6- 6x^4 - 4x^3+9x^2+12x+4$. Маємо

$$f'(x) = 6(x^5 - 4x^3 - 2x^2 + 3x + 2); f'(2) = 0;$$
$$f''(x) = 6(5x^4 -12x^2-4x + 3); f'(2) = 162 \neq 0.$$

Отже, кратність кореня 2 дорівнює двом.

Наведені міркування показують, що, знаючи корінь многочлена, легко визначити його кратність. Тому на практиці дослідження многочленів, які мають кратні корені, у більшості випадків зводять до дослідження многочленів нижчих степенів, що вже не мають кратних коренів. Це завжди можна зробити відокремленням кратних множників методами, описаними вище.

Приклад. Розглянемо знову многочлен

$$f(x)=x^6- 6x^4 - 4x^3+9x^2+12x+4.$$

Як нам вже відомо з прикладу

$$\text{НСД}(f, f') = x^4 +x^3-3x^2-5x-2.$$

Це свідчить про наявність кратних множників. Щоб позбутися їх, поділимо $f(x)$ на НСД(f, f'). Одержимо: $q(x) = x^2 - x - 2$.

Цей многочлен має ті самі незвідні множники, що й $f(x)$, але вже першої кратності. Оскільки $q(x)$ – квадратний тричлен, легко знайти його корені. Маємо $x_1 = 2$, $x_2 = -1$. Тепер можна з'ясувати їх кратність. Вище було показано, що 2 є двократним коренем. Просте врахування степенів показує, що $x + 1$ є чотирикратним множником многочлена $f(x)$, тобто –1 є коренем кратності 4.

Приклади розв'язування типових завдань

№1. *Знайти корені многочлена*

$f(x) = x^3 - 4x^2 + x + 6$.

Розв'язання. Для того, щоб знайти корені многочлена $f(x) = x^3 - 4x^2 + x + 6$ розв'яжемо рівняння $x^3 - 4x^2 + x + 6 = 0$. Безпосередньо підстановкою знаходимо перший корінь $x_1 = -1$:

$$f(-1) = (-1)^3 - 4(-1)^2 + (-1) + 6 = 0.$$

Поділимо $f(x) = x^3 - 4x^2 + x + 6$ на двочлен $x+1$ за схемою Горнера.

	1	-4	1	6
-1	1	-5	6	0

$$f(x) = x^3 - 4x^2 + x + 6 = (x + 1)(x^2 - 5x + 6) = \\ = (x + 1)(x - 2)(x - 3).$$

Отже, коренями многочлена є числа -1; 2; 3.

Відповідь: -1; 2; 3.

№2. *Знайти кратність кореня $x = x_0$ многочлена $f(x)$:*

$f(x) = x^5 - 10x^4 + 34x^3 - 36x^2 - 27x + 54$, $x_0 = 3$.

Розв'язання. 1*-й спосіб.* Послідовно поділимо многочлен $f(x) = x^5 - 10x^4 + 34x^3 - 36x^2 - 27x + 54$ на $x - 3$, отримуємо:

$$\frac{f(x)}{x-3} = g_1(x) = x^4 - 7x^3 + 13x^2 + 3x - 18;$$

$$\frac{g_1(x)}{x-3} = g_2(x) = x^3 - 4x^2 + x + 6;$$

$$\frac{g_2(x)}{x-3} = g_3(x) = x^2 - x - 2;$$

$$\frac{g_3(x)}{x-3} = x + 2 + \frac{4}{x-3},$$

тобто $g_3(x)$ не ділиться націло на $x - 3$.

Отже, $f(x) = (x-3)g_1(x) = (x-3)^2 g_2(x) =$

$= (x-3)^3 g_3(x)$, причому $g_3(3) \neq 0$. Це означає, що корінь $x_0 = 3$ многочлена $f(x)$ має кратність 3.

Ділити многочлен $f(x) = x^5 - 10x^4 + 34x^3 - 36x^2 - 27x + 54$ на $x - 3$ зручно за допомогою схеми Горнера:

	1	-10	34	-36	-27	54
3	1	-7	13	3	-18	0
3	1	-4	1	6	0	
3	1	-1	-2	0		
3	1	2	4			

Отже, многочлен $f(x) = x^5 - 10x^4 + 34x^3 - 36x^2 - 27x + 54$ ділиться націло на $(x-3)^3$, але не ділиться на $(x-3)^4$. Кратність кореня x_0=3 дорівнює 3.

2-*й спосіб.* Скористаємося теоремою про кратність кореня зі сторінки 180.

Знайдемо першу похідну многочлена $f(x)$.

За умовою $f(x) = x^5 - 10x^4 + 34x^3 - 36x^2 - 27x + 54$, тоді

$$f'(x) = 5x^4 - 40x^3 + 102x^2 - 72x - 27.$$

Обчислимо значення многочлена $f(x)$ та першої похідної многочлена $f'(x)$ в точці x_0=3.

$$f(3) = 3^5 - 10 \cdot 3^4 + 34 \cdot 3^3 - 36 \cdot 3^2 - 27 \cdot 3 + 54 =$$
$$= 243 - 810 + 918 - 324 - 81 + 54 = 0;$$
$$f'(3) = 5 \cdot 3^4 - 40 \cdot 3^3 + 102 \cdot 3^2 - 72 \cdot 3 - 27 =$$
$$= 405 - 1080 + 918 - 216 - 27 = 0.$$

Оскільки $f(x_0) = f'(x_0) = 0$, то знайдемо другу похідну многочлена $f(x)$ та її значення в точці x_0=3.

$f''(x) = 20x^3 - 120x^2 + 204x - 72$, тоді

$f''(3) = 20 \cdot 3^3 - 120 \cdot 3^2 + 204 \cdot 3 - 72 = 540 -$
$- 1080 + 612 - 72 = 0.$

Оскільки $f(x_0) = f'(x_0) = f''(x_0) = 0$, то продовжимо цей процес і знайдемо третю похідну многочлена $f(x)$ та її значення в точці x_0=3.

$f'''(x) = 60x^2 - 240x + 204$, тоді $f'''(3) = 60 \cdot 3^2 -$
$- 240 \cdot 3 + 204 = 540 - 720 + 204 = 24 \neq 0.$

Отже, кратність кореня x_0=3 дорівнює трьом.

Відповідь: кратність три.

№3. *Визначити коефіцієнт a так, щоб многочлен* $f(x)=x^5 - ax^2 - ax+1$ *мав коренем число* (-1) *кратності не нижче двох.*

Розв'язання. За умовою число мінус 1 є коренем кратності щонайменше другого порядку, тоді $f(-1)=0$ та $f'(-1)=0$.

$f(x)= x^5 - ax^2 - ax+1, f(-1)= -1 - a+a+1=0,$

$f'(x)= 5x^4 - 2ax - a, f'(-1)= 5+2a - a=0, a=-5,$

$f(x)= x^5+5x^2+5x+1.$

Відповідь: $a = -5$.

№4. *Побудувати многочлен найменшого порядку за даними коренями: подвійний корінь* 1, *прості корені* 2, 3, 1+*i.*

Розв'язання. Відповідно до умови до канонічного розкладу многочлена входять такі вирази: $(x-1)^2$ – двократний корінь, $(x-2)$, $(x-3)$, $(x-1-i)$ – однократні корені. Тому:

$f(x)=(x-1)^2(x-2)(x-3)(x-1-i)=x^5-(8+i)\,x^4+(24+7i)\,x^3-$
$-(34+27i)\,x^2+(23+17i)\,x-(6+6i).$

Завдання для аудиторного заняття

№1. Знайти корені многочлена на множині дійних чисел:

а) $f(x) = x^4 - 3x^3 + 2x^2 + 3x - 6;$

б) $g(x) = x^5 + 6x^3 - 7x^2 + x - 1;$

в) $f(x) = x^4 + 2x^3 - 2x^2 - 6x + 5;$

г) $f(x) = x^4 + x^3 - x^2 - 7x - 6;$

д) $f(x) = x^4 + x^3 - 11x^2 - 5x + 30;$

е) $f(x) = x^4 + 3x^2 + 2;$

є) $f(x) = x^5 + 6x^4 + x^3 + 12x^2 + 40x + 24;$

ж) $f(x) = 3x^4 + \frac{1}{2}x^3 + x^2 - 2x + \frac{1}{2}.$

№2. Знайти кратність кореня $x = x_0$ многочлена $f(x)$*:*

а) $f(x) = x^7 + 11x^6 + 48x^5 + 100x^4 + 80x^3 - 48x^2 - -128x - 64,\ \ x_0 = -2;$

б) $f(x) = 3x^5 + 2x^4 + x^3 - 10x - 8,\quad x_0 = -1;$

в) $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8,\quad x_0 = 2;$

г) $f(x) = x^5 + 8x^4 + 21x^3 + 14x^2 - 20x - 24,$
$x_0 = -2;$

д) $f(x) = 8x^5 + 44x^4 + 18x^3 - 103x^2 + 65x - 12,$
$x_0 = -0{,}5.$

№3. Визначити A і B так, щоб тричлен Ax^4+Bx^3+1 ділився на $(x-1)^2$.

№4. Побудувати многочлен найменшого порядку за даними коренями: потрійний корінь -1, прості корені 3 і 4.

№5. Не розв'язуючи рівняння $x^3-4x^2+3x+2=0$, знайти:

а) $x_1+x_2+x_3$; б) $x_1x_2+x_1x_3+x_2x_3$;

в) $x_1x_2x_3$; г) $\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}$; д) $x_1^2+x_2^2+x_3^2$.

Відповіді: ***№1.*** а) $x=2$; б) $x=1$; в) $x=1$; г) $x=-1$, $x=2$. ***№2.*** а) 6; б) 0; в) 3; г) 3; д) 3. ***№3.*** $A=3$, $B=-4$. ***№4*** $f(x)=(x+1)^3(x-3)(x-4)$. ***№5.*** а) 4; б) 3; в) -2; г) -1,5; д) 10.

Завдання для самостійного розв'язування

№1. Знайти кратність кореня $x=x_0$ многочлена $f(x)$:

а) $f(x)=x^6-4x^5-5x^4+40x^3-40x^2-32x+48$, $x_0=2$;

б) $f(x)=x^6-12x^5+53x^4-96x^3+27x^2+108x-81$, $x_0=3$;

в) $f(x)=x^8+3x^7+3x^6-x^5-6x^4-x^3+13x^2+15x+5$, $x_0=-1$;

г) $f(x)=x^6+2x^5-5x^4-20x^3-25x^2-14x-3$, $x_0=-1$;

д) $f(x)=x^7+5x^6+6x^5-3x^4-4x^3-16x-16$, $x_0=-2$.

№2. Визначити A і B так, щоб тричлен $Ax^{n+1}+Bx^n+1$ ділився на $(x-1)^2$.

№3. Побудувати многочлен з дійсними коефіцієнтами найменшого порядку за даними коренями:

а) подвійний корінь 1, прості корені 2, 3 і $1+i$;

б) потрійний корінь $2-3i$.

№4. Відокремте кратні множники многочленів:

а) $x^5+5x^4-40x^2-80x-48$;

б) $x^5-5x^4-5x^3+45x^2-108$;

в) $x^6+6x^5+9x^4-8x^3-24x^2+16$;

г) $x^6+4x^5+5x^4-5x^2-4x-1$;

д) $x^6+4x^5+4x^4-6x^3-12x^2+9$.

№5. Доведіть, що многочлен x^n-1 не має кратного кореня.

№6. Відокремте кратні множники многочленів і знайдіть їх корені:

а) $x^5 - 5x^4 - 5x^3 + 25x^2 + 40x + 16$;

б) $x^5 + 5x^4 + 3x^3 - 13x^2 - 8x + 12$;

в) $2x^6 + 6x^5 + 6x^4 + x^3 - 3x^2 - 3x - 1$;

г) $x^5 - 6ix^4 - 14x^3 + 16ix^2 + 9x - 2i$;

д) $x^7 + 3x^6 - 5x^5 - 7x^4 + 15x^3 - 19x^2 + 21x - 9$.

№7. Знаючи, що многочлен $x^4 - 4x^3 + 11x^2 - -14x + 10$ має корінь $1 - 2i$, знайдіть решту його корені.

Відповіді: ***№1.*** а) 4; б) 4; в) 3; г) 0; д) 3. ***№2.*** *A=n, B= -* (*n+*1). ***№3.*** а) $f(x)=(x-1)^2(x-2)(x-3)(x^2-2x+2)$; б) $f(x)=(x^2-4x+13)$.

Тема дев'ята
МНОГОЧЛЕНИ З РАЦІОНАЛЬНИМИ КОЕФІЦІЄНТАМИ

Попередні зауваження. Властивості модуля многочлена

У цій темі ми будемо дотримуватись функціонального погляду на многочлени, оскільки він використовується для встановлення існування і дослідженні кількості та розміщення коренів рівняння з числовими коефіцієнтами і відповідає як історичному розвитку алгебри, так і змісту сучасної шкільної програми з математики.

Важливими властивостями многочлена є наявність, кількість і розміщення його коренів. Приступаючи до вивчення цих питань, ми вже не можемо розраховувати на те, що відповідні властивості многочленів не залежатимуть від вибору основного поля *P.* Адже той самий многочлен може мати корені в одному і не мати їх у другому полі.

Для кожного многочлена $f(x)$ з кільця $P[x]$ існує своє *поле розкладу*, а саме таке розширення L поля P, в якому многочлен $f(x)$ розкладається в добуток лінійних множників. Серед числових полів найбільш важливу властивість має поле C усіх комплексних чисел. Виявляється, що полем розкладу для будь-якого многочлена $f(x)$ над полем C є саме поле C, тобто в полі комплексних чисел будь-який многочлен розкладається на лінійні множники. Іншими словами, *поле C алгебраїчно замкнуте* і є єдиним числовим полем, яке має цю фундаментальну властивість (тема вісім).

***Теорема**. Якщо $f(z)$ – многочлен ненульового степеня, то для довільного додатного числа M можна знайти таке число N, що для $|z|>N$ виконується нерівність $|f(z)| > M$.*

Це твердження означає, що $|f(z)|$ необмежено зростає, коли точка z необмежено віддаляється від початку координат, бо яким би великим не було число M, $|f(z)|$ перевищуватиме M, як тільки відстань точки z від початку координат буде більша за відповідне N.

З теореми, можна безпосередньо дістати такі важливі наслідки:

Наслідок 1. *Многочлен* $f(z)= a_nz^n + ... + a_1z + a_0$ *може мати тільки такі корені, модуль яких менший від числа* $N_0 = 1 + \frac{A}{|a_n|}$, *де A - найбільший з модулів коефіцієнтів* $|a_{n-1}|,...|a_1|, |a_0|$.

Наслідок 2. *Для* $|z| > N_0 = 1 + \frac{A}{|a_n|}$ *модуль старшого члена многочлена* $f(z)$ *більший за модуль суми всіх інших членів цього многочлена.*

Застосування попередньої теореми і її наслідків до окремого випадку – многочлена непарного степеня над полем R дійсних чисел – дає змогу встановити такий важливий факт.

***Теорема**. Многочлен непарного степеня над полем R дійсних чисел має принаймні один дійсний корінь.*

***Теорема**. Кожний многочлен степеня* $n \geq 1$ з *дійсними коефіцієнтами має принаймні один комплексний корінь.*

Ця теорема сформульована для многочленів з дійсними коефіцієнтами. Розглянемо аналогічну теорему для більш широкого класу многочленів з комплексними коефіцієнтами – основну теорему теорії многочленів.

***Теорема.** Довільний многочлен ненульового степеня з комплексними коефіцієнтами* $f(z)=a_nz^n + ...+a_1z+a_0$ *має хоча б один комплексний корінь.*

Межі дійсних коренів. Кількість дійсних коренів

Щоб знайти корені многочлена з достатнім степенем точності, треба знати, як ці корені розміщені на комплексній площині або на дійсній осі. Зауважимо, що іноді навіть немає потреби знаходити числові значення коренів, а досить лише з'ясувати їх розміщення на площині (кількість дійсних, зокрема, додатних і від'ємних коренів тощо). Наприклад, одна з важливих проблем механіки – теорія стійкості – потребує з'ясування умов, за яких усі корені даного алгебраїчного рівняння мають від'ємні дійсні частини (тобто лежать на комплексній площині зліва від уявної осі). Питання цього циклу досить складні і потребують застосування теорії функцій комплексної змінної.

Тому тут ми обмежимось розглядом питань, пов'язаних з розміщенням на дійсній осі коренів рівнянь з дійсними коефіцієнтами, що мають особливо важливе значення для задач практичного характеру.

Переходячи до розгляду дійсних коренів многочленів з дійсними коефіцієнтами, будемо знову позначати змінну буквою *x,* а не *z.*

***Теорема (про межі коренів рівняння)**. Усі дійсні корені рівняння* $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$

містяться в інтервалі $(-N_0, N_0)$, *де* $N_0 = 1 + \frac{A}{|a_n|}$, *де A - найбільший з модулів коефіцієнтів* $|a_{n-1}|, \ldots |a_1|, |a_0|$.

Справді, всі комплексні корені лежать у крузі $|z| < N_0$, а тому, якщо серед них є дійсні, то вони повинні потрапити в зазначений проміжок.

Приклад. Для рівняння $2x^5 + x^3 + x^2 - 2x - 3 = 0$ $A=3$, $a_5 = 2$ і тому $N_0 = 1 + 1{,}5 = 2{,}5$. Отже, дійсні корені цього рівняння повинні лежати в інтервалі (- 2,5; 2,5).

Є чимало способів, які дають змогу з більшою точністю встановлювати межі дійсних коренів алгебраїчних рівнянь. Ми розглянемо лише один з них, так званий *спосіб Ньютона*.

Зробимо деякі попередні зауваження.

Число N_0, визначене за теоремою, дає одночасно верхню межу додатних коренів многочлена і нижню межу його від'ємних коренів, бо вказує інтервал, в якому лежать усі дійсні корені, якщо вони існують. Один з шляхів уточнення, звуження меж, між якими слід шукати дійсні корені, полягає в тому, щоб окремо *знаходити нижню і верхню межі додатних коренів та нижню і верхню межі від'ємних коренів* даного многочлена, тобто такі чотири числа m_+, M_+, m_-, M_-, що всі додатні корені многочлена лежать в інтервалі (m_+, M_+), а всі від'ємні – в інтервалі (m_-, M_-). Якщо многочлен має корінь нуль, досить розглянути многочлен, утворений з даного діленням на *x.*

Завдання полегшується тим, що фактично досить знати як знайти лише одне з цих чотирьох чисел, наприклад M_+ – верхню межу додатних коренів. Знаходження інших трьох меж дійсних коренів рівняння $f(x)=0$ легко звести до знаходження верхньої межі додатних коренів деяких допоміжних рівнянь.

Так, зробивши в рівнянні $f(x)=0$ заміну змінної $x=1/t$, одержимо рівняння $g(t)=0$, корені якого t_i, пов'язані з відповідними коренями x_i заданого рівняння співвідношенням $t_i=1/x_i$. Якщо M'_+ – верхня межа додатних коренів рівняння $g(t)=0$, тобто $0<t_i<M'_+$ то $x_i>1/M'_+>0$, звідки видно, що за нижню межу додатних коренів рівняння $f(x)=0$ можна взяти число $1/M'_+$: $m_+=1/M'_+$.

Аналогічно, заміна $x = -y$ переводить рівняння $f(x)=0$ в рівняння $\varphi(y)=0$, корені якого y_i зв'язані з відповідними коренями x_i, рівняння $f(x)=0$ рівністю $y_i=- x_i$. Якщо y_i ($i = 1, 2, ..., q$) – всі додатні корені рівняння $\varphi(y) = 0$, то x_i ($i = 1, 2, ..., q$) – всі від'ємні корені рівняння $f(x)=0$. З нерівності $m''_+ < y_i < M''_+$ видно, що $-M''_+< x_i < -m''_+$, тобто верхня і нижня межі від'ємних коренів рівняння $f(x) = 0$ виражаються через межі додатних коренів рівняння $\varphi(y) = 0$:

$$m_- = -M''_+, M_- = -m''_+.$$

Отже, досить мати правило для знаходження верхньої межі додатних коренів многочлена.

Теорема (Ньютона). *Число M є верхньою межею додатних коренів многочлена $f(x)$, якщо для $x = M$ многочлен $f(x)$ має додатне значення, а всі його похідні – невід'ємні значення.*

Причому в більшості випадків немає потреби обчислювати всі коефіцієнти: як тільки в процесі ділення на $x - M$ отримуємо рядок з невід'ємних чисел, можна прийняти M за верхню межу додатних коренів, бо подальше застосування схеми Горнера ніколи не приведе до від'ємних коефіцієнтів. Зокрема, якщо заданий многочлен $f(x)$ має невід'ємні коефіцієнти, можна вважати $M=0$, тобто *многочлен не має додатних коренів.*

Маємо такий ***алгоритм***:

1. Знайти M_+ – верхню межу додатних коренів.

2. Зробити в рівнянні $f(x)=0$ заміну змінної $x=1/t$, одержимо рівняння $g(t)=0$. Знайти M'_+ – верхню межу додатних коренів рівняння $g(t)=0$. Тоді нижня межа додатних коренів рівняння $f(x)=0$ є число $m_+=1/M'_+$.

3. Замінити $x = -y$, отримати із рівняння $f(x)=0$ рівняння $\varphi(y)=0$. Знайти верхню межу отриманого рівняння M''_+. Замінити $y=1/u$ знайти m''_+. Тоді від'ємні корені заданого

рівняння $f(x)=0$ будуть лежати в межах $-M''_{+} < x_i < -m''_{+}$.

Наприклад. Розглянемо рівняння

$2x^5 + x^3 + x^2 - 2x - 3 = 0$.

Вище нами були знайдені межі існування дійсних коренів цього рівняння: (- 2,5; 2,5).

Враховуючи теорему Ньютона, маємо:

$f(x)=2x^5 + x^3 + x^2 - 2x - 3$,

$f'(x)=10x^4 + 3x^2 + 2x - 2$,

$f''(x)=40x^3 + 6x + 2$,

$f'''(x)=120x^2 + 6$,

$f^{(4)}(x)=240x$,

$f^{(5)}(x)=240$,

$f^{(6)}(x)=0$.

Для верхньої межі перевіримо $x=M=1$ (всі похідні для $x=1$ невід'ємні). Для цього скористаємося схемою Горнера.

	2	0	1	1	-2	-3
1	2	2	3	4	2	-1

Тут є від'ємний коефіцієнт. Спробуємо $M=1,1$.

	2	0	1	1	-2	-3
1,1	2	2,2	3,42	4,76	3,24	0,56

Отримали рядок додатних чисел, тому за верхню межу можна взяти число $M_{+} = 1,1$. Для знаходження нижньої межі додатних коренів підставимо у рівняння $x=1/t$:

$3t^5 + 2t^4 - t^3 - t^2 - 2 = 0$.

Поділивши його ліву частину на $t-1$, маємо:

	3	2	-1	-1	0	-2
1	3	5	4	3	3	1

Отримали рядок додатних чисел, тому верхньою межею створеного рівняння є число 1, а тоді за нижню межу додатних коренів заданого рівняння можна взяти число $m_{+} = 1/1 = 1$.

Для знаходження нижньої межі від'ємних коренів підставимо у задане рівняння $x = -y$:

$2y^5 + y^3 - y^2 - 2y + 3 = 0$.

Поділивши його ліву частину на y-1, маємо:

	2	0	1	-1	-2	3
1	2	2	3	2	0	3

Отже, для верхньої межі додатних коренів створеного рівняння маємо число 1, тоді для нижньої межі від'ємних коренів даного рівняння маємо $m_- = 1$.

Для знаходження нижньої межі від'ємних коренів підставимо в останнє рівняння $y = 1/u$:

$3u^5 - 2u^4 - u^3 + u^2 + 2 = 0$.

Поділивши його ліву частину на u-1, маємо:

	3	-2	-1	1	0	2
1	3	1	0	1	1	3

Отже, для верхньої межі додатних коренів створеного рівняння маємо число 1, тоді для верхньої межі від'ємних коренів даного рівняння маємо $M_- = 1$. Оскільки $m_- = M_-$, то задане рівняння не має від'ємних коренів.

Відповідь: задане рівняння має лише додатні корені, які належать проміжку (1; 1,1).

У правильності розв'язання можна переконатися, побудувавши графік функції $y = 2x^5 + x^3 + x^2 - 2x - 3$, наприклад, у програмі Desmos (рис. 9.1).

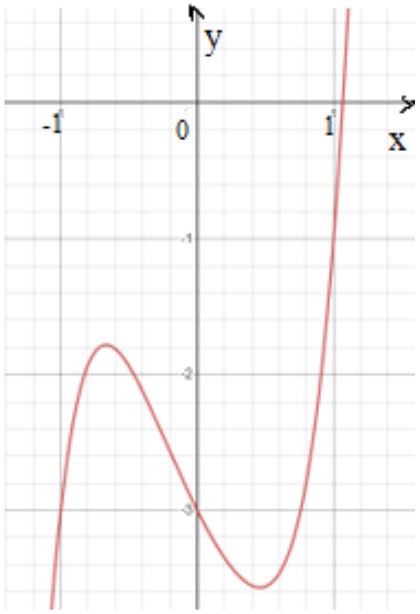


Рис. 9.1. Графік функції $y = 2x^5 + x^3 + x^2 - 2x - 3$.

Як бачимо метод Ньютона дає змогу істотно уточнити попередні відомості про межі коренів рівняння. Якщо

застосування першої теореми привело до досить «грубих» меж (-2,5; 2,5), то тепер ми знаємо, що додатні корені рівняння (якщо вони існують) розміщені в інтервалі (1; 1,1), а від'ємних коренів це рівняння не має зовсім.

Метод Ньютона настільки елементарний, що його можна використати в шкільному курсі математики, якщо тільки учні обізнані із схемою Горнера.

Знання кількості та розміщення дійсних коренів многочленів є важливою передумовою застосування багатьох методів чисельного розв'язування рівнянь. В окремих випадках деякі відомості про кількість дійсних коренів можна одержати за допомогою досить поверхового аналізу. Так, з теорем можна зробити висновок, що кількість дійсних коренів многочлена з дійсними коефіцієнтами дорівнює степеню многочлена або на парне число менше. Іноді під час знаходження меж коренів виявляється, що многочлен не має додатних або від'ємних коренів. Однак для повної відповіді на питання про кількість дійсних коренів многочлена з дійсними коефіцієнтами (або навіть про кількість таких коренів на довільному, наперед заданому інтервалі) потрібні більш глибокі дослідження.

У багатьох випадках кількість дійсних коренів рівняння з дійсними коефіцієнтами можна визначити за простим *правилом, яке дав Декарт*. Перш ніж формулювати це правило, зробимо деякі ***зауваження***.

1. Ми розглядатимемо кількість змін знаків у даній упорядкованій скінченній послідовності дійсних чисел c_1, c_2, ..., c_m розуміючи під цим *кількість пар сусідніх чисел цієї послідовності, які мають протилежні знаки.*

Наприклад, у послідовності -1, -2, 6, 3, -1, 4 є 3 зміни знаків, а в послідовності -1, -2, -6, -3, -1, -4 є 0 змін знаків.

Якщо які-небудь з чисел c_1, c_2, ..., c_m дорівнюють нулю, то під час підрахунку числа змін знаків їх до уваги не беруть.

Зауважимо, що *коли перше й останнє числа* c_1 *і* c_m *послідовності* c_1, c_2, ..., c_m *мають однакові знаки, то кількість змін знаків у послідовності парна; якщо ж* c_1 *і* c_m *мають протилежні знаки, то кількість змін знаків – непарна.*

2. Припускатимемо, що розглядуваний многочлен не має кратних коренів, оскільки завжди можна відокремити кратні множники.

***Правило Декарта**. Кількість додатних коренів многочлена з дійсними коефіцієнтами*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

дорівнює кількості змін знаків у послідовності його коефіцієнтів або на парне число менше.

Приклади.

1. Для многочлена $f(x) = x^3 - 6x + 1$ кількість змін знаків у послідовності коефіцієнтів 1, 0, -6, 1 дорівнює двом. Отже, за теоремою Декарта він має або два або 0 додатних коренів.

2. Для лівої частини рівняння $x^4+x^3+x^2+2=0$ кількість змін знаків коефіцієнтів: 1, 1, 1, 0, 2 дорівнює 0, тому додатних коренів це рівняння не має.

3. Для лівої частини рівняння $2x^5 + x^3 + x^2 - 2x - 3=0$ кількість змін знаків у послідовності коефіцієнтів дорівнює 1, тому воно має один додатний корінь (ми у цьому переконалися рис. 9.1).

Зауваження. *Правило Декарта можна застосувати і для оцінки числа від'ємних коренів рівняння з дійсними коефіцієнтами.* Для цього в рівнянні $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ потрібно зробити заміну змінної $x = -y$. Зрозуміло, що кількість від'ємних коренів даного рівняння дорівнює кількості додатних коренів рівняння $f(-y)=0$, яке можна оцінити за правилом Декарта.

Приклади.

1. У рівнянні $x^3 - 6x + 1 = 0$ заміна $x = -y$ дає рівняння $y^3 - 6y - 1=0$. Тут кількість змін знаків дорівнює 1. Отже, є один додатний корінь. А значить задане рівняння має один від'ємний корінь.

2. Рівняння $x^4 + x^3 + x^2 + 2 = 0$ заміною $x = -y$ перетворюємо в рівняння $y^4 - y^3 + y^2 + 2 = 0$. Тут маємо дві зміни знаків. Отже, задане рівняння має або два від'ємних корені, або жодного.

3. Двочленне рівняння $x^n - a=0$ для $a > 0$ має, за правилом Декарта, один додатний корінь. Якщо n парне, то

кількість від'ємних коренів також дорівнює 1, якщо n непарне, то від'ємних коренів немає. Для $a < 0$ додатних коренів немає, а кількість від'ємних коренів дорівнює 1 за непарного n і нулю – для парного n.

Як бачимо, в цьому випадку правило Декарта дає повну відповідь на питання про кількість дійсних коренів рівняння.

Якщо дане рівняння *повне*, тобто жодний його коефіцієнт не дорівнює нулю, то кількість від'ємних коренів можна визначити і не виконуючи заміни $x = -y$. Справді, в цьому випадку кількість σ змін знаків у ряді коефіцієнтів многочлена $f(-x)$ дорівнює кількості t *збережень знаків у ряді коефіцієнтів многочлена* $f(x)$. Отже, *кількість* q *від'ємних коренів повного рівняння дорівнює кількості* t *збережень знаків у ряді його коефіцієнтів або на парне число менше.* Зауважимо також, що для такого рівняння $s+t=n$ (де n – степінь рівняння), бо низка коефіцієнтів складається з $n+1$ числа.

Зауваження. Коли наперед відомо, що всі корені даного рівняння $f(x) = 0$ дійсні, то правило Декарта дає точну відповідь на питання про кількість дійсних коренів, а саме: *кількість додатних коренів дорівнює числу змін знаків у ряді коефіцієнтів многочлена* $f(x)$, *а кількість від'ємних коренів – числу змін знаків у ряді коефіцієнтів многочлена* $f(-x)$.

Справді, нехай, як і вище, p і q – кількість додатних і від'ємних коренів даного многочлена $f(x)$ n-го степеня; s і σ – кількість змін знаків у ряді коефіцієнтів многочлена $f(x)$ і многочлена $f(-x)$ відповідно. З умови, що всі корені дійсні, випливає: $p+q=n$. Якби рівняння було повним, то ми мали б також $s+\sigma = n$. Якщо ж деякі з коефіцієнтів многочлена $f(x)$ (а тому й многочлена $f(-x)$) перетворюються в нуль, то числа s і σ можуть тільки зменшитись. Тому в загальному випадку $s + \sigma \le n$, звідки $s + \sigma \le p + q$, або $(s - p) + (\sigma - q) \le 0$. Але з правила Декарта ми знаємо, що $s - p \ge 0$, $\sigma - q \ge 0$. Тому насправді $s = p$, $\sigma = q$, чим наше твердження доведене.

Отже, необхідною умовою того, щоб всі корені рівняння були дійсними, є рівність $s + \sigma = n$. Однак ця умова

не є достатньою; так, рівняння $x^2 + x + 1 = 0$ задовольняє цю умову, але не має жодного дійсного кореня.

На жаль, у більшості випадків наперед невідомо, чи всі корені рівняння дійсні. У зв'язку з цим правило Декарта, хоч і зручне з точки зору простоти застосування, *не дає повної відповіді на питання про кількість дійсних коренів рівнянь з дійсними коефіцієнтами* та їх розподіл між додатною і від'ємною півосями.

Відокремлення коренів методом Штурма

Поставимо тепер питання про те, *скільки дійсних коренів рівняння з дійсними коефіцієнтами лежить у довільному, наперед заданому інтервалі* (a, b) *дійсної осі.* Повну відповідь на це питання дає *теорема Штурма*.

Нехай дано рівняння $f(x)=0$. Насамперед побудуємо деяку послідовність многочленів, пов'язаних з многочленом $f(x)$ – так званий *ряд функцій Штурма*, який відіграє основну роль у методі Штурма. Припустимо, що $f(x)$ уже не має кратних коренів.

Знайдемо похідну $f'(x)$ і побудуємо для $f(x)$ та $f'(x)$ алгоритм, подібний до алгоритму Евкліда; відмінність полягатиме в тому, що всі остачі $R_k(x)$ ми братимемо з протилежними знаками, тобто замінюватимемо многочленами $F_k(x)=-R_k(x)$. Матимемо:

$$\begin{gathered}
f(x) = f'(x)\overline{\Phi_1}(x) - F_1(x),\\
f'(x) = F_1(x)\overline{\Phi_2}(x) - F_2(x),\\
F_1(x) = F_2(x)\overline{\Phi_3}(x) - F_3(x),\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
F_{k-1}(x) = F_k(x)\overline{\Phi_{k+1}}(x) - F_{k+1}(x),\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
F_{m-2}(x) = F_{m-1}(x)\overline{\Phi_m}(x) - F_m,\\
F_{m-1}(x) = F_m(x)\overline{\Phi_{m+1}}(x). \qquad (9.1)
\end{gathered}$$

Ми тут пишемо F_m, не зазначаючи аргументу, бо $f(x)$ та $f'(x)$ взаємно прості (за припущенням, $f(x)$ не має кратних коренів) і тому $F_m=const$. Послідовність многочленів

$$f(x), f'(x), F_1(x), F_2(x),\ldots,F_{m-1}(x), F_m \qquad (9.2)$$

і *називається рядом функцій Штурма, або просто рядом Штурма* для многочлена $f(x)$. Іноді для зручності позначатимемо $f'(x) = F_0(x)$, $f(x) = F_{-1}(x)$.

У методі Штурма нас цікавитимуть не самі функції ряду Штурма або їх значення, а лише *знаки* числових значень цих функцій. У зв'язку з цим функції ряду (9.2) можна знаходити з точністю до *сталого додатного множника*, тобто, виконуючи ділення з остачею, домножати на сталі множники; ці множники обов'язково повинні бути додатні, щоб не змінювались знаки значень многочленів.

Наприклад. Знайдемо ряд Штурма для многочлена $f(x) = x^3 - 6x + 1$.

Через те що $f'(x) = 3x^2 - 6 = 3(x^2 - 2)$, то за $F_0(x)$ можна взяти $x^2 - 2$. Маємо:

$$\begin{array}{r} x^3 - 6x + 1 \,|\, \underline{x^2 - 2} \\ \underline{-(x^3 - 2x)} \quad |x \\ -4x + 1 \end{array}$$

Остача $R_1(x) = -4x + 1$, тому за $F_1(x)$ слід узяти $-R_1(x) = 4x - 1$. Далі поділимо $F_o(x)$ на $F_1(x)$:

$$\begin{array}{r} x^2 - 2 \,|\, \underline{4x - 1} \\ \text{помножимо на 4} \quad 4x^2 - 8 \;\; |x{+}1 \\ \underline{-(4x^2 - x)} \\ x - 8 \end{array}$$

$$\begin{array}{r} \text{помножуємо на 4} \quad 4x - 32 \\ \underline{-(4x - 1)} \\ -31 \end{array}$$

Остача R_2 дорівнює -31, а $-R_2 = 31$, тобто можна узяти $F_2 = 1$. Отже, остаточно маємо:

$$F_{-1}(x) = f(x) = x^3 - 6x + 1,\ F_0(x) = x^2 - 2,$$
$$F_1(x) = 4x - 1,\ F_2 = 1.$$

Введемо поняття *кількості змін знаків у ряді Штурма.* Візьмемо в ряді функцій (9.2) $x = a$, де a – якесь дійсне число. Тоді скінченна послідовність функцій (9.2) перетворюється в послідовність чисел

$$f(a), f'(a), F_1(a), F_2(a), \ldots, F_{m-1}(a), F_m.$$

Кількість змін знаків у цій послідовності позначатимемо через $s(a)$ і називатимемо його числом змін знаків у ряді Штурма в точці a.

Наприклад. Для многочлена $f(x) = x^3 - 6x + 1$

а) для $x = 2$ маємо: $F_{-1}(2) = -3$, $F_o(2) = 2$, $F_1(2)=7$, $F_2=1$. У послідовності чисел -3, 2, 7, 1, очевидно, тільки одна зміна знаків, тобто $s(2) = 1$;

б) для $x = -1$ маємо: $F_{-1}(-1) = 6$, $F_o(-1) = -1$, $F_1(-1) = -5$, $F_2 = 1$, тобто для цього значення x маємо дві зміни знаків: $s(-1) = 2$.

Зауважимо, що при зростанні x від $x = -1$ до $x=2$ число змін знаків у ряді Штурма змінилося: $s(2) - s(-1) = -1$.

Це пов'язано з тим, що в інтервалі (-1, 2) міститься корінь многочлена $f(x) = x^3 - 6x + 1$.

Розглянемо *основні властивості ряду функцій Штурма.*

Лема 1. *Ніякі дві сусідні функції ряду Штурма* (9.2) *не мають спільних коренів.*

Лема 2. *Якщо a є коренем однієї* з *проміжних функцій ряду Штурма, то значення сусідніх з нею функцій ряду Штурма мають при цьому значенні змінної протилежні знаки.*

Оскільки кожна функція ряду Штурма є многочлен і тому неперервна на всій дійсній осі, то вона може змінити знак лише при проходженні аргументу x через її корінь. Отже, якщо x, зростаючи, не проходить через корінь жодної функції ряду Штурма, то знаки всіх функцій цього ряду, а тому й число змін знаків у ньому залишаються незмінними.

Розглянемо тепер, як впливатиме на число змін знаків у ряді Штурма проходження x через корінь якоїсь з функцій цього ряду.

Лема 3. *Якщо x, зростаючи, проходить через корінь якої-небудь проміжної функції ряду Штурма, але не проходить через корінь $f(x)$, то число змін знаків у ряді Штурма не змінюється.*

Лема 4. *Якщо x, зростаючи, проходить через корінь многочлена $f(x)$, то число змін знаків у ряді Штурма зменшується на одиницю.*

Леми 3 і 4 показують, що на число змін знаків у ряді Штурма впливає лише проходження x через корені

многочлена $f(x)$. Отже, зміна цього числа на певному проміжку може характеризувати кількість дійсних коренів многочлена $f(x)$ на цьому проміжку.

***Теорема* (*Штурма*).** *Якщо a і b* ($a<b$) *– довільні дійсні числа, які не є коренями многочлена* $f(x)$, *то кількість p дійсних коренів многочлена* $f(x)$ *в інтервалі* (a, b) *дорівнює* $p = s(a) - s(b)$, *де* $s(a)$ *і* $s(b)$ *є кількість змін знаків у ряді Штурма відповідно в точках a і b.*

Зауваження.

1. У теоремі зазначено, що a і b не є коренями многочлена $f(x)$. Ця умова практично не становить труднощів під час застосування теореми Штурма. Справді, якщо a (або b) є коренем многочлена $f(x)$, то питання про розміщення цього дійсного кореня розв'язується само собою, а для визначення положення інших коренів слід змінити межі вибраного інтервалу або розглядати многочлен, який отримуємо у результаті ділення $f(x)$ на лінійний двочлен $x - a$ (або $x - b$).

Теорема Штурма істинна і для випадку, коли кінці інтервалу можуть бути коренями многочлена. Тільки тоді $s(a)$-$s(b)$ є кількість коренів не на інтервалі (a, b), а на півінтервалі $(a, b]$.

2. Якщо якась з проміжних функцій ряду Штурма $F_k(x)$ не має дійсних коренів, то можна наступних функцій Штурма не знаходити і користуватися в теоремі Штурма «скороченим» рядом

$$f(x), f'(x), F_1(x), \ldots F_k(x).$$

Справді, число змін знаків у «залишковому» ряді Штурма $F_k(x)$, …, $F_{m-1}(x)$, F_m є сталим для будь-якого x. Адже x може пройти лише через корінь проміжної функції ряду, що, за лемою 3, не впливає на число змін знаків у цьому ряді. Отже, «залишковий» ряд не впливає на різницю $s(a)$- $s(b)$.

3. Метод Штурма можна застосувати і без попереднього відокремлення кратних коренів. Якщо $f(x)$ має кратні корені, то остання функція ряду Штурма $F_m(x)$ вже не є сталою. Але тоді $F_m(x)$ є спільним дільником $f(x)$, $f'(x)$ та всіх проміжних функцій ряду Штурма і можна розглянути ряд многочленів

$$\frac{f(x)}{F_m(x)}, \frac{f'(x)}{F_m(x)}, \frac{F_1(x)}{F_m(x)}, \dots, \frac{F_{m-1}(x)}{F_m(x)}, 1 \qquad (9.3)$$

який вже має всі властивості, зазначені в лемах 1-4. Через те, що число змін знаків у ряді (9.3) збігається з числом змін знаків у звичайному ряді Штурма (9.2), то теорема Штурма залишається в силі. Слід лише ураховувати, що вона дає в цьому випадку кількість дійсних коренів не самого многочлена $f(x)$, а многочлена $\frac{f(x)}{F_m(x)}$ (в якому вже немає кратних коренів), тобто кількість різних коренів многочлена $f(x)$ в інтервалі (a, b) без урахування їх кратності.

Наприклад. Застосуємо теорему Штурма до многочлена $f(x)=x^3-6x+1$, для якого ми в попередньому прикладі побудували ряд Штурма і для інтервалу (-1; 2) отримали такі результати щодо числа змін знаків у цьому ряді:

x	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$s(x)$
-1	6	-1	-5	1	2
2	-3	2	7	1	1

Ми бачимо, що $s(-1) - s(2) = 1$, тобто інтервал (- 1; 2) містить один корінь даного многочлена.

Зауважимо, що практично немає потреби обчислювати значення функцій ряду Штурма в точках a і b, можна лише визначати їх знаки в цих точках (виконуючи обчислення наближено). Відповідно до цього ми в таблицях наводитимемо лише знаки функцій Штурма.

Теорема Штурма дає змогу розв'язувати найрізноманітніші задачі щодо розміщення коренів многочленів на дійсній осі. Розглянемо дві такі задачі.

Задача 1. За допомогою ряду Штурма для довільного многочлена $f(x)$ над полем дійсних чисел можна *точно визначити загальну кількість дійсних коренів,* а також *кількість його додатних і від'ємних коренів.* Для цього достатньо застосувати теорему Штурма до інтервалів $(-N_0, 0)$ і $(0, N_0)$, де N_0 – межа модуля коренів, бо поза інтервалом $(-N_0, N_0)$ многочлен $f(x)$ дійсних коренів не має.

На практиці, щоб не підставляти чисел $\pm N_0$ у функції ряду Штурма, замість інтервалів $(-N_0, 0)$ і $(0, N_0)$

розглядають інтервали (-∞, 0) і (0, + ∞). При цьому користуються тим, що для $x \geq N_0$ знак многочлена визначається знаком його старшого члена. Тому під знаком многочлена «коли $x = \infty$» розуміють знак його старшого члена при додатному x, а під знаком многочлена «коли $x = -\infty$» – знак його старшого члена при від'ємному x.

Наприклад. Знайдемо кількість дійсних (додатних і від'ємних) коренів многочлена $f(x)=x^3 - 6x + 1$.

Нагадаємо, що його функціями Штурма є: $F_0(x)= x^2 - 2$, $F_1(x)= 4x - 1$, $F_2 = 1$.

Складемо таблицю:

x	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$s(x)$
-∞	-	+	-	+	3
0	+	-	-	+	2
+∞	+	+	+	+	0

Отже, многочлен $f(x)$ має три дійсних корені, з них два додатних і один від'ємний. Це збігається з результатом дослідження цього многочлена за допомогою правила Декарта.

Якщо кількість окремо додатних і окремо від'ємних коренів нас не цікавить, то теорему Штурма застосовуємо відразу до інтервалу (-∞;∞).

Задача 2. За допомогою теореми Штурма можна здійснювати так зване відокремлення дійсних коренів. Відокремлення коренів полягає в знаходженні таких інтервалів, у кожному з яких лежить точно один дійсний корінь многочлена. Ця задача дуже важлива, бо більшість методів наближеного обчислення коренів потребує попереднього відокремлення їх. Практично відокремлення коренів зводиться до підбору кінців потрібних інтервалів. Покажемо на прикладі, як роблять такий підбір.

Наприклад. Відокремимо дійсні корені многочлена $f(x) = x^3 - 6x + 1$.

Дійсні корені $f(x)$ лежать в інтервалі $(-N_0, N_0)$, де $N_0 = 1 + \frac{A}{|a_n|}$. У цьому разі $N_0 = 7$. Отже, за найлівішу точку дослідження можна взяти -7. Для $f(x)$ маємо такі функції ряду Штурма: $F_0(x)= x^2 - 2$, $F_1(x)= 4x - 1$, $F_2 = 1$ (див. приклад вище).

Складемо таблицю:

x	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$s(x)$
-7	-	+	-	+	3
-6	-	+	-	+	3
-5	-	+	-	+	3
-4	-	+	-	+	3
-3	-	+	-	+	3
-2	+	+	-	+	2
-1	+	-	-	+	2
0	+	-	-	+	2
1	-	-	+	+	1
2	-	+	+	+	1
3	+	+	+	+	0
7	+	+	+	+	0

З цієї таблиці видно, що один корінь лежить в інтервалі (-3, -2), другий – в інтервалі (0, 1), а третій – в інтервалі (2, 3). Корені відокремлено.

Зауважимо, що на практиці відокремлюють корені і визначають загальну кількість дійсних коренів, як правило, одночасно, у зв'язку з чим спочатку в таблиці проставляють знаки функцій ряду Штурма коли $x = -\infty$, $x=0$, $x = +\infty$, а потім уже заповнюють проміжні рядки.

При цьому часто доцільно, щоб зменшити кількість спроб, визначити знаки функцій Штурма в точках, які приблизно є серединами вже досліджених проміжків. Так, у розглянутому вище прикладі ми з'ясували, що в інтервалі (-7, 0) лежить один корінь многочлена. Тому, можна було перевірити після x=-7, x=-3. Визначивши s(-3)= s(-7) ми з'ясовуємо, що один корінь лежить у правій «половині» цього інтервалу, а саме між -3 і 0. У цьому випадку відпадає потреба перевіряти x=-6, x=-5, x=-4. Аналогічно на інтервалі (0; 7) ми знаємо, що існує два кореня. Знаходимо s(7)=s(3), отже, шукані корені належать інтервалу (0; 3), тому відпадає необхідність перевіряти x=4, x=5, x=6.

Задача 3. За допомогою ряду Штурма можна знайти просту ознаку того, що всі n коренів многочлена $f(x)$ n-го степеня є дійсні різні числа. Для цього, очевидно, потрібно, щоб у ряді Штурма при зростанні x від $-\infty$ до $+\infty$ число змін знаків зменшилось на n. У свою чергу, для цього насамперед потрібно, щоб кількість функцій у ряді Штурма

була не меншим за $n + 1$. Оскільки за самою побудовою цього ряду вона не може бути більшою за $n + 1$, то у випадку всіх дійсних коренів ряд Штурма складається точно з $n + 1$ функцій, причому кожна наступна функція цього ряду є многочленом степеня на одиницю нижчого, ніж попередня. Тепер видно, що всі корені будуть дійсними, якщо $s(-\infty) = n$, а $s(+\infty) = 0$. Зрозуміло, що це має місце тоді і тільки тоді, коли старші коефіцієнти всіх функцій Штурма одного знаку.

Отже, *для того щоб усі корені многочлена $f(x)$ степеня n були дійсні й різні, необхідно і достатню, щоб відповідний ряд Штурма складався з $n+1$ многочленів, старші коефіцієнти яких усі того самого знаку.*

Зауважимо, що розглянутий вище многочлен $f(x)= x^3 - 6x + 1$ задовольняє ці умови.

Отже, теорема Штурма дає змогу повністю розв'язати всі питання, пов'язані з розміщенням дійсних коренів алгебраїчних рівнянь. Недоліком методу Штурма є деяка громіздкість його. Є й інші способи знаходження послідовності функцій, що має всі властивості ряду функцій Штурма (9.2) і тому може замінити його у теоремі Штурма, проте ці способи не простіші за знаходження ряду (9.2). Іноді застосовують також деякі «спрощені ряди функції Штурма», але вони в загальному випадку не дають точної відповіді на питання про кількість коренів (подібно до правила Декарта).

Звідність і незвідність многочленів у полі раціональних чисел

***Означення**. Алгебраїчні рівняння – це рівняння виду $P(x_1, x_2, \ldots, x_n)=0$, де P – многочлен від змінних $x_1, x_2, \ldots, x_n$.*

Наявність раціональних коренів у довільно взятого алгебраїчного рівняння – явище досить рідкісне. Тому знаходження таких коренів не має великого практичного значення. Але, якщо многочлен $f(x)$ над полем Q раціональних чисел, або, що те саме, рівняння $f(x) = a_nx^n + \ldots + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ з раціональними коефіцієнтами має раціональні корені, то в багатьох випадках ці корені можна знайти. Знаючи навіть один корінь r, можна

спростити дане рівняння, звівши його до рівняння (n - 1)-го степеня діленням на $x - r$.

Основна відмінність многочленів над полем Q раціональних чисел від многочленів над полем R всіх дійсних чисел або полем C всіх комплексних чисел полягає в тому, що *існують многочлени з раціональними коефіцієнтами як завгодно високого степеня, незвідні у полі раціональних чисел,* тоді як у кільці $C[x]$ звідним є довільний многочлен, степінь якого вищий від одиниці (п.1), а в кільці $R[x]$ звідним є кожний многочлен, степінь якого перевищує 2, навіть якщо цей многочлен не має жодного дійсного кореня.

Розглянемо деякі властивості многочленів з раціональними коефіцієнтами.

Насамперед зауважимо, що *будь-яке алгебраїчне рівняння з раціональними коефіцієнтами множенням на спільний знаменник усіх коефіцієнтів можна звести до рівняння з цілими коефіцієнтами.*

Наприклад. Рівняння $\frac{1}{3}x^3 + \frac{1}{2}x^2 + x - \frac{2}{3} = 0$ множенням на 6 можна звести до вигляду

$$2x^3 + 3x^2 + 6x - 4=0.$$

Оскільки зручніше мати справу з цілими, а не з дробовими числами, ми далі намагатимемося зводити всі питання щодо многочленів над полем Q до відповідних питань відносно многочленів з цілими коефіцієнтами. Зокрема, так можна зробити з питанням про звідність многочленів в полі Q.

Означення. *Многочлен $p(x)$ з цілими коефіцієнтами називається примітивним, якщо його коефіцієнти не мають спільних дільників, відмінних від* ± 1.

Наприклад. Многочлен $2x^3+3x^2+6x-4$ примітивний, тоді як многочлен $2x^4 - 4x^3 +6x^2-12$ не є примітивним.

Лема. *Добуток двох примітивних многочленів є примітивним многочленом.*

Розглянемо тепер питання про звідність многочлена з цілими коефіцієнтами в полі раціональних чисел.

Теорема. *Для того, щоб многочлен $f(x)$ з цілими коефіцієнтами був звідним у полі Q раціональних чисел, необхідно і достатньо, щоб він був звідним у кільці Z цілих чисел,*

тобто щоб існували многочлени $f_1(x)$ і $f_2(x)$ ненульового степеня з цілими коефіцієнтами такі, що $f(x) = f_1(x)\, f_2(x)$.

Теорема (Ейзенштейна). *Якщо в многочлені з цілими коефіцієнтами*

$$f(x) = a_n x_n + a_{n-1} x_{n-1} + \ldots + a_1 x + a_0$$

коефіцієнти a_0, a_1, ..., a_{n-1} – діляться на деяке просте число p, причому a_0 не ділиться на p^2, а старший коефіцієнт a_n не ділиться на p, то многочлен $f(x)$ незвідний у полі раціональних чисел.

Теорема. *Якщо многочлен $f(x)$ з раціональними коефіцієнтами, степінь якого більший за одиницю, має хоча б один раціональний корінь r, то $f(x)$ звідний у полі раціональних чисел.*

Твердження, обернене до цієї теореми, неправильне: многочлен $f(x)$ може не мати жодного раціонального кореня, але бути звідним у полі раціональних чисел. Наприклад, многочлен $x^4 - 4$ звідний у полі Q: $x^4 - 4 = (x^2-2)(x^2+2)$, але раціональних коренів не має.

Проте у випадку многочлена третього степеня обернена теорема істинна.

Теорема*. Якщо многочлен третього степеня $f(x)$ з раціональними коефіцієнтами не має раціональних коренів, то він незвідний у полі раціональних чисел.*

Раціональні корені многочленів з раціональними коефіцієнтами

Розглянемо елементарні способи знаходження раціональних коренів рівнянь з раціональними коефіцієнтами. Ми вже зазначали, що рівняння над полем Q, завжди можна вважати рівнянням з цілими коефіцієнтами.

Основне практичне значення для цього питання має така теорема.

Теорема*. Щоб число $\frac{p}{q}$, де p і q – взаємно прості числа, було коренем рівняння $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$ з цілими коефіцієнтами, необхідно, щоб p було дільником вільного члена a_0, а q – дільником старшого коефіцієнта a_n цього рівняння.*

Наслідок. *Якщо старший коефіцієнт рівняння з цілими коефіцієнтами дорівнює* 1, *то всі раціональні корені цього рівняння є цілі числа і дільники вільного члена.*

Теорема дає змогу за коефіцієнтами a_0 і a_n даного рівняння визначити всі раціональні числа, які можуть бути коренями цього рівняння. Далі, підставляючи ці числа в рівняння, можна знайти, які з них є його коренями.

Наприклад. Рівняння $6x^4 + 19x^3 - 7x^3 - 26x + 4 = 0$ може мати раціональними коренями лише такі числа:

$$\pm 1, \pm 2, \pm 4, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{4}{3},$$

тобто ті нескоротні дроби $\frac{p}{q}$, чисельники яких є дільниками числа 4, а знаменники – дільниками числа 6.

На практиці частіше користуються не самою теоремою, а її наслідком. Адже кожне рівняння з цілими коефіцієнтами можна звести до рівняння з цілими коефіцієнтами, в якому старший коефіцієнт 1. Для цього треба помножити рівняння на a_n^{n-1} і зробити заміну $a_n x = y$.

Приклад. Для рівняння $2x^3 + 3x^2 + 6x - 4=0$ після множення на 2^2 і заміни $y=2x$ маємо:

$y^3 + 3y^2+12y - 16=0$.

До такого рівняння вже можна застосувати наслідок з теореми. Його раціональними коренями можуть бути лише цілі числа – дільники вільного члена тобто ±1; ±2; ±4; ±8; ±16.

Проте таке зведення не завжди доцільно робити.

Теорема дає необхідну умову того, щоб раціональне число було коренем даного рівняння з цілими коефіцієнтами. Проте бажано мати кілька необхідних умов, щоб за допомогою їх зменшувати число спроб-підставлянь у рівняння.

Теорема. *Для того, щоб* $\frac{p}{q}$, де $(p, q) = 1$, *було раціональним коренем многочлена з цілими коефіцієнтами* $f(x) = a_n x^n + \ldots + a_1 x + a_0$, *необхідно, щоб при довільному цілому* k *число* $f(k)$ *ділилося на* $p - qk$ (*якщо тільки* $p - qk \neq 0$).

Наслідок. *Якщо старший коефіцієнт* a_n *даного многочлена* $f(x)$ з *цілими коефіцієнтами дорівнює одиниці, то його раціональними коренями можуть бути лише такі*

цілі числа p, для яких f(k) ділиться на p – k при всякому цілому k, при якому p – k ≠ 0.

Теорема дає змогу отримати довільну кількість необхідних умов того, щоб число $\frac{p}{q}$ було коренем даного рівняння, бо числу k можна надавати довільних цілих значень. Найбільш поширені на практиці умови, що відповідають $k = \pm 1$, бо вирази $f(1)$ і $f(-1)$ легко обчислити, їх можна сформулювати так:

Щоб число $\frac{p}{q}$ *було раціональним коренем многочлена з цілими коефіцієнтами, потрібно, щоб* $\frac{f(1)}{p-q}$ *і* $\frac{f(-1)}{p+q}$ *були цілими числами.*

Приклад. Застосуємо наслідок теореми до рівняння:

$$6x^4 + 19x^3 - 7x^2 - 26x + 12 = 0.$$

Воно може мати лише такі раціональні корені:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12,$$
$$\pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{3}{2}, \pm\frac{4}{3}, \pm\frac{1}{6}.$$

Для даного рівняння $f(1) = 4$, $f(-1)=18$.

Подивимось, для яких з чисел, крім ± 1, відношення $\frac{4}{p-q}$ є цілим числом. Такими є числа:

$$2, \pm 3, \frac{1}{2}, \pm\frac{1}{3}, \frac{2}{3}, \frac{3}{2}, \frac{4}{3}.$$

Як бачимо, замість 24 чисел маємо вже тільки 9 чисел, які можуть бути коренями рівняння. Тепер застосуємо до останніх чисел умову, щоб $\frac{18}{p+q}$ було цілим числом. Залишаються числа 2; -3; $\frac{1}{2}$; $\frac{-1}{3}$. Ці числа доцільно вже перевірити безпосередньо. Якби їх було ще багато, можна було б застосувати теорему при k=2. Перевірка показує, що лише два з цих чисел, а саме $\frac{1}{2}$ і -3 є раціональними коренями даного рівняння. Ділячи ліву частину рівняння на $x + 3$ і $x-\frac{1}{2}$ за схемою Горнера, отримуємо квадратне рівняння, що має корені

$$x_{1,2} = \frac{-1 \pm \sqrt{13}}{3}.$$

Разом з числами $\frac{1}{2}$ і -3 маємо всі чотири корені даного рівняння.

На практиці доцільно поєднувати наведені тут прийоми знаходження раціональних коренів рівнянь із способами обчислення меж дійсних коренів (п.1). Так, для останнього прикладу вже найпростіший метод обмеження коренів показує, що всі дійсні його корені лежать в інтервалі $\left(-5\frac{1}{3}, 5\frac{1}{3}\right)$, бо для цього рівняння $N_0 = 1 + \frac{26}{6} = 5\frac{1}{3}$, тому потреба у перевірці деяких з чисел відпадає відразу. Тим більше слід ураховувати межі коренів, якщо користуватись наслідками з теорем.

Зауважимо, що замість того, щоб підставляти раціональне число *r* у многочлен *f*(*x*), можна поділити *f*(*x*) на *x* - *r*. Якщо остача дорівнює нулю, то *r* є коренем *f*(*x*), у противному разі *r* не є коренем *f*(*x*). Цей метод має ту перевагу перед звичайною підстановкою, що він дає змогу відразу отримати коефіцієнти частки від ділення на *x*-*r*, якщо *r* буде коренем, і перейти до розгляду рівняння нижчого степеня.

Приклади розв'язування типових завдань

№1. *Знайти раціональні корені многочлена* $f(x)=x^3- 6x^2+15x - 14$.

Розв'язання. Корені шукаємо серед дільників вільного члена*:* $p= \pm1, \pm2, \pm7, \pm14$, $q=1$.

$f(1)=1- 6+15-14=-4$, тоді p-1 має бути дільником числа 4, тоді залишаються лише варіанти p = -1 та p = 2.

$$f(-1)=-1-6-15-14\neq0, f(2)=8-24+30-14=0.$$

Отже, маємо єдиний раціональний корінь x=2.

*Відповід*ь: 2.

№2. *Користуючись ознакою Ейзенштейна довести незвідність многочлена* $f(x)=x^4-8x^3+12x^2-6x+2$.

Розв'язання. Відповідно до теореми, якщо в многочлені з цілими коефіцієнтами

$$f(x) = a_n x_n + a_{n-1}x_{n-1} + \ldots + a_1 x + a_0$$

коефіцієнти $a_0, a_1, \ldots, a_n$ – діляться на деяке просте число p, причому a_0 не ділиться на p^2, а старший коефіцієнт a_n не ділиться на p, то многочлен $f(x)$ незвідний у полі раціональних чисел. Підберемо таке число p. Коефіцієнт $a_4=1$, ділиться лише на ± 1, $a_3=-8$, $a_2=12$, $a_1=-6$, $a_0=2$. $p=$ СД(-8, 12, -6, 2) $=\pm 2$, a_4 не ділиться на ± 2, a_0 не ділиться на $(\pm 2)^2=4$. Тоді відповідно до ознаки Ейзенштейна многочлен є незвідним.

№3. *Знайти систему многочленів Штурма для многочлена* $f(x) = x^4 - x - 3$.

*Розв'язання. З*находимо $f_0(x) = f'(x) = 4x^3 - 1$.

Далі потрібно поділити (кутом) $f(x)$ на $f_0(x)=f'(x)$. Щоб уникнути дробів, скористаємося можливістю помножити будь-який многочлен Штурма на додатнє число: $4f(x) = 4x^4 - 4x - 12$. Ділитимемо на $4x^3-1$. У залишку отримаємо $-3x - 12$. Відповідно до алгоритму треба взяти $F_1(x) = -R_1(x) = 3x + 12$. Але ми, користуючись можливістю множити будь-який многочлен Штурма на додатнє число, візьмемо $F_1(x)=x+4$. Тепер ділимо $f_0(x)$ на $F_1(x)$ із залишком (кутом) і отримаємо в залишку число -257. Отже, можна взяти $F_2(x) = 1$. Одночасно ми переконуємося, що НСД $\big(f(x), f'(x)\big) = 1$, отже даний многочлен немає кратних множників.

Відповідь:

$f(x) = x^4 - x - 3, f_0(x) = 4x^3 - 1, F_1(x) = x + 4, F_2 = 1$

– система многочленів Штурма для даного многочлена $f(x)$.

Завдання для аудиторного заняття

№1. Знайти раціональні корені многочленів:

а) $f(x)=x^4-2x^3-8x^2+13x-24$;

б) $f(x)=x^5-7x^3-12x^2+6x+36$;

в) $f(x)=6x^4+19x^3-7x^2-26x+12$;

г) $f(x)=10x^4-13x^3+15x^2-18x-24$.

№2. Користуючись ознакою Ейзенштейна довести незвідність многочлена $f(x)=x^5-12x^3+36x-12$.

№3. Обмежити зверху та знизу дійсні корені многочлена:

а) $f(x)=x^4-4x^3+7x^2-8x+3$;

б) $f(x)=x^4+4x^3-8x^2-10x+14$.

№4. Скласти многочлени Штурма і відділити корені многочленів:

а) $f(x)=x^3+x^2-2x-1$; б) $f(x)=x^3-x+5$;

в) $f(x)=x^4-12x^2-16x-4$; г) $f(x)=x^4-2x^3-4x^2+5x+5$.

Відповіді: ***№1.*** а)-3; б)-2, 3; в)-3, 0,5; г) раціональних коренів нема. **№2**. для $p=3$. ***№3***. а) (0, 3); б) (-6,2). ***№4.*** а) $f(x)=x^3+x^2-2x-1$, $F_0(x)=3x^2+2x-2$, $F_1(x)=2x+1$, $F_2(x)=1$, три дійсні корені (- 2,-1), (-1,0), (1,2); б) $f(x)=x^3-x+5$, $F_0(x)=3x^2-1$, $F_1(x)=2x-15$, $F_2(x)=-1$, один дійсний корінь (-2,-1); *в)* $f(x)=x^4-12x^2-16x-4$, $F_0(x)=x^3-6x-4$, $F_1(x)=3x^2+6x+2$, $F_2(x)=x+1$, $F_3(x)=1$, чотири дійсні корені (-3,-2) (-2,-1), (-1,0), (4,5); *г)* $f(x)=x^4-2x^3-4x^2+5x+5$, $F_0(x)=4x^3-6x^2-8x+5$, $F_1(x)=22x^2-22x-45$, $F_2(x)=2x-1$, $F_3(x)=1$, чотири дійсні корені (1,2) (2,3), (- 1,0), (-2,-1) .

Завдання для самостійного розв'язування

№1. Знайти раціональні корені многочленів:

а) $f(x)=24x^4-42x^3-77x^2+56x+60$;

б) $f(x)=x^5-2x^4-4x^3+4x^2-5x+6$;

в) $f(x)=x^4+2x^3-13x^2-38x-24$.

№2. Користуючись ознакою Ейзенштейна довести незвідність многочлена $f(x)=x^4-x^3+2x+1$.

№3. Обмежити зверху та знизу дійсні корені многочлена $f(x)=x^7-108x^5-445x^3+900x^2+801$.

№4. Скласти многочлени Штурма і відділити корені многочленів:

а) $f(x) = x^3+3x - 5$;

б) $f(x) = x^4+4x^3 - 12x+9$;

в) $f(x) = x^4 - 2x^3 + x^2 - 2x+1$.

№5. Методом Штурма відокремити дійсні корені многочленів:

а) $x^4 - 6x^3 + 13x^2 - 14x + 7$;

б) $2x^5 - 10x^4 + 10x^3 + 10x^2 - 10x - 5$;

в) $x^4 - 4x^3 + 10x^2 - 12x + 4$.

№6. Знайти найбільший спільний дільник многочлена і його похідну:

а) $(x-2)^3(x+1)^2(x-3)$;

б) $(x^4-1)(1-x)^3(x^2-1)^2(x-1)^3$;

в) $x^4 - 8x^3 + 12x^2 - 6x + 2$.

Відповіді: ***№1.*** *а*)2,5, -3/4; б)1, -2, 3; в)-1, -2, -3, 4. ***№2.*** для p=3, після розкладу за степенями x-1. ***№3.*** (-11,11). ***№4.*** а) $f(x)=x^3+3x-5$, $F_0(x)=x^2+1$ один дійсний корінь (1,2); б) $f(x)=x^4+4x^3-12x+9$, $F_0(x)=x^3+3x^2-3$, $F_1(x)=x^2+3x-4$, $F_2(x)=-4x+3$, $F_3(x)=1$, дійсних коренів нема; *в)* $f(x)=x^4-2x^3+x^2 - 2x+1$, $F_0(x)=2x^3-3x^2+x-1$, $F_1(x)=x^2+5x-3$, $F_2(x)=-9x+5$, $F_3(x)= =-1$, два дійсні корені (0,1) (1,2).

Тема десята
РІВНЯННЯ ТРЕТЬОГО ТА ЧЕТВЕРТОГО СТЕПЕНЯ. ПОНЯТТЯ РОЗВ'ЯЗНОСТІ У КВАДРАТНИХ РАДИКАЛАХ

Кубічні рівняння

Загальний вигляд кубічного рівняння такий:

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \ (a_3 \neq 0).$$

Якщо старший коефіцієнт a_3 кубічного рівняння відмінний від 1 то, поділивши обидві частини даного рівняння на a_3, отримуємо рівняння рівносильне даному, але в якого старший коефіцієнт уже дорівнює одиниці. Тому далі обмежимось розглядом кубічного рівняння, старший коефіцієнт якого дорівнює 1. Нехай дано кубічне рівняння:

$$x^3+ax^2+bx + c = 0 \qquad (10.1)$$

з будь-якими комплексними коефіцієнтами.

Щоб позбутися в рівнянні члена з невідомим у другому степені, замінимо в рівнянні (10.1) невідоме x новим невідомим y:

$$x = y - \frac{a}{3} \qquad (10.2)$$

Тоді отримуємо рівняння:

$$y^3 + (-\frac{a^2}{3} + b)y + (\frac{2a^3}{27} - \frac{ab}{3} + c) = 0. \qquad (10.3)$$

Якщо знайдемо корені рівняння (10.3), то, підставивши їх у співвідношення (10.2) замість невідомого y, одержимо корені заданого рівняння (10.1).

Отже, щоб розв’язати рівняння (10.1), досить уміти розв’язувати «неповне» кубічне рівняння:

$$y^3+py+q=0 \qquad (10.4)$$

з будь-якими комплексними коефіцієнтами.

Розглянемо один з кількох відомих способів

розв'язування рівняння (10.4). Запишемо невідоме y у вигляді суми $y=u+v$, де u і v – нові невідомі, і підставимо цей вираз у рівняння (10.4). Маємо:

$$(u+v)^3 + p(u+v) + q = 0,$$

або, після розкриття дужок і перегрупування членів, $(u^3+v^3+q)+(3uv+p)(u+v)=0$. Якщо u і v вибрати так, щоб

$$u^3 + v^3 = -q, uv = -\frac{p}{3}, \qquad (10.5)$$

то тоді $y=u+v$ буде коренем рівняння (10.4). Але якщо для u і v справджуватимуться рівності (10.5), то справджуватимуться також і рівності

$$u^3 + v^3 = -q, u^3v^3 = -(\frac{p}{3})^3, \qquad (10.6)$$

і тому u^3 і v^3 за формулами Вієта для коренів квадратного рівняння будуть коренями квадратного рівняння $z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$.

Нехай $v^3 = z_2 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$,

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}},$$

$$v = \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}. \qquad (10.7)$$

Відповідно до цього:

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}. \qquad (10.8)$$

Це і є формула коренів кубічного рівняння, яку називають *формулою Кардано.*

Кубічний корінь з будь-якого комплексного числа, відмінного від нуля, має в полі комплексних чисел три значення. Отже, *u* і *v* мають по три значення.

Може виникнути думка, що, комбінуючи три значення *u* з трьома значеннями *v,* одержимо дев'ять різних значень *y* за формулою (10.3). Проте не слід забувати, що система (10.6), яку ми фактично розв'язували, не рівносильна системі (10.5), бо рівняння $uv=(-p/3)$ замінено рівнянням $u^3v^3 = -(p/3)^3$. Внаслідок цього не всі розв'язки системи (10.6) будуть розв'язками системи (10.5). Тому слід вибрати лише ті значення коренів (10.7), які задовольняють друге з рівнянь (10.5), тобто умову:

$$uv = (-p/3). \qquad (10.9)$$

Застосовуючи формулу Кардано, знаходять значення одного з радикалів, а відповідні їм значення другого радикала визначають, користуючись співвідношенням (10.9), і, таким чином, знаходять усі три корені рівняння (10.4).

Спинимося на цьому питанні докладніше.

Нехай u_0 – будь-яке одне з трьох значень *u.* Тоді два інших значення *u* можна дістати множенням u_0 на кубічні корені ε_1 і ε_2 з одиниці. Отже,

$$\varepsilon_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2},$$

$$\varepsilon_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Позначимо символом v_0 те з трьох значень радикала *y*, яке відповідає значенню u_0 радикала *u.* Із співвідношення (10.9): $v_0 = -\frac{p}{3u_0}$. Двома іншими значеннями *y* будуть $v_0\varepsilon_1$ і $v_0\varepsilon_2$. Значенню $u_a\varepsilon_1$ радикала *u* відповідатиме значення $v_0\varepsilon_2$ радикала *v,* бо:

$$(u_a\varepsilon_1)(v_0\varepsilon_2)=(u_0v_0)(\varepsilon_1\varepsilon_2) = u_0v_0=(-p/3).$$

Так само легко переконатися, що значенню $u_0\varepsilon_2$ радикала u відповідає значення $v_0\varepsilon_1$ радикала v. Додаючи відповідні значення u і v, знайдемо три корені рівняння (10.3):

$$y_0=u_0+v_0,\ y_1=u_0\varepsilon_1+v_0\varepsilon_2,\ y_2=u_0\varepsilon_2+v_0\varepsilon_1. \qquad (10.10)$$

Отже, кожне кубічне рівняння з будь-якими числовими коефіцієнтами має в полі комплексних чисел три корені.

Наприклад. Розв'язати рівняння: $x^3 - 9x^2 + 21x - 5 = 0$. Замінемо в цьому рівнянні невідоме x новим невідомим y, пов'язаним з x співвідношенням:

$$x=y-a/3=y+3.$$

Отримуємо рівняння

$$(y + 3)^3 - 9(y+ 3)^2 + 21 (y + 3) - 5=0, \text{ тобто}$$

$$y^3-6y+4=0.$$

У цьому рівнянні $p = -6$, $q = 4$. Отже,

$$u = \sqrt[3]{-\frac{q}{2}+\sqrt{(\frac{q}{2})^2+(\frac{p}{3})^3}}=\sqrt[3]{-2+\sqrt{4-8}}=$$

$$=\sqrt[3]{-2+2i}=\sqrt[3]{2\sqrt{2}(cos\frac{3}{4}\pi+isin\frac{3}{4}\pi)}=$$

$$=\sqrt{2}(cos\frac{\frac{3}{4}\pi+2\pi k}{3}+isin\frac{\frac{3}{4}\pi+2\pi k}{3}),\ k=0,\ 1,\ 2$$

Позначимо символом u_0 значення радикала u, яке ми отримуємо для $k = 0$, тобто

$$u_0=\sqrt{2}\left(cos\frac{\pi}{4}+isin\frac{\pi}{4}\right)=1+i.$$

Із співвідношення $uv = (-p/3)$ маємо:

$$v_0=-\frac{p}{3u_0}=1-i,$$

$$y_0=u_0+v_0=1+i+1-i=2,$$

$$y_1 = u_0\varepsilon_1 + v_0\varepsilon_2 = (1+i)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)+$$

$$+(1-i)\left(-\tfrac{1}{2}-\tfrac{\sqrt{3}}{2}i\right) = -1-\sqrt{3},$$

$$y_2 = u_0\varepsilon_2 + v_0\varepsilon_1 = (1+i)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)+$$

$$+(1-i)\left(-\tfrac{1}{2}+\tfrac{\sqrt{3}}{2}i\right) = -1+\sqrt{3}.$$

Знаючи, що $x=y+3$, знаходимо, нарешті, корені заданого рівняння:

$$x_0 = y_0 + 3 = 5, x_1 = y_1 + 3 = 2 - \sqrt{3},$$

$$x_2 = y_2 + 3 = 2 + \sqrt{3}.$$

Нехай дано неповне кубічне рівняння:

$$y^3+py+q=0 \qquad (10.11)$$

з дійсними коефіцієнтами. З'ясуємо, що можна сказати про корені цього рівняння. В цьому випадку вираз $\mathbf{(q/2)^2+(p/3)^3}$, що стоїть у формулі Кардано під знаком квадратного кореня, є дійсне число. Воно може бути додатним, дорівнювати нулю або бути від'ємним. Розглянемо кожну з цих можливостей.

1. Нехай $\mathbf{(q/2)^2+(p/3)^3 > 0.}$ У цьому випадку в формулі Кардано під знаком кожного з квадратних коренів стоїть додатне число, а тому під знаком кожного з кубічних коренів стоятиме дійсне число. Отже, кожен з кубічних радикалів u і v матиме одне дійсне значення й два – комплексні спряжені. Позначимо символом u_0 дійсне значення радикала u. Тоді відповідне йому значення v_0 радикала v також буде дійсним, оскільки добуток u_0v_0 повинен дорівнювати дійсному числу $-p/3$. Таким чином, корінь $y_0=u_0+v_0$, рівняння (10.11) буде дійсним числом. Два інші корені цього рівняння ми знайдемо за формулами (10.10):

$$y_1 = u_0\varepsilon_1 + v_0\varepsilon_2 = u_0\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) +$$
$$+v_0\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = -\frac{u_0+v_0}{2} + i\sqrt{3}\frac{u_0-v_0}{2},$$
$$y_2 = u_0\varepsilon_2 + v_0\varepsilon_1 = u_0\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) +$$
$$+v_0\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = -\frac{u_0+v_0}{2} - i\sqrt{3}\frac{u_0-v_0}{2}.$$

Оскільки u_0 і v_0 є дійсні значення різних кубічних радикалів, то $u_0 \neq v_0$. І, таким чином, корені y_1 й y_2 є спряженими комплексними числами.

Отже, *якщо* $\boldsymbol{(q/2)^2+(p/3)^3>0}$*, то рівняння* (10.11) *має один дійсний і два комплексні спряжені корені.*

2. Нехай $\boldsymbol{(q/2)^2+(p/3)^3=0}$*.* У цьому випадку $u = \sqrt[3]{-\frac{q}{2}}$, $v = \sqrt[3]{-\frac{q}{2}}$.

Нехай u_0 – дійсне значення радикала u. Відповідне йому значення v_0 радикала v також є дійсним числом, бо $u_0v_0=-p/3$. Але оскільки $\sqrt[3]{-\frac{q}{2}}$ має лише одне дійсне значення, то $v_0=u_0$. Тому:

$y_0=u_0+v_0=2u_0$

$$y_1 = u_0\varepsilon_1 + v_0\varepsilon_2 = u_0\varepsilon_1 + u_0\varepsilon_2 = u_0(\varepsilon_1 + \varepsilon_2) =$$
$$= u_0\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2} - \frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = -u_0,$$
$$y_1 = u_0\varepsilon_2 + v_0\varepsilon_1 = u_0\varepsilon_2 + u_0\varepsilon_1 = u_0(\varepsilon_2 + \varepsilon_1) =$$
$$= u_0\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2} - \frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = -u_0.$$

Отже, *якщо* $\boldsymbol{(q/2)^2+(p/3)^3=0}$*, то всі корені рівняння* (10.11) *дійсні, причому два з них рівні між содою.*

3. Нехай, нарешті $\boldsymbol{(q/2)^2+(p/3)^3<0}$. У цьому випадку в формулі Кардано під знаком кожного з квадратних радикалів стоїть дійсне від'ємне число. Отже, під знаком кубічних радикалів u і v стоятимуть комплексні числа,

а тому всі значення радикалів будуть комплексними числами.

Покажемо, що в цьому випадку у формулі Кардано значення радикала *v* повинно бути спряжене відповідному значенню радикала *u.* Справді, нехай $u_0 = a+bi$ буде будь-яке із значень радикала *u,* а v_0 – відповідне йому значення радикала *v.* Тоді відповідно до правила добування кореня *n*-го степеня:

$$|u_0| = \left|\sqrt[3]{-\frac{q}{2}+\sqrt{(\frac{q}{2})^2+(\frac{p}{3})^3}}\right| =$$

$$= \sqrt[3]{\left|-\frac{q}{2}+\sqrt{(\frac{q}{2})^2+(\frac{p}{3})^3}\right|} =$$

$$= \sqrt[3]{\left|-\frac{q}{2}+i\sqrt{-(\frac{q}{2})^2-(\frac{p}{3})^3}\right|} = \sqrt[3]{\sqrt{\left(\frac{q}{2}\right)^2-\left(\frac{q}{2}\right)^2-\left(\frac{p}{3}\right)^3}} =$$

$$= \sqrt[3]{\sqrt{-\left(\frac{p}{3}\right)^3}} = \sqrt{-\frac{p}{3}},$$

і тому $v_0 = -\frac{p}{3u_0} = -\frac{p\overline{u_0}}{3u_0\overline{u_0}} = -\frac{p\overline{u_0}}{3|u_0|^2} =$

$$= -\frac{p\overline{u_0}}{3(-\frac{p}{3})} = \overline{u_0}\,,$$ тобто $v_0 = a-bi.$

Таким чином, за формулами (10.10)

$$y_0=u_0+v_0=(a+bi)+(a-bi)=2a,$$

$$y_1 = u_0\varepsilon_1 + v_0\varepsilon_2 = (a+bi)\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) +$$

$$+(a-bi)\left(-\tfrac{1}{2}-\tfrac{\sqrt{3}}{2}i\right) = -a-b\sqrt{3},$$

$$y_2 = u_0\varepsilon_2 + v_0\varepsilon_1 = (a+bi)\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) +$$

$$+(a-bi)\left(-\tfrac{1}{2}+\tfrac{\sqrt{3}}{2}i\right) = -a+b\sqrt{3}.$$

Як бачимо, в цьому випадку рівняння (10.11) має три різні дійсні корені. Тим часом формула Кардано виражає

ці корені через корені з комплексних чисел, причому можна довести, що їх ніяким способом не можна виразити через коефіцієнти за допомогою радикалів з дійсними підкореневими виразами. Тому розглядуваний випадок дістав назву *незвідного*. Останній випадок переконливо доводить, що практична цінність формули Кардано невелика. Справді, хоч у цьому випадку всі корені рівняння з дійсними коефіцієнтами дійсні, проте відшукання їх за формулою Кардано вимагає добування кубічного кореня з комплексних чисел, для чого треба записувати ці числа в тригонометричній формі. Отже, запис коренів кубічного рівняння за допомогою радикалів втрачає практичне значення.

Рівняння четвертого степеня

Перейдемо тепер до розгляду рівняння четвертого степеня $a_4x^4+a_3x^3+a_2x^2+a_1x+a_0=0.$ (10.12)

Якщо старший коефіцієнт a_4 рівняння (10.12) відмінний від 1, то, поділивши обидві частини цього рівняння на a_4, одержимо рівняння вигляду

$$x^4+ax^3+bx^2+cx+d=0. \qquad (10.13)$$

Є багато способів розв'язання рівняння четвертого степеня (10.13). Ми викладемо найбільш ранній метод розв'язання рівняння, який належить Феррарі.

Насамперед рівняння підстановкою $x = y -(a/4)$ зведемо до рівняння вигляду

$$y^4+py^2+qy+r= 0. \qquad (10.14)$$

Перетворимо тотожно ліву частину рівняння за допомогою допоміжного параметра α:

$y^4+py^2+qy+r=(y^2+\alpha)^2-[(2\alpha-p)y^2-qy+(\alpha^2-r)]$.

Тоді рівняння, (10.14) запишеться так:

$$(y^2+\alpha)^2-[(2\alpha-p)y^2-qy+(\alpha^2-r)]=0. \qquad (10.15)$$

Підберемо тепер α так, щоб многочлен, який стоїть у квадратних дужках, став повним квадратом. Це очевидно, буде тоді, коли цей многочлен матиме один дво-

кратний корінь, тобто коли його дискримінант дорівнюватиме нулю:

$$q^2-4(2\alpha-p)(\alpha^2-r)=0. \qquad (10.16)$$

Співвідношення (10.16) є кубічним рівнянням відносно невідомого α з комплексними коефіцієнтами. Корені цього рівняння можна знайти за формулою Кардано. Нехай α_0 – один з коренів цього рівняння, який виражається за допомогою радикалів через коефіцієнти рівняння (10.16), тобто рівняння (10.14). При такому виборі значення α_0 многочлен, що стоїть у квадратних дужках в лівій частині рівняння (10.15), має двократний корінь $\frac{q}{2(2\alpha-p)}$, і тому рівняння (10.15), тобто рівняння (10.14), запишеться так:

$$(y^2+\alpha_0)^2 - (2\alpha_0 - p)[y^2 - \frac{q}{2(2\alpha-p)}]^2=0. \qquad (10.17)$$

Рівняння (10.17), як легко бачити, рівносильне сукупності рівнянь:

$$\begin{bmatrix} y^2 + \sqrt{2a_0 - p}y + \left(a_0 - \frac{q}{2\sqrt{a_0-p}}\right) = 0 \\ y^2 - \sqrt{2a_0 - p}y + \left(a_0 + \frac{q}{2\sqrt{a_0-p}}\right) = 0 \end{bmatrix},$$

Розв'язавши цю сукупність рівнянь, ми знайдемо чотири корені рівняння (10.14). Як легко побачити, корені рівняння (10.14) за допомогою алгебраїчних дій виражаються через його коефіцієнти.

Двочленні рівняння

Двочленним рівнянням n-го степеня називається рівняння виду $ax^n + b = 0$, *де n – натуральне число і* $a\neq0$.

Поділивши обидві частини рівняння на відмінне від 0 число й позначивши $(-b/a)$ буквою q одержимо рівняння:

$$x^n - q=0 \qquad (10.18)$$

Розв'язками рівняння (10.18) будуть значення $x = \sqrt[n]{q}$. Отже, розв'язування рівняння зводиться до добування кореня n-го степеня з числа q. Якщо $q\neq0$, то корінь $\sqrt[n]{q}$ має n

різних коренів. Якщо ж q=0, то рівняння зводиться до одночленного, яке задовольняє лише значення $x = 0$.

Зауважимо, що коли відоме одне із значень $\sqrt[n]{q}$, то розв'язування рівняння (10.18) зводиться до розв'язування рівняння $y^n-1=0$.

Справді, нехай x_0 – одне із значень $\sqrt[n]{q}$. Замінивши в рівнянні (10.18) невідоме x новим невідомим y, пов'язаним з x співвідношенням $x = x_0y$, одержимо рівняння $x_0^n\, y^n - q = 0$. Звідси, поділивши обидві частини рівняння на $x_0^n = q \neq 0$, маємо: $y^n-1=0$. Розв'язками рівняння є значення кореня n-го степеня з 1. Знайшовши ці значення за формулою

$$\varepsilon_k = cos\frac{2\pi k}{n} + isin\frac{2\pi k}{n}, k = 0,1 \dots n-1$$

і помноживши кожне з них на x_0, одержимо всі n розв'язків рівняння (10.18).

Наприклад. 1. Розв'язати рівняння $x^4-16 = 0$.

Візьмемо за x_0 арифметичне значення $\sqrt[4]{16} = 2$, тобто $x_0 = 2$.

$$x_k = 2\left(cos\frac{2\pi k}{n} + isin\frac{2\pi k}{n}\right), k = 0, 1, 2, 3.$$

Тобто: $x_0 = 2$, $x_1 = 2i$, $x_2 = -2$, $x_3 = -2i$.

Слід зауважити, що окремі двочленні рівняння можна розв'язати розкладанням лівої частини їх на множники. Зокрема, такі завдання наявні у шкільному курсі математики після вивчення формул скороченого множення, методу інтервалів тощо. Наприклад, рівняння $x^4-16 = 0$, де $x \in R$, у шкільному курсі математики розв'язується шляхом розкладання лівої частини рівняння на множники і прирівнювання кожного з них до нуля. У результаті чого отримують, що на множині дійсних чисел рівняння має два корені $x_1 = 2$ і $x_2 = -2$.

Наведемо ще один приклад, зокрема обчислення виразу $a^{2020} + \frac{1}{a^{2020}}$, якщо $a^2 + a + 1 = 0$, використовуючи апарат шкільного курсу математики базового рівня та апарат алгебри і теорії чисел.

Перший спосіб (*завдання розглядається як олімпіадне*). Використаємо формулу різниці кубів*:*

$a^3 - 1 = (a-1)(a^2 + a + 1)$, звідси
$a^3 = (a-1)(a^2 + a + 1) + 1 = (a-1) \cdot 0 + 1 = 1.$

Тоді $(a^3)^{673} \cdot a + \frac{1}{(a^3)^{673} \cdot a} = 1^{673} \cdot a + \frac{1}{1^{673} \cdot a} = \frac{a^2+1}{a} =$
$= \frac{(a^2+a+1)-a}{a} = -\frac{a}{a} = -1.$

*Відповід*ь: -1*.*

Другий спосіб. Знайдемо *a,* розв'язавши квадратне рівняння

$$a^2 + a + 1 = 0.$$

Отримуємо, що дискримінант $D = -3 < 0$, отже дане рівняння не має розв'язків на множині дійсних чисел.

Знайдемо розв'язки квадратного рівняння на множині комплексних чисел. Маємо:

$$a_1 = \frac{-1+i\sqrt{3}}{2};\ a_2 = \frac{-1-i\sqrt{3}}{2}.$$

Числа a_1 та a_2 є спряженими.

Застосувавши формулу Муавра, можемо обчислити значення виразу $a^{2020} + \frac{1}{a^{2020}}$. Для цього попередньо запишемо a_1 і a_2 в тригонометричній формі. Маємо: $a_1 = cos\frac{2\pi}{3} + i\ sin\frac{2\pi}{3}$; $a_2 = cos\frac{2\pi}{3} - i\ sin\frac{2\pi}{3}$.

За формулою Муавра обчислюємо значення виразу для a_1. Маємо:

$$a^{2020} = 1^{2020}\left(\cos 2020 \cdot \frac{2\pi}{3} + i\ \ sin\, 2020 \cdot \frac{2\pi}{3}\right) =$$
$$= 1\left(\cos\cdot \frac{2\pi}{3} + i\ \ sin\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Тоді $a^{2020} + \frac{1}{a^{2020}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} - \frac{1}{2} - i\frac{\sqrt{3}}{2} = -1.$

Аналогічно обчислюється значення виразу для a_2*.*

Відповідь: -1*.*

Розв’язність рівнянь у квадратних радикалах

Як відомо, не кожне алгебраїчне рівняння можна розв’язати у радикалах, тобто виразити всі його корені через коефіцієнти за допомогою скінченного числа дій додавання, віднімання, множення, ділення і добування кореня з цілим показником степеня.

***Теорема* (*Руффіні-Абеля*).** *Алгебраїчне рівняння n-го степеня з довільними буквеними коефіцієнтами при n≥5 не можна розв’язати в радикалах.*

Разом з тим існують окремі класи рівнянь вищих степенів, які можна розв’язати у радикалах. Загальне дослідження проблеми розв’язності алгебраїчних рівнянь у радикалах є предметом важливої галузі алгебри – так званої теорії Галуа. Виклад цієї теорії виходить за межі цього курсу. Проте одне з питань теорії розв’язності рівнянь у радикалах ми розглянемо тут (в елементарній формі), ураховуючи його особливе значення для традиційного шкільного курсу математики. Йдеться про *розв'язність алгебраїчних рівнянь у квадратних радикалах.* Саме до цього питання зводиться дослідження можливості чи неможливості розв’язати певну геометричну *задачу на побудову за допомогою циркуля і лінійки.*

***Означення**. Вважатимемо, що алгебраїчне рівняння*

$$a_n x^n + \ldots + a_1 x + a_0 = 0 \ (a_n \neq 0) \qquad (10.19)$$

можна розв’язати у квадратних радикалах, якщо кожний з його n коренів можна подати через коефіцієнти a_j (j = 0, 1, ..., n) за допомогою скінченної кількості дій додавання, віднімання, множення, ділення та добування квадратного кореня.

Якщо дії додавання, віднімання, множення і ділення назвати *раціональними операціями*, то формулювання означення можна дещо скоротити, а саме:

***Означення**. Рівняння* (10.19) *розв’язне у квадратних радикалах, якщо кожний його корінь можна подати через коефіцієнти a_j (j= 0, 1, ..., n) за допомогою скінченної кількості раціональних операцій та дій добування квадратного кореня.*

Очевидно, будь-яке лінійне рівняння $ax + b = 0$ та будь-яке квадратне рівняння $ax^2 + bx + c = 0$ розв'язуються у квадратних радикалах.

Існують рівняння, степінь яких перевищує 2 і які розв'язуються у квадратних радикалах.

Очевидно, виконання раціональних операцій рівносильне розв'язуванню лінійного рівняння виду $ax+b=c$, а добування квадратного кореня – розв'язуванню двочленного квадратного рівняння $x^2- a = 0$. Тому *можливість розв'язати деяке рівняння в квадратних радикалах означає, що його можна звести до скінченного ланцюжка двочленних рівнянь, степінь яких не вищий від* 2, *а коефіцієнти раціонально виражаються через коефіцієнти даного рівняння та корені проміжних рівнянь ланцюжка.*

Наприклад. Розглянемо квадратне рівняння

$$ax^2 + bx + c = 0 \quad (a \neq 0).$$

Звичайне виведення формули для розв'язків цього рівняння рівносильне послідовному розв'язанню такого ланцюжка двочленних рівнянь:

$$y^2 - \frac{b^2-4ac}{4a^2} = 0, x + \frac{b}{2a} - y = 0.$$

Подивимось тепер на розв'язність рівняння в квадратних радикалах з точки зору алгебраїчних розширень числових полів.

Нехай $f(x)$ – ліва частина даного рівняння (10.19) – є многочлен над числовим полем Δ. При цьому вважатимемо, що Δ – мінімальне числове поле, яке містить коефіцієнти a_0 , a_1, ..., a_n многочлена $f(x)$, тобто $\Delta=Q(a_0 , a_1, ..., a_n)$, оскільки будь-яке числове поле містить підполе Q усіх раціональних чисел.

Означення. *Основним полем* Δ (або областю раціональності) *рівняння* $a_nx^n + ... + a_1x + a_0 = 0$ *називають алгебраїчне розширення* $Q(a_0 , a_1, ..., a_n)$ *поля Q раціональних чисел, утворене приєднанням коефіцієнтів даного рівняння.*

Лема. *Для того щоб рівняння* (10.19) *було розв'язним у квадратних радикалах, необхідно і достатньо, щоб кожний з його коренів можна було виразити через деякі числа поля* Δ

за допомогою скінченної кількості раціональних операцій та дій добування квадратного кореня.

Далі нам зручно вживати вислів типу «число η виражається у квадратних радикалах через числа b_1, b_2, ..., b_m». Це означає, що число η можна подати через числа b_j (j=1,2, ..., m) за допомогою скінченної кількості раціональних операцій та дій добування квадратного кореня.

Розв'язність рівняння у квадратних радикалах означає можливість виразити всі його корені у квадратних радикалах через числа основного поля Δ.

З другого боку, очевидно, що *можливість виразити якесь число η у квадратних радикалах через числа поля* Δ *означає можливість виразити усі числа поля* Δ (η) *у квадратних радикалах через числа поля* Δ.

***Означення**. Якщо* Δ *– основне поле рівняння* $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$, *а* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *– корені цього рівняння, то поле* $Q = A(\alpha_1, \alpha_2, \ldots, \alpha_n)$, *утворене приєднанням до* Δ *усіх коренів* α_j ($j = 1, \ldots. n$) *називається нормальним полем* (нормою) *або полем розкладу даного рівняння.*

Теорема. *Для того, щоб рівняння* (10.19) *розв'язувалось у квадратних радикалах, необхідно і достатньо, щоб будь-яке число з його нормального поля n виражалось у квадратних радикалах через числа основного поля* Δ.

Наслідок. *Якщо* Δ_1 *– квадратичне розширення поля* Δ, *то будь-яке число* $\eta \in \Delta_1$ *виражається у квадратних радикалах через число поля* Δ.

Числа, що виражаються у квадратних радикалах

Число η, яке виражається у квадратних радикалах через числа поля Δ, як випливає з означення, можна подати у формі

$$\eta = r\left(\sqrt{q_1}, \sqrt{q_2}, \ldots \sqrt{q_m}\right), \qquad (10.20)$$

де r (x_1, x_2, ..., x_n) – раціональна функція над полем Δ, а q_1, ..., q_m – числа, які виражаються у квадратних радикалах через числа поля Δ.

У загальному випадку кореневий вираз $\sqrt{q_i}$ побудовано так, що у ньому кілька квадратних коренів добуваються

один з одного. Назвемо *порядком* даного кореневого виразу *кількість послідовних квадратних радикалів, що стоять один під одним.* Так, вираз $\sqrt{5}$ має порядок 1; вираз $\sqrt{2\sqrt{5}-10}$ – порядок 2; вираз виду $\sqrt{a+b\sqrt{c+d\sqrt{c}}}$ має порядок 3. Позначимо через p найбільший з порядків виразів $\sqrt{q_i}$, i=1…m у представлені (10.20) числа η.

У подальшому викладі, вживаючи величину порядку p_η, матимемо на увазі, що вона відноситься до певного (взагалі кажучи, не єдино можливого) зображення цього числа у квадратних радикалах, є показником цього зображення. Якщо $\eta \in \Delta$, вважатимемо $p_\eta = 0$.

Теорема. *Для того щоб число η виражалось у квадратних радикалах через числа поля Δ, необхідно і достатньо, щоб існувала скінченна сукупність полів* $\Delta_1, \Delta_2, \ldots, \Delta_k$ таких, що:

1) Δ_1 є *квадратичним розширенням поля* Δ;
2) Δ_{j+1} *є квадратичним розширенням поля* Δ_j (j= 1, 2, ..., k-1);
3) *число η належить полю* Δ_k.

$\Delta \subseteq \Delta_1 \subseteq \ldots \subseteq \Delta_k$, з яких перше є заданим полем, кожне наступне – квадратичним розширенням попереднього, а останнє містить число η.

Зауважимо, що разом з η в Δ_k входить усе поле $\Delta(\eta)$, тобто мінімальне поле, що містить η і Δ (бо Δ_k також містить як η, так і Δ).

Наприклад. Для числа $\eta = \sqrt{\sqrt{1+\sqrt{2}}+\sqrt{5}}$ відповідний ланцюжок полів буде:

$$\Delta = Q, \Delta_1 = Q(\sqrt{5}), \Delta_2 = \Delta_1(\sqrt{2}), \Delta_3 = \Delta_2\left(\sqrt{1+\sqrt{2}}\right),$$

$$\Delta_4 = \Delta_3(\sqrt{\sqrt{1+\sqrt{2}}+\sqrt{5}}).$$

Остання теорема є *критерієм* можливості виразити число у квадратних радикалах через числа даного поля Δ. Цей критерій має той недолік, що його важко застосовувати при дослідженні конкретної задачі.

***Теорема**. Всі числа, які можна виразити у квадратних радикалах через числа поля* Δ, *алгебраїчні над цим полем.*

Нехай η – деяке число, і треба з'ясувати, чи можна його виразити у квадратних радикалах через числа поля Δ. Ураховуючи теорему, завжди можна вважати, що η є коренем деякого многочлена над полем Δ: $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, бо для трансцендентного (не-алгебраїчного) над полем Δ числа це питання вже з'ясоване – таке число не можна виразити у квадратних радикалах через числа поля Δ. Отже, бажано було б мати ознаку, за допомогою якої з властивостей многочлена можна було б зробити висновок про можливість чи неможливість виразити корінь η у квадратних радикалах через елементи основного поля Δ.

***Теорема.* (*Необхідна умова можливості виразити корінь многочлена у квадратних радикалах*).** *Якщо корінь* η *незвідного у полі* Δ *многочлена виражається у квадратних радикалах через числа поля* Δ, *то степінь* n *многочлена* $f(x)$ *є числом виду* 2^m (m – ціле невід'ємне).

Наслідок. *Корені многочлена* $f(x)$, *незвідного в полі* Δ, *степінь якого не є степенем числа* 2, *не виражаються в квадратних радикалах через числа цього поля.*

Розв'язність у квадратних радикалах рівнянь 3-го і 4-го степенів. Загальний критерій розв'язності у квадратних радикалах

Багато цікавих і важливих задач зводиться до з'ясування питання про можливість виразити у квадратних радикалах корені многочленів 3-го степеня. Для таких многочленів легко знайти зручний і простий критерій розв'язності у квадратних радикалах.

***Теорема.** Для того щоб усі корені кубічного многочлена над полем* Δ *виражались у квадратних радикалах через числа поля* Δ, *необхідно і достатньо, щоб цей многочлен був звідним у полі* Δ.

Або інакше. *Алгебраїчне рівняння* 3-го *степеня* $ax^3 + bx^2 + cx + d = 0$ *розв'язується у квадратних радикалах тоді і тільки тоді, коли многочлен* $f(x)=ax^3 + bx^2 + cx + d$ *звідний у полі* Δ.

Зауважимо, що умова для всіх коренів кубічного многочлена рівносильна умові хоч для одного кореня цього многочлена. Справді, з можливості виразити якийсь корінь многочлена 3-го степеня у квадратних радикалах випливає звідність цього многочлена, а із звідності випливає така можливість для усіх трьох коренів.

Наприклад. Нехай над полем Q задано многочлен

$$f(t) = t^3+16t - 32.$$

Щоб з'ясувати питання про можливість виразити його корені у квадратних радикалах, слід встановити звідність чи незвідність $f(t)$ в полі Q. Для цього, в свою чергу, досить з'ясувати, чи має $f(t)$ раціональні корені.

Як відомо, всі раціональні корені зведеного многочлена з цілими коефіцієнтами є цілі числа і дільники вільного члена. Отже, ці корені слід шукати серед чисел ±1; ±2; ±4; -±8; ±16; ±32. Легко впевнитись безпосередньо, що жодне з цих чисел не є коренем многочлена. Отже, $f(t)$ – незвідний у полі раціональних чисел многочлен, тому жодний його корінь не виражається у квадратних радикалах через числа поля Q.

Розглянемо тепер довільне рівняння

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \qquad (10.21)$$

з основним полем Δ і поставимо питання про критерій розв'язності цього рівняння у квадратних радикалах.

Теорема. **(*Критерій розв'язності рівняння у квадратних радикалах*).** *Для того щоб рівняння* (10.21) *з основним полем* Δ *і нормою* Ω *розв'язувалось у квадратних радикалах, необхідно і достатньо, щоб степінь норми* Ω *відносно поля* Δ *був цілим невід'ємним степенем числа* 2, *тобто* $(\Omega : \Delta) = 2^m$ ($m \geq 0$, ціле).

Сформульований критерій, застосовний у принципі до будь-якого алгебраїчного рівняння, має той недолік, що стосовно до окремих конкретних задач він часто виявляється недостатньо ефективним. Це пов'язано з тим, що в більшості випадків для даного многочлена над полем Δ зовсім не просто побудувати норму Ω і визначити її степінь $(\Omega : \Delta)$.

Приклади розв'язування типових завдань

№1. *Розв'язати рівняння*: $x^3 + 3x - 3x - 14 = 0$.

Розв'язання. Пам'ятаємо, що для того, щоб отримати загальний розв'язок кубічного рівняння виду $ax^3 + bx + + cx + d = 0$ (де $a \neq 0$), потрібно його звести до канонічного вигляду $z^3 + pz + q = 0$. Це можна зробити шляхом ділення рівняння на старший коефіцієнт a та зробивши заміну змінної

$x = z - \frac{b}{3a}$, тобто $x = z - \frac{3}{3} = z - 1$.

Підставимо заміну в задане кубічне рівняння, отримаємо:

$(z-1)^3 + 3(z-1)^2 - 3(z-1) - 14 = 0$.

$z^3 - (-1)z^2 + 3z - 1 + 3(z^2 - (-1)2z + 1) - 3z + 3 - - 14 = 0$.

$$z^3 - 3z^2 + 3z - 1 + 3z^2 + 6z + 3 - 3z + 3 - 14 = 0$$

$$z^3 + 6z - 9 = 0.$$

Знайдемо коефіцієнти p і q:

$$q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a} = \frac{2 \cdot 3^3}{27 \cdot 1^3} - \frac{3 \cdot (-3)}{3 \cdot 1^2} + \frac{(-14)}{1} = = \frac{2 \cdot 27}{27} - \frac{(-9)}{3} + (-14) = 2 + 3 - 14 = -9;$$

$$p = \frac{c}{a} - \frac{b^2}{3a^2} = \frac{-3}{1} - \frac{3^2}{3 \cdot 1^2} = -3 - \frac{9}{3} = -3 - 3 = -6.$$

$$z^3 - 6z - 9 = 0.$$

$$D = \frac{q^2}{4} + \frac{p^3}{27} = \frac{81}{4} + \frac{(-6)^3}{27} = \frac{81}{4} - \frac{216}{27} = = \frac{2187 - 864}{108} = \frac{49}{4}.$$

$D = \frac{49}{4} > 0$, отже рівняння має один дійсний і два комплексні корені (якщо D<0, то всі три корені рівняння є різними дійсними числами, якщо D=0, то всі корені рівняння є дійсними числами, де два з них будуть однаковими).

$$z_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{D}} + \sqrt[3]{-\frac{q}{2} + \sqrt{D}} = \sqrt[3]{\frac{9}{2} - \frac{7}{2}} + \sqrt[3]{\frac{9}{2} + \frac{7}{2}} = 1 + 2 = 3;$$

$$z_2 = -\frac{1}{2}\left(\sqrt[3]{-\frac{q}{2}-\sqrt{D}}+\sqrt[3]{-\frac{q}{2}+\sqrt{D}}\right)+$$
$$+\frac{\sqrt{3}}{2}i\left(\sqrt[3]{-\frac{q}{2}-\sqrt{D}}-\sqrt[3]{-\frac{q}{2}+\sqrt{D}}\right)=-\frac{1}{2}\cdot 3+\frac{\sqrt{3}}{2}i=$$
$$=-\frac{3}{2}+\frac{\sqrt{3}}{2}i;$$
$$z_2 = -\frac{1}{2}\left(\sqrt[3]{-\frac{q}{2}-\sqrt{D}}+\sqrt[3]{-\frac{q}{2}+\sqrt{D}}\right)-$$
$$-\frac{\sqrt{3}}{2}i\left(\sqrt[3]{-\frac{q}{2}-\sqrt{D}}-\sqrt[3]{-\frac{q}{2}+\sqrt{D}}\right)=-\frac{1}{2}\cdot 3-\frac{\sqrt{3}}{2}i=$$
$$=-\frac{3}{2}-\frac{\sqrt{3}}{2}i.$$

Повернувшись до заміни $x = z - 1$, отримаємо:

$$x_1 = 2; \quad x_2 = -\frac{5}{2}+\frac{\sqrt{3}}{2}i; \quad x_3 = -\frac{5}{2}-\frac{\sqrt{3}}{2}i.$$

Відповідь: $x_1 = 2; \quad x_2 = -\frac{5}{2}+\frac{\sqrt{3}}{2}i; \quad x_3 = -\frac{5}{2}-\frac{\sqrt{3}}{2}i.$

№2*. Розв'язати рівняння*: $x^4 - 2x^3 + 6x^2 - 2x + 5 = 0$.

Розв'язання. Застосовуємо метод Феррарі. Залишимо в лівій частині рівняння перші два доданки, а решту перенесемо в праву частину:

$$x^4 - 2x^3 = -6x^2 + 2x - 5.$$

У лівій частині виділимо повний квадрат додавши до обох частин ввівши нову зміну *t*:

$$(x^2 - x)^2 = -5x^2 + 2x - 5.$$

Доповнимо ліву частину цього рівняння до повного квадрата ввівши нову зміну *t*:

$$(x^2 - x)^2 + 2t(x^2 - x) + t^2 =$$
$$= 2t(x^2 - y) - 5x^2 + 2x + t^2 - 5.$$

$$(x^2 - x + t)^2 = (2t - 5)x^2 + (2 - 2t)x + t^2 - 5.$$

Виберемо *t* так, щоб у правій частині рівняння був теж повний квадрат. При цьому дискримінант квадратного

тричлена відносно змінної t має дорівнювати нулю:

$$(1-t)^2-(t^2-5)(2t-5)=0,$$
$$1-2t+t^2-2t^3+5t^2+10t-25=0,$$
$$t^3-3t^2-4t+12=0.$$

Знайдемо один з коренів останнього рівняння. У цьому разі можна не застосовувати формулу Кардано. Тоді

$$t^2(t-3)-4(t-3)=0,$$
$$(t-3)(t^2-4)=0.$$

Одним з коренів останнього рівняння є $t_1=3$. Отже, маємо

$$(x^2-x+3)^2=x^2-4x+4,$$
$$(x^2-x+3)^2-(x-2)=0,$$
$$(x^2-2x+5)(x^2+1)=0.$$

Останнє рівняння рівносильне сукупності рівнянь

$$x^2-2x+5=0,$$
$$x^2+1=0.$$

Розв'язуючи її знаходимо

$$x_{1,2}=\pm 1, \qquad x_{3,4}=1\pm 2i.$$

Відповідь: $x_{1,2}=\pm 1,\ x_{3,4}=1\pm 2i$.

№3. *Розв'язати рівняння* $y^3-24y-32=0$.

Розв'язання. Тут $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3<0$. Отже, ми маємо незвідний випадок.

Радикал u у цьому випадку запишеться так:

$$u=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}=$$
$$=\sqrt[3]{16+\sqrt{256-512}}=\sqrt[3]{16+16i}.$$

Щоб добути кубічний корінь з комплексного числа $\alpha=a+bi=16+16i$, запишемо це число в тригонометричній

формі. Знайдемо його модуль ρ і аргумент φ.

$$\rho = \sqrt{16^2 + 16^2} = 16\sqrt{2};$$

$$cos\varphi = \frac{16}{16\sqrt{2}} = \frac{\sqrt{2}}{2};\ \ sin\varphi = \frac{16}{16\sqrt{2}} = \frac{\sqrt{2}}{2};\ \varphi = \frac{\pi}{4}.$$

Отже, $u = \sqrt[3]{16\sqrt{2}\left(cos\frac{\pi}{4} + i\,sin\frac{\pi}{4}\right)} =$

$$= \sqrt[6]{512}\left[cos\frac{\frac{\pi}{4} + 2\pi k}{3} + i\,sin\frac{\frac{\pi}{4} + 2\pi k}{3}\right], k = 0, 1, 2.$$

Звідси

$$u_0 = 2\sqrt{2}\left(cos\frac{\pi}{12} + isin\frac{\pi}{12}\right) = 2\sqrt{2}cos\frac{\pi}{12} + 2\sqrt{2}sin\frac{\pi}{12}.$$

І за формулами:

$$y_0 = 4\sqrt{2}cos\frac{\pi}{12},$$

$$y_1 = -2\sqrt{2}\left(cos\frac{\pi}{12} + \sqrt{3}sin\frac{\pi}{12}\right),$$

$$y_2 = -2\sqrt{2}\left(cos\frac{\pi}{12} - \sqrt{3}sin\frac{\pi}{12}\right).$$

Застосувавши формули половина кута, знаходимо:

$$sin\frac{\pi}{12} = \sqrt{\frac{1-cos\frac{\pi}{6}}{2}} = \sqrt{\frac{1-\frac{\sqrt{3}}{2}}{2}} = \frac{1}{2}\sqrt{2-\sqrt{3}} = \frac{\sqrt{3}-1}{2\sqrt{2}}.$$

$$cos\frac{\pi}{12} = \sqrt{\frac{1+cos\frac{\pi}{6}}{2}} = \sqrt{\frac{1+\frac{\sqrt{3}}{2}}{2}} = \frac{1}{2}\sqrt{2+\sqrt{3}} = \frac{\sqrt{3}+1}{2\sqrt{2}}.$$

Підставивши знайдені значення $\cos\frac{\pi}{12}$, $\sin\frac{\pi}{12}$ у записані вище рівності, матимемо:

$$y_0 = 2(1+\sqrt{3}),\ \ y_1 = -4,\ \ y_2 = 2(1-\sqrt{3}).$$

Відповідь: $y_0 = 2(1+\sqrt{3}),\ \ y_1 = -4,\ \ y_2 = 2(1-\sqrt{3})$.

Завдання для аудиторного заняття

№1. Розв'язати рівняння 3-го степеня:

а) $x^3 + 12x^2 + 42x + 44 = 0$;

б) $x^3 - 6x^2 + 18x - 13 = 0$;

в) $x^3 - 9x^2 + 15x - 7 = 0$;
г) $x^3 - 3x^2 + 12x + 16 = 0$;
д) $x^3 + 3x^2 - 12x - 18 = 0$;
е) $x^3 - 6x^2 + 32 = 0$;
є) $x^3 + 3x^2 - 6x - 36 = 0$;
ж) $x^3 - 15x^2 + 57x - 70 = 0$;
з) $x^3 - 12x^2 + 42x - 36 = 0$;
и) $x^3 - 9x^2 + 36x - 28 = 0$;
і) $x^3 - 3x^2 - 24x - 28 = 0$.

№2. Розв'язати рівняння 4-го степеня:
а)$x^4 - 3x^3 - 2x^2 + 2x + 12 = 0$;
б) $x^4 - 6x^3 + 18x^2 - 30x + 25 = 0$;
в) $x^4 - 8x^3 + 12x^2 - 8x + 156 = 0$;
г) $x^4 - 4x^3 - 20x^2 - 12x + 35 = 0$;
д) $x^4 - 2x^3 + 4x^2 + 6x + 27 = 0$;
е) $x^4 + 4x^3 - 19x^2 - 46x + 120 = 0$;
є) $x^4 - 6x^3 + 18x^2 - 22x + 9 = 0$;
ж) $x^4 + 4x^3 + 14x^2 + 20x + 24 = 0$;

№3. Розв'язати рівняння: $x^3 + 4\sqrt{2}x^2 + 2x + a = 0$, якщо один із його коренів більше від іншого на $\sqrt{2}$.

№4. Розв'язати рівняння: $4x^3 - 20x^2 + x + a = 0$, якщо його корені x_1, x_2 задовольняють умову $3x_1 + x_2 = -2$.

№5. Розв'язати рівняння: $x^3 + \left(4\sqrt{2} - 1\right)x^2 + (2 - \sqrt{2})^2 x - - 6 = 0$, якщо його корені x_1, x_2 задовольняють умову $5x_1 - 2x_2 = \sqrt{2}$.

№6. Розв'язати рівняння: $x^3 + 3\sqrt{3}x^2 + a = 0$, якщо два його корені співпадають.

№7. Розв'язати рівняння: $x^3 - 3\sqrt{3}x^2 + 7x - \sqrt{3} = 0$, якщо його корені утворюють арифметичну прогресію.

№8. Розв'язати рівняння: $x^3 - i\sqrt{3}x^2 + 12x + a = 0$, якщо два його корені комплексно спряжені.

Відповіді: ***№1.*** а) *x*= -2; -5+$\sqrt{3}$; -5-$\sqrt{3}$; б) *x*=1; $\frac{5+3i\sqrt{3}}{2}$; $\frac{5-3i\sqrt{3}}{2}$; в) *x*=1;7; г) *x*=-1; 2+2*i*$\sqrt{3}$; 2-2*i*$\sqrt{3}$; д) *x*=3; -3+$\sqrt{3}$; - 3- $\sqrt{3}$; е) *x*=-2,4; є) *x*=3; -3+*i*$\sqrt{3}$; - 3- *i*$\sqrt{3}$; ж) *x*=10; $\frac{5+i\sqrt{3}}{2}$; $\frac{5-i\sqrt{3}}{2}$; з) *x*=6; 3+$\sqrt{3}$; 3-$\sqrt{3}$; и) *x*=1; 4+2*i*$\sqrt{3}$; 4-2*i*$\sqrt{3}$; і) *x*=-2;7; ***№2.*** а) *x*=2; 3; -1+*i*; -1-*i*; г) *x*=1; 7; -2+*i*; -2-*i*; е) *x*=2; 3; -4; -5; є) *x*=1; 2+$\sqrt{5}$;2-$\sqrt{5}$.

Завдання для самостійного розв'язування

№1. Розв'язати рівняння 3-го степеня*:*

а) $x^3 - 9x^2 + 33x - 38 = 0$;
б) $x^3 - 6x^2 - 3x + 44 = 0$;
в) $x^3 + 12x^2 + 30x - 43 = 0$;
г) $x^3 + 6x^2 - 32 = 0$;
д) $x^3 - 9x^2 + 12x + 14 = 0$;
е) $x^3 - 6x^2 + 3x - 18 = 0$;
є) $x^3 - 12x^2 + 33x + 18 = 0$;
ж) $x^3 - 15x^2 + 48x - 44 = 0$;
з) $x^3 - 6x^2 + 6x + 8 = 0$;
и) $x^3 - 9x^2 + 24x - 20 = 0$;
і) $x^3 - 12x^2 + 57x - 74 = 0$.

№2. *Розв'язати рівняння 4-го степеня:*

а) $x^4 + 9x^3 - 19x^2 - 201x - 270 = 0$;
б) $x^4 + 2x^3 - 5x^2 - 16x + 78 = 0$;
в) $x^4 + x^3 - 7x^2 + 17x - 12 = 0$;
г) $x^4 + 8x^3 + 27x^2 + 42x + 36 = 0$;
д) $x^4 + 8x^3 + 7x^2 - 2x - 14 = 0$;
е) $x^4 - 11x^3 + 29x^2 + 11x - 30 = 0$;
є) $x^4 - 5x^3 + 11x^2 - 13x + 6 = 0$;
ж) $x^4 - x^3 + 5x^2 + x + 10 = 0$;
з) $x^4 + 4x^3 + 3x^2 - 2x - 6 = 0$;
и) $x^4 + 2x^3 + 2x^2 + 4x + 24 = 0$;
і) $x^4 + 4x^3 + 8x^2 + 29x + 42 = 0$;
к) $x^4 + 3x^2 + 2x + 3 = 0$;
л) $x^4 - 6x^3 + 6x^2 + 27x - 56 = 0$;

№3. Розв'язати рівняння: $x^3 - 12x^2 + 43x - 52 = 0$, якщо його корені утворюють арифметичну прогресію

№4. Розв'язати рівняння: $x^3 - 20x^2 + ax + b = 0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1 : x_2 : x_3 = 2 : 3 : 5$.

№5. Один із коренів многочлена $f(x) = x^3 - 7x + a$ дорівнює подвоєному другому. Знайти $f(x)$ і його корені.

№6. Розв'язати рівняння: $x^3 + (3i + 2)x^2 + 2(3i + 2)x + 8 = 0$, якщо його корені утворюють геометричну прогресію.

№7. Розв'язати рівняння: $x^3 - 17x^2 + ax + b = 0$, якщо його другий корінь на 1 більше за перший, а третій – вдвічі більший за перший.

№8. Знайти зведений многочлен 3-го степеня, корені якого x_1, x_2, x_3 задовольняють умови $\begin{cases} \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = 1, \\ \frac{1}{x_1 x_2} + \frac{1}{x_1 x_3} + \frac{1}{x_2 x_3} = \frac{11}{36}, \\ x_1 x_2 x_3 = 36. \end{cases}$

№9. Розв'язати рівняння: $x^3 + \left(1 - 3\sqrt{3}\right)x^2 - 3\sqrt{3}x + 6x + + 6 = 0$, якщо його корені x_1, x_2 задовольняють умову $6x_1 - x_2 = 4\sqrt{3}$.

№10. Розв'язати рівняння: $x^3 - 2\left(2 + \sqrt{3i}\right)x^2 + +4\sqrt{3}\left(2i - \sqrt{3}\right)x + 24\sqrt{3}i = 0$.

№11. Розв'язати рівняння: $x^3 + ax - 30 = 0$, якщо його корені x_1, x_2 задовольняють умову $x_1 x_2 = 6$.

№12. Розв'язати рівняння: $x^3 - 9ix^2 - 14x + a = 0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1 - 2x_2 = x_3$.

№13. Розв'язати рівняння: $x^3 - 8ix^2 - 19x + +a = 0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1 : x_2 : x_3 = 1 : 3 : 4$.

№14. Розв'язати рівняння: $x^3 - 31ix^2 - 155x + 125i = 0$, якщо його корені утворюють геометричну прогресію.

Відповіді: ***№1.*** а) *x*= 2; $\frac{7+3i\sqrt{3}}{2}$; $\frac{7-3i\sqrt{3}}{2}$; б) *x*=4; 1+2$\sqrt{3}$; 1-2$\sqrt{3}$; в) *x*=1; $-\frac{13-i\sqrt{3}}{2}$; $-\frac{13+i\sqrt{3}}{2}$ г) *x*=-4; 2; д) *x*=7; 1+$\sqrt{3}$; 1- $\sqrt{3}$; е) *x*=6; *i*$\sqrt{3}$; -*i*$\sqrt{3}$; є) *x*=6; 3+2$\sqrt{3}$; 3- 2$\sqrt{3}$; ж) *x*=2; 11; з) *x*=4; 1+$\sqrt{3}$; 1-$\sqrt{3}$; и) *x*=2; 5; і) *x*=2; 5+2*i*$\sqrt{3}$; 5-2*i*$\sqrt{3}$; ***№2.*** а) *x*=-2; -3; 5; -9; в) *x*=1; -4; 1+*i*$\sqrt{2}$; 1-*i*$\sqrt{2}$; д) *x*=1; -7; -1+*i*; -1-*i*; є) *x*=1; 2; 1+*i*$\sqrt{2}$; 1-*i*$\sqrt{2}$; з) *x*=1; -3; -1+ *i*; 1- *i*; і) *x*=-2; -3; $\frac{1+3i\sqrt{3}}{2}$; $\frac{1-3i\sqrt{3}}{2}$; л) *x*= $\frac{1+\sqrt{29}}{2}$; $\frac{1-\sqrt{29}}{2}$.

Тема одинадцята
АЛГЕБРАЇЧНІ РОЗШИРЕННЯ ЧИСЛОВИХ ПОЛІВ

Алгебраїчні числа і скінченні розширення числових полів

***Означення**. Число називається алгебраїчним, якщо воно є коренем деякого многочлена з раціональними коефіцієнтами.*

Очевидно, будь-яке раціональне число *r* алгебраїчне, бо його можна розглядати як корінь многочлена $f(x) = x - r$ з раціональними коефіцієнтами. Проте ірраціональні числа також можуть бути алгебраїчними. Наприклад, числа $\sqrt{2}, \sqrt[3]{5}$ алгебраїчні, бо вони є коренями многочленів x^2-2, x^3-5 (відповідно) над полем *Q.*

Проте не всі ірраціональні числа алгебраїчні. Існує безліч ірраціональних чисел, які не є коренями жодного многочлена над полем *Q*. Такі числа називаються *трансцендентними.* Прикладами трансцендентних чисел можуть бути числа $\pi, lg3, 2^{\sqrt{2}}$ та інші.

Поняття алгебраїчного числа можна узагальнити, увівши таке означення.

***Означення**. Число* α *називається алгебраїчним відносно числового поля* Δ*, якщо воно є коренем деякого многочлена над полем* Δ*. Число, яке не є алгебраїчним відносно поля* Δ*, називається трансцендентним відносно* Δ.

Очевидно, алгебраїчні в розумінні першого означення числа – це числа, алгебраїчні відносно поля *Q* раціональних чисел. Оскільки *Q* є підполем будь-якого поля Δ, то ці числа алгебраїчні відносно довільного поля. Зрозуміло також, що кожне число поля Δ є алгебраїчним відносно цього самого поля Δ.

Нехай α – корінь многочлена степеня *n* над полем Δ: $f(x) = x^n + ...+a_1x + a_0$.

Вважатимемо, що цей многочлен незвідний у полі Δ, бо в противному разі ми могли б розглядати той незвідний множник многочлена, який має α своїм коренем.

Якщо $g(x)$ – будь-який многочлен над полем Δ, коренем якого є α, то внаслідок незвідності $f(x)$ многочлен $g(x)$ ділиться на $f(x)$ (взаємно простими вони бути не можуть, бо мають спільний множник $(x-\alpha)$) і тому має степінь, не нижчий за n. Зокрема, якщо $g(x)$ – також незвідний многочлен, то він збігається з $f(x)$ з точністю до сталого множника. Отже, зведений многочлен $f(x)$ – єдиний незвідний многочлен над полем Δ, який має α своїм коренем, а його степінь n найнижчий серед степенів усіх многочленів з коренем α.

***Означення**. Зведений многочлен $f(x)$, незвідний у полі Δ, який має α своїм коренем, називається мінімальним многочленом числа α, а його степінь n – степенем алгебраїчного числа α відносно поля Δ.*

Якщо α – число першого степеня відносно Δ, то $\alpha \in \Delta$. При $n > 1$ з незвідності $f(x)$ випливає, що $\alpha \in \Delta$. Справді, якби $\alpha \in \Delta$, то подільність многочлена $f(x)$ на лінійний двочлен $(x - \alpha)$ означала б, що $f(x)$ звідний у полі Δ.

Просте алгебраїчне розширення поля

Нехай тепер дано довільну числову множину *M.* Очевидно, завжди знайдуться числові поля, які містять всі числа множини *M,* наприклад, поле всіх комплексних чисел.

Мінімальним полем $P\{M\}$, що містить дану числову множину M, називається поле, яке є перетином усіх числових полів, що містять множину M. Це означення спирається на відомий факт, що непорожній перетин довільної сукупності полів знову є полем.

Для будь-якої числової множини *M* мінімальне поле $P\{M\}$ завжди існує і є підполем довільного іншого поля, яке містить множину *M.*

Приклад. Нехай множина *M* складається лише з одного числа 1. Тоді кожне числове поле містить цю множину. Мінімальним полем, яке містить це число, є поле *Q* раціональних чисел. Справді, поле *Q* належить усім числовим полям. З другого боку, ніяке ірраціональне число не може належати всім числовим полям, бо воно не належить хоча б числовому полю *Q.* Зауважимо, що *Q* природно назвати просто *мінімальним числовим полем.*

Нехай Δ – деяке числове поле і α – число, яке не належить цьому полю. Розглянемо мінімальне поле $P\{\Delta, \alpha\}$, яке містить і поле Δ, і число α. Очевидно, $P\{\Delta, \alpha\}$ є розширенням поля Δ, причому мінімальним розширенням, яке містить число α.

Відомо, що мінімальне розширення поля Δ, яке містить, число $\alpha \in \Delta$, називають також *розширенням поля* Δ, *утвореним приєднанням числа* α, і позначають через Δ(α). Аналогічно можна розглядати розширення $\Delta(\alpha_1, \alpha_2, ..., \alpha_k)$, утворене приєднанням кількох чисел α_1 α_2, ..., α_k до поля Δ, тобто мінімальне поле $P\{\Delta, \alpha_1, ..., \alpha_k\}$, яке містить як Δ, так і числа α_1, α_2, ..., α_k. Розширення, утворене приєднанням одного числа, часто називають *простим*.

Відповідно до цієї термінології поле чисел виду $a + b\sqrt{2}$ (a, b – раціональні) можна назвати простим розширенням поля раціональних чисел, утвореним приєднанням числа $\sqrt{2}$.

***Означення**. Поле* Δ(α)*, утворене приєднанням до поля* Δ *числа* α*, алгебраїчного відносно поля* Δ*, називається простим алгебраїчним розширенням поля* Δ.

Будова простого алгебраїчного розширення характе ризується такою теоремою.

***Теорема**. Поле* Δ(α), *утворене з поля* Δ *приєднанням кореня* α*, незвідного у полі* Δ *многочлена n-го степеня* $f(x)=x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$*, складається з усіх чисел виду* $j = c_o + c_1\alpha + c_2\alpha^2 + ... + c_{n-1}\alpha^{n-1}$*, де* $c_0, c_1, ..., c_{n-1}$ *– довільні числа з поля* Δ.

Наслідок. *Якщо* α *– корінь многочлена другого степеня над полем* Δ, $f(x) = x^2 + px + q$*, причому* $\alpha \in \Delta$*, то просте алгебраїчне розширення* Δ(α) *поля* Δ*, утворене приєднанням числа* α*, складається з усіх чисел виду* $a + b\alpha$*, де* a, b *– довільні числа з поля* Δ.

Приклад. Поле $Q(\sqrt{2})$ утворюється приєднанням до поля Q кореня $\sqrt{2}$ незвідного у полі Q многочлена другого степеня $f(x)=x^2 - 2$. Елементи поля $Q(\sqrt{2})$ мають вигляд $a+b\sqrt{2}$, де a, b – раціональні числа.

Поле C комплексних чисел утворюється з поля R дійсних чисел приєднанням до нього кореня незвідного в R многочлена другого степеня $f(x)=x^2+1$. З попередньої

теореми випливає, що всі елементи $j \in C$, тобто всі комплексні числа, мають вигляд $j = a + bi$, де a, b – дійсні числа.

***Означення**. Якщо корінь* α *квадратного тричлена над полем* Δ *не належить полю* Δ, *то просте алгебраїчне розширення* Δ(α), *утворене з поля* Δ *приєднанням до нього числа* α, *називається квадратичним розширенням поля* Δ.

Розглянуте вище поле $Q(\sqrt{2})$ є квадратичним розширенням поля Q раціональних чисел, утворене приєднанням кореня многочлена $f(x) = x^2-2$.

Скінченні розширення полів

Числа j поля Δ(α) мають специфічну структуру. Вони являють собою суму виду $j = c_0 + c_1\alpha + c_2\alpha^2 + ... + c_{n-1}\alpha^{n-1}$, де кожний член є добутком елемента c_k поля Δ на елемент α^k ($k = 0, 1, ..., n-1$) поля Δ(α). Отже, можна сказати, що довільний елемент j поля Δ(α), де α є коренем незвідного в Δ многочлена степеня n, є лінійною комбінацією елементів $1, \alpha_1, \alpha_2, ..., \alpha_{n-1}$ з коефіцієнтами з поля Δ. Оскільки сума елементів Δ(α) і добуток їх на числа з поля Δ є знову елементи поля Δ(α), то Δ(α) можна розглядати як лінійний простір над полем Δ. Більше того, Δ(α) є алгеброю над полем Δ; проте тут для нас істотні лише властивості Δ(α) як лінійного простору.

Узагальнюючи це спостереження, розглянемо деяке поле Ω і його підполе Δ. Ω є лінійний простір над полем Δ. Елементами цього простору є числа з поля Ω, а операціями – додавання елементів поля Ω і множення їх на числа з поля Δ.

Нагадаємо тепер деякі прості властивості лінійно залежних і лінійно незалежних систем елементів:

1) *кожна частина лінійно незалежної системи елементів відносно поля* Δ *є також лінійно незалежною системою елементів відносно поля* Δ;
2) *будь-яка система елементів* $\alpha_1, \alpha_2, ..., \alpha_k, 0$ *поля* Ω, *яка включає число нуль, є лінійно залежною відносно поля* Δ;
3) *якщо система елементів* $\alpha_1, \alpha_2, ..., \alpha_k$ *поля* Ω *є лінійно залежною відносно поля* Δ, *то хоч один з елементів системи є лінійною комбінацією інших елементів з коефіцієнтами з поля* Δ;

4) *якщо хоч один з елементів системи* $\alpha_1, \alpha_2, , \alpha_3 ..., \alpha_k$ *поля* Ω *є лінійною комбінацією інших елементів цієї системи з коефіцієнтами з поля* Δ*, то система* $\alpha_1, \alpha_2, ..., \alpha_k$ *є лінійно залежною відносно поля* Δ*.*

Коли α – алгебраїчне число *n*-го степеня відносно поля Δ, то елементи розширення $\Delta(\alpha)$ є лінійними комбінаціями (з коефіцієнтами з поля Δ) елементів лінійно незалежної відносно Δ системи $1, \alpha, \alpha^2, ..., \alpha^{n-1}$.

У загальному випадку розглянемо деяке числове поле Δ і його розширення Ω; припустимо, що в полі Ω існує лінійно незалежна відносно Δ система елементів $\alpha_1, \alpha_2, ..., \alpha_n$ така, що кожний елемент $j \in \Omega$ подається у вигляді лінійної комбінації чисел $\alpha_1, \alpha_2, ..., \alpha_n$ з коефіцієнтами з поля Δ.

Систему $\alpha_1, \alpha_2, ..., \alpha_n$ можна назвати *базисом розширення* Ω відносно поля Δ, бо вона утворює базис лінійного простору Ω над полем Δ. Кількість елементів цього базису скінченна і дорівнює *n.*

Такі розширення поля мають назву *скінченних*. Дамо повне означення згаданих понять.

Означення*. Розширення* Ω *поля* Δ *називається скінченним, якщо в полі* Ω *існує така лінійно незалежна відносно поля* Δ *система елементів* $\alpha_1, \alpha_2, ..., \alpha_n$ *, що будь-який елемент* $j \in \Omega$ *є лінійною комбінацією цих елементів з коефіцієнтами з поля* Δ: $j=\lambda_1\alpha_1+...+\lambda_n\alpha_n$*. Система елементів* $\alpha_1, \alpha_2, ..., \alpha_n$ *називається базисом поля* Ω *відносно поля* Δ.

Базис скінченного розширення Ω можна вибрати не одним способом. Проте всі базиси поля Ω мають те саме число елементів *n.* Більш того: *довільна лінійно незалежна система з n елементів є базисом*.

Отже, число *n* є характеристикою скінченного розширення Ω поля Δ, незалежною від вибору базису. Число *n* називається *степенем розширення* Ω над полем Δ і позначається символом $(\Omega : \Delta)$. Зрозуміло, що $(\Omega:\Delta)$ є *розмірністю лінійного простору* Ω над полем Δ.

Розглянемо деякі властивості базисів.

Якщо n – степінь розширення Ω *над полем* Δ*, то будь-яка лінійно незалежна відносно* Δ *система* $\alpha_1, \alpha_2, ..., \alpha_m$ *елементів поля* Ω *не може містити більш як n чисел.*

Степінь n скінченного розширення Ω над полем Δ дорівнює максимальному числу l елементів поля Ω, які можуть утворювати лінійно незалежну систему.

Якщо l – максимальне число елементів розширення Ω поля Δ, що утворюють лінійно незалежну систему відносно поля Δ, то Ω є скінченним розширенням над полем Δ степеня l.

Зауважимо, що не кожне розширення поля є скінченним. Так, поле *R* дійсних чисел є розширенням поля *Q* раціональних чисел. Проте це розширення не є скінченним, бо в ньому не існує скінченного базису, через який лінійно виражалося б будь-яке дійсне число. Розширення Ω першого степеня над полем Δ просто збігається з полем Δ.

Теорема. *Нехай Ω – розширення поля Δ, $j \in \Omega$ – алгебраїчний елемент над полем Δ. Нехай $f(x)$ – незвідний многочлен з коефіцієнтами з поля Δ степеня n, коренем якого є j. Тоді $\Delta(j) \cong \Delta[x]/f(x)\Delta[x]$ причому $(\Delta(j):\Delta)=n$ і кожний елемент и поля Δ однозначно представляється у вигляді: $u=a_0*1+a_1j+\ldots+a_{n-1}j^{n-1}$ ($a_0,\ldots,a_{n-1} \in \Delta$).*

Поняття алгебраїчного розширення

Розширення Ω поля Δ, утворене за допомогою кількох послідовно виконаних простих алгебраїчних розширень, називається *складним алгебраїчним розширенням поля* Δ.

Означення*. Ω є складним алгебраїчним розширенням поля Δ, якщо існує такий ланцюжок розширень*

$$\Delta \subseteq \Delta_1 \subseteq \cdots \subseteq \Delta_k = \Omega$$

що $\Delta_1 = \Delta(\alpha_1)$, $\Delta_2 = \Delta_1(\alpha_2)$, ..., $\Delta_k = \Delta_{k-1}(\alpha_k)$, *причому кожне* α_i *є алгебраїчним числом над полем* Δ_{i-1} (при $i=1$ $\Delta_{i-1} = \Delta$).

Це означення не вимагає, щоб всі числа α_i, були алгебраїчними відносно початкового поля Δ, бо алгебраїчність числа α_i відносно поля Δ_{i-1} безпосередньо ще не означає його алгебраїчності відносно його підполя Δ.

Складне алгебраїчне розширення поля Δ позначатимемо символом $\Delta(\alpha_1)(\alpha_2)\ldots(\alpha_k)$. Це позначення не слід змішувати з символом $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_k)$, який означає розширення поля Δ, утворене одночасним приєднанням до нього чисел α_i.

Природно розглядати складне алгебраїчне розширення як узагальнення простого, тобто вважати просте розширення $\Delta(\alpha_1)$ також складним з $k = 1$, або, що те саме, при $\alpha_2 \in \Delta(\alpha_1)$, $\alpha_3 \in \Delta(\alpha_1)$,...,$\alpha_k \in \Delta(\alpha_1)$.

Крім поняття *простого* чи *складного алгебраїчного розширення* введемо ще поняття *алгебраїчного розширення числового поля.*

***Означення**. Розширення* Ω *поля* Δ *називається алгебраїчним, якщо всі його елементи є алгебраїчними відносно поля* Δ.

Усі раніше введені типи розширень (просте і складне алгебраїчне, скінченне) належать до категорії алгебраїчних розширень. Звичайно, не кожне розширення поля є алгебраїчним: так, можна показати, що поле дійсних чисел R не є алгебраїчним розширенням поля Q раціональних чисел. Розширення, які не є алгебраїчними, називають *трансцендентними*.

Скінченність простих і складних алгебраїчних розширень

Теорема. *Просте алгебраїчне розширення* $\Delta(\alpha)$, *утворене з* Δ *приєднанням алгебраїчного відносно* Δ *числа* α, *є скінченним розширенням поля* Δ. *Степінь розширення* $\Delta(\alpha)$ *над полем* Δ *дорівнює степеню числа* α *відносно* Δ.

Наслідок. *Степінь будь-якого квадратичного розширення числового поля дорівнює* 2.

***Лема* 1**. *Якщо* Δ_2 *– скінченне розширення поля* Δ_1, *а* Δ_1 *– скінченне розширення поля* Δ, *то* Δ_2 *– скінченне розширення поля* Δ, *причому* $(\Delta_2 : \Delta) = (\Delta_2 : \Delta_1)(\Delta_1 : \Delta)$.

Лема 2. *Якщо* Δ_2 *– скінченне розширення поля* Δ *степеня* m, *а* Δ_1 *– довільне розширення поля* Δ, *що міститься в* Δ_2: $\Delta \subseteq \Delta_1 \subseteq \Delta_2$, *то* Δ_1 *– також скінченне розширення* Δ, *причому його степінь* $(\Delta_1:\Delta)$ *є дільником числа* m.

З теореми і леми 1 тепер безпосередньо випливає така теорема:

Теорема. *Складне алгебраїчне розширення* $\Delta(\alpha_1)(\alpha_2)$ *є скінченним розширенням поля* Δ. *Степінь цього розширення дорівнює добутку степеня розширення* $\Delta(\alpha_1)$ *відносно поля* Δ *на степінь розширення* $\Delta(\alpha_1)(\alpha_2)$ *відносно поля* $\Delta(\alpha_1)$.

Наслідок 1. *Складне алгебраїчне розширення* $\Delta(\alpha_1)(\alpha_2)...(\alpha_k)$ *є скінченним розширенням поля* Δ*. Степінь цього розширення дорівнює добутку степенів усіх послідовних простих розширень.*

Оскільки у випадку ланцюжка квадратичних розширень степінь кожного послідовного простого розширення дорівнює 2, приходимо до такого наслідку.

Наслідок 2. *Якщо* $\Delta \subseteq \Delta_1 \subseteq ... \subseteq \Delta_k$ *є ланцюжком квадратичних розширень, то* Δ_k *є скінченним розширенням поля* Δ *степеня* 2^k*.*

Алгебраїчність і простота скінченних розширень

Ми показали, що як прості, так і складні алгебраїчні розширення поля є завжди скінченними розширеннями. Для доведення того, що всі згадані розширення *алгебраїчні,* досить встановити алгебраїчність довільного скінченного розширення поля.

Теорема. *Будь-яке скінченне розширення поля є його алгебраїчним розширенням.*

Кожний елемент γ *з квадратичного розширення поля* Δ *є коренем деякого многочлена над полем* Δ*, степінь якого не перевищує* 2. *Якщо* $\gamma \notin \Delta$*, то напевно* γ *є коренем незвідного квадратного тричлена над полем* Δ.

Теореми дають змогу прийти до такого висновку:

Кожне просте або складне алгебраїчне розширення числового поля Δ *є алгебраїчним розширенням цього поля.*

Справедливим є твердження, що *скінченне розширення поля* Δ *є не тільки алгебраїчним, але й простим алгебраїчним розширенням* Δ.

Теорема. *Розширення* $\Delta(\alpha_1, \alpha_2,..., \alpha_k)$*, утворене з* Δ *приєднанням алгебраїчних відносно* Δ *чисел* $\alpha_1, \alpha_2, ..., \alpha_k$*, збігається зі складним алгебраїчним розширенням* $\Delta(\alpha_1)(\alpha_2)...(\alpha_k)$.

Розширення $\Delta(\alpha_1, \alpha_2,..., \alpha_k)$, іноді називають *алгебраїчно породженим*. Таким чином, клас алгебраїчно породжених розширень збігається з класом складних алгебраїчних розширень.

***Теорема**. Будь-яке скінченне розширення поля Δ є складним алгебраїчним розширенням цього поля.*

***Теорема.** Будь-яке складне алгебраїчне розширення* $\Omega=\Delta(\alpha_1)(\alpha_2)\ \dots\ (\alpha_k)$ *поля Δ є простим розширенням цього поля, тобто існує таке число w, алгебраїчне відносно Δ,* що $\Omega = \Delta\ (w)$.

Наслідок. *Будь-яке розширення другого степеня поля Δ є квадратичним розширенням поля Δ.*

Отже, було розглянуто такі п'ять класів розширень числового поля Δ:

K_1: прості алгебраїчні розширення;

K_2: складні алгебраїчні розширення;

K_3: скінченні розширення;

K_4: алгебраїчно породжені розширення;

K_5: алгебраїчні розширення.

Встановлені щодо цих класів факти можна символічно подати так:

Теорема:

$$K_1 \subseteq K_3;\ K_2 \subseteq K_3;\ K_3 \subseteq K_5;\ K_2 = K_4; K_3 \subseteq K_2;\ K_2 \subseteq K_1.$$

Поняття *простого* і *складного алгебраїчних розширень, алгебраїчно породженого розширення* і *скінченного розширення* по суті збігаються. Різні за способом побудови, всі вони являють собою ту саму алгебраїчну структуру.

Поле алгебраїчних чисел

Розглянемо сукупність $A(\Delta)$ усіх алгебраїчних чисел відносно поля Δ, тобто множину коренів усіх многочленів з $\Delta[x]$.

***Теорема**. Сукупність $A(\Delta)$ алгебраїчних чисел відносно поля Δ є поле.*

Наслідок. *Множина A усіх алгебраїчних чисел* (тобто $A = A\ (Q)$) *є поле.*

З $A(\Delta)$ є алгебраїчне розширення поля Δ. Покажемо тепер, що *в загальному випадку це розширення не є скінченним.* Для цього досить перевірити, що поле A не є скінченним розширенням поля Q раціональних чисел. Але це насправді так, бо у кільці $Q[x]$ існують незвідні многочлени як завгодно великого степеня. Отже, в A існують числа як завгодно великого степеня відносно поля Q. Але тоді A не може бути скінченним розширенням

поля Q, бо степінь скінченного розширення поля Δ не нижчий від степеня кожного елемента цього розширення відносно Δ.

З наведених міркувань випливає, що *існують алгебраїчні розширення полів, які не є скінченними,* тобто $К_5 \supset К_0$, але $K_5 \neq K_0$, як і було зазначено у попередньому пункті. Цей факт не означає, що будь-яке розширення A (Δ) є нескінченним. Так, поле C комплексних чисел є скінченним розширенням поля R дійсних чисел. В той же час $C=A(R)$, бо корені усіх многочленів з дійсними коефіцієнтами належать C, і будь-яке комплексне число $a+bi$ є коренем многочлена над R (наприклад, многочлена $f(x) = x^2 - 2ax + (a^2+b^2)$).

Як відомо, поле C алгебраїчно замкнуте, тобто всі алгебраїчні числа над цим полем належать самому полю С: $A(C)=C$. Виявляється, що цю властивість має сукупність A(Δ) алгебраїчних чисел над довільним числовим полем A: $A[A(\Delta)] = A(\Delta)$.

***Теорема**. Поле алгебраїчних чисел A(Δ) над довільним числовим полем Δ алгебраїчно замкнуте.*

Основна теорема теорії многочленів стверджує алгебраїчну замкненість поля C усіх комплексних чисел. Поле $A = A(Q)$ алгебраїчних чисел є підполем поля C: $A \in C$ (причому правильним підполем, бо в C існують трансцендентні числа). З теореми випливає, що і підполе A поля C має властивість алгебраїчної замкненості.

Приклади розв'язування типових завдань

***№1.** Показати, що $\frac{-1+i\sqrt{3}}{2}$ є алгебраїчним числом.*

Розв'язання. Достатньо показати, що число $\frac{-1+i\sqrt{3}}{2}$ є коренем деякого ненульового многочлена $f(x)$ з коефіцієнтами з поля Q раціональних чисел. Розглянемо многочлен $f(x)=(x-f(x)) = (x-\alpha)(x-\overline{\alpha})$:

$$f(x) = \left(x - \frac{-1+i\sqrt{3}}{2}\right)\left(x - \frac{-1-i\sqrt{3}}{2}\right) = x^2 + x + 1.$$

Отже, $\frac{-1+i\sqrt{3}}{2}$ є алгебраїчним числом.

№2. *Нехай F – розширення поля Z_p і $(F:Z_p)=n$. Показати, що поле F складається із p^n елементів.*

Розв'язання. Із умови $(F:Z_p)=n$ випливає, що в полі F існують n елементів $u_1, u_2, \ldots, u_n$, які утворюють базис лінійного простору F над полем Z_p. Отже, довільний елемент u поля F однозначно представляється у вигляді: $u = \propto_1 u_1 + \cdots + \propto_n u_n, \propto_1 \ldots \propto_n \epsilon Z_p$.

Враховуючи, що поле Z_p складається з p елементів, одержимо, що в полі F є точно p^n елементів.

№3. *Знайти степінь поля $Q(\varepsilon)$ над полем, де ε – первісний корінь третього степеня з одиниці.*

Розв'язання. ε – первісний корінь третього степеня з одиниці, отже, він є коренем многочлена третього степеня: $x^3-1=(x-1)(x^2+x+1)$. Тоді ε – корінь незвідного над полем Q многочлена $f(x) = x^2+x+1$. Тоді за теоремою $Q(\varepsilon) \cong \frac{Q[x]}{f(x)Q[x]}$, а отже, $(Q(\varepsilon): Q) = 2$. Тому довільний елемент $u \in Q(\varepsilon)$ має вигляд $u=\alpha+\beta\varepsilon, \alpha, \beta \epsilon Q$.

№4. *Довести, що число $\sqrt[5]{2} + \sqrt[7]{3}$ є цілим алгебраїчним числом.*

Розв'язання. Оскільки $\sqrt[5]{2}$ є коренем многочлена $x^5 - 2$, а $\sqrt[7]{3}$ є коренем многочлена $x^7 - 3$, тому числа $\sqrt[5]{2}$ і $\sqrt[7]{3}$ є цілими алгебраїчними числами. Оскільки сума цілих алгебраїчних чисел є ціле алгебраїчне число, то $\sqrt[5]{2} + \sqrt[7]{3}$ є цілим алгебраїчним числом.

№5. *Показати, що $u = \frac{-1+\sqrt{d}}{2}$ є цілим алгебраїчним числом, якщо $d \in Z$, $d \equiv 1 (mod\ 4)$.*

Розв'язання. Нехай $u' = \frac{-1-\sqrt{d}}{2}$. Тоді $u+u' = -1$, $uu'=(1-d)/4$. За умовою $d \equiv 1 (mod\ 4)$, отже $uu' \in Z$. Отже, u – є коренем многочлена

$$(x-u)(x-u') = x^2 + x + \frac{1-d}{4} \in Z[x].$$

Таким чином, u – ціле алгебраїчне число.

№6. *Показати, що у полі $Q(\sqrt{2})$ числа $\alpha_1=1$, $\alpha_2=\sqrt{2}$ є лінійно незалежною системою елементів відносно поля Q.*

Розв'язання. Нехай λ_1, $\lambda_2 \in Q$. Тоді $\lambda_1 \cdot 1 + \lambda_2 \cdot \sqrt{2} = 0$. Покажемо, що ця рівність можлива лише при $\lambda_1 = \lambda_2 = 0$. Припустимо супротивне. Тоді маємо: $\sqrt{2} = -\frac{\lambda_1}{\lambda_2}$, тобто $\sqrt{2}$ – раціональне число, що неможливо. Отже, числа $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$ є лінійно незалежною системою елементів відносно поля Q.

№7. *Показати, що поле $Q(\sqrt{2})$ чисел $a+b\sqrt{2}$, де a, b довільні раціональні числа, є розширенням поля Q степеня 2.*

Розв'язання. Необхідно показати, що існує базис поля $Q(\sqrt{2})$ відносно поля Q, який складається з двох елементів. Як показано у №6, за базис можна взяти лінійно незалежні відносно Q елементи 1 і $\sqrt{2}$. За базис можна взяти й інші числа, наприклад, $1-\sqrt{2}$, $1+\sqrt{2}$.

Завдання для аудиторного заняття

№1. Чи є алгебраїчними числа:

а) $1-i$; б) $2 + \sqrt[3]{3}$.

№2. Чи буде поле $Q(\sqrt{2})$ алгебраїчно замкнутим?

№3. Знайти степінь поля Q над полем $Q(\sqrt{2})$.

№4. Перевірити, чи будуть цілими алгебраїчними числами:

а) $2\sqrt[5]{7}$; б) $\frac{7}{\sqrt{2}-\sqrt{3}}$.

№5. Довести, що наступні числа є алгебраїчними над полем Q:

а) $\sqrt{2}$; б) $\sqrt[3]{1-\sqrt{2}}$; в) $-1 + i\sqrt{5}$.

№6. Звільнитися від ірраціональності в знаменнику дробу:

а) $\frac{1}{\sqrt[3]{4}-\sqrt[3]{2}+3}$; б) $\frac{7-4\sqrt[3]{49}}{2\sqrt[3]{49}+7\sqrt[3]{7}-21}$;

в) $\frac{\sqrt[4]{2}}{\sqrt[4]{8}+\sqrt[4]{2}-2}$; г) $\frac{1}{\sqrt{2}+\sqrt{3}+1}$;

д) $\frac{1}{1+\sqrt[3]{2}+3\sqrt[3]{4}}$; е) $\frac{1}{\sqrt[3]{6}-\sqrt[3]{5}}$;

є) $\frac{1}{\sqrt[9]{5}+\sqrt[9]{3}}$; ж) $\frac{1}{\sqrt{a}+\sqrt{b}+\sqrt{c}}$;

з) $\frac{1}{\sqrt[3]{2}+\sqrt[3]{3}+\sqrt[3]{5}}$; і) $\frac{1}{\sqrt[3]{a}+\sqrt[3]{b}+\sqrt[3]{c}}$. .

№7. Довести, що число α є алгебраїчним і знайти його мінімальний многочлен, якщо:

а) $\alpha = \sqrt{2+\sqrt{3}}$; б) $\alpha = 1 + \sqrt{3-\sqrt{5}}$;

в) $\alpha = \sqrt{13} - \sqrt{15}$; г) $\alpha = \sqrt{5} - \sqrt[3]{3}$.

№8. Описати розширення поля Q:

а) $Q\left(\sqrt[3]{2}\right)$; б) $Q\left(\sqrt[4]{2}\right)$; в) $Q\left(\sqrt{\sqrt[3]{3}-1}\right)$.

Відповіді: ***№6*** г) $\frac{2\sqrt{3}-\sqrt{2}-\sqrt{6}+4}{2}$; є) $\frac{\left(\sqrt[9]{25}-\sqrt[9]{15}+\sqrt[9]{9}\right)\left(\sqrt[3]{25}-\sqrt[3]{15}+\sqrt[3]{9}\right)}{8}$.

№8. а) базисом цього поля відносно Q є, наприклад, числа 1, $\sqrt[3]{2}$, $\sqrt[3]{2^2}$.

Завдання для самостійного розв'язування

№1. Чи є алгебраїчними числа:

а)$1+i$; б) $\frac{-1+\sqrt{-15}}{2}$.

№2. Перевірити, чи будуть цілими алгебраїчними числами:

а) $\sqrt{3}\sqrt[3]{4}$; б) $\frac{\sqrt{7}}{2-\sqrt{5}}$.

№3. Довести, що наступні числа є алгебраїчними над полем Q:

а) $\sqrt[3]{2}$; б) $1-i\sqrt{3}$; в) $\sqrt[3]{-1-i\sqrt{2}}$.

№4. Звільнитися від ірраціональності в знаменнику дробу:

а) $\frac{4}{2\sqrt[3]{25}-\sqrt[3]{5}+3}$; б) $\frac{7}{1-\sqrt[4]{2}+\sqrt{2}}$;

в) $\frac{1}{1+\sqrt{2}-\sqrt[3]{2}}$; г) $\frac{1}{\sqrt{5}-2\sqrt{3}-1}$;

д) $\frac{\sqrt[3]{2}}{\sqrt[3]{4}+2\sqrt[3]{2}}$; е) $\frac{2}{\sqrt[3]{49}-\sqrt[3]{7}+3}$;

є) $\frac{1}{\sqrt[5]{3}-\sqrt[5]{2}}$; ж) $\frac{1}{\sqrt[8]{3}+\sqrt[8]{2}}$;

з) $\frac{1}{\sqrt[4]{27}-2\sqrt[4]{9}+\sqrt[4]{3}-1}$; і) $\frac{1}{\sqrt[4]{a}+\sqrt[4]{b}+\sqrt[4]{c}}$.

№5. Довести, що число α є алгебраїчним і знайти його мінімальний многочлен, якщо:

а) $\alpha=\sqrt[3]{2+\sqrt{7}}$;

б) $\alpha=1+\sqrt{\sqrt[3]{6}+1}$;

в) $\alpha=i\sqrt{3}+1$.

№6. Нехай $F=Q(\sqrt{\sqrt[3]{5}-2}\,)$. Довести, що:

а) $\sqrt[3]{5}\in F$; б) $(\sqrt[3]{5}+2\,)\in F$;

в) $\left(\sqrt[3]{5}+\sqrt{\sqrt[3]{5}-2}\right)\in F$.

Тема дванадцята
КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД КІЛЬКОХ ЗМІННИХ

Побудова кільця многочленів

Розглянемо спочатку окремий випадок, а саме – сукупність многочленів від 2-х змінних.

Нехай R – якась область цілісності з одиницею, а $R[x]$ – сукупність усіх многочленів від однієї змінної x над R. Як відомо, $R[x]$ є також областю цілісності з одиницею. Отже, ми можемо побудувати кільце многочленів над $R[x]$ від однієї змінної (позначимо цю змінну через y), тобто сукупність усіх многочленів виду

$$a_n(x)y^n + a_{n-1}(x)y^{n-1} + \ldots + a_1(x)y + a_0(x), \qquad (12.1)$$

коефіцієнти яких $a_n(x), \ldots, a_1(x), a_0(x)$ є елементи області цілісності $R[x]$ (многочлени від змінної x над кільцем R). Природно позначити сукупність многочленів виду (9.1) через $R[x][y]$ – *кільце* (*область цілісності*). Надалі для цього кільця вживатимемо позначення $R[x, y]$ або $R[y, x]$, елементи якого називатимемо *многочленами від 2-х змінних x і y над R* – позначатимемо $f(x, y)$, $g(x, y)$ тощо.

***Означення**. Кільцем многочленів $R[x_1, x_2, \ldots, x_{n-1}, x_n]$ від n змінних x_i над областю цілісності R називається кільце многочленів від змінної x_n над кільцем $R[x_1, x_2, \ldots, x_{n-1}]$, тобто*

$$R[x_1, x_2, \ldots, x_{n-1}, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n].$$

***Теорема**. Кільце многочленів $R[x_1, x_2, \ldots, x_{n-1}, x_n]$ над областю цілісності R є область цілісності.*

***Теорема**. Кожний елемент $f \in R[x_1, x_2, \ldots, x_{n-1}, x_n]$ можна подати у вигляді скінченної суми*

$$f = \sum_{i=1}^{N} A_i x_1^{k_{1i}} x_2^{k_{2i}} \ldots x_n^{k_{ni}}, A_i \in R, k_{ji} \in Z_+, i = 1, 2, \ldots N, j = 1, 2, \ldots, n \qquad (12.2)$$

Навпаки, будь-який вираз виду (9.2) *є елементом кільця* $R[x_1, x_2, \ldots, x_n]$.

***Означення**. Кожний елемент кільця $R[x_1, x_2, \ldots, x_{n-1}, x_n]$ називають многочленом від n змінних $x_1, x_2, \ldots, x_n$ над R і*

позначають $f(x_1, \ldots, x_n)$, $g(x_1, \ldots x_n)$ *і т. д.*

Кожний доданок $A_i x_1^{k_{1i}} \ldots x_n^{k_{ni}}$ цієї суми називають *членом* многочлена $f(x_1, \ldots, x_n)$, відповідний елемент $A_i \in R$ – *коефіцієнтом* члена (і многочлена). Два члени, які відрізняються лише коефіцієнтами, називають *подібними*; іншими словами, члени подібні, якщо усі змінні входять множниками в ці члени у попарно рівних степенях.

Виконання над многочленами з кільця $R[x_1, x_2, \ldots, x_{n-1}, x_n]$ дій додавання і множення зводиться внаслідок дистрибутивного закону, що діє в кільці, до дій над членами цих многочленів. Під час додавання двох (або більшої кількості) подібних членів отримуємо один член, подібний до кожного з даних. Множення членів многочлена здійснюють за правилом

$$(Ax_1^{k_1} \ldots x_n^{k_n})(Bx_1^{l_1} \ldots x_n^{l_n}) = ABx_1^{k_1+l_1} \ldots x_n^{k_n+l_n}.$$

Результати дій додавання і множення не залежать від порядку запису змінних.

Різні форми зображення многочленів

Записуючи многочлен $f(x_1, x_2, \ldots, x_n)$ у формі (12.2), ми завжди вважатимемо, що серед членів многочлена немає подібних (тобто здійснено попереднє зведення подібних членів). Таку форму многочлена називають *канонічною* або *нормальною*. Канонічна форма має ту позитивну особливість, що вона *єдина* (з точністю до порядку членів). Цю єдиність слід розуміти так, що коли два многочлени $f(x_1, x_2, \ldots, x_n)$ і $g(x_1, x_2, \ldots, x_n)$ подані у канонічній формі, рівні між собою, то кожний член многочлена $f(x_1, x_2, \ldots, x_n)$ є також членом многочлена $g(x_1, \ldots, x_n)$ і навпаки.

***Теорема**. Будь-який многочлен $f(x_1, x_2, \ldots, x_n) \in R[x_1, \ldots, x_n]$ можна подати в канонічній формі лише одним способом* (з точністю до порядку членів).

Нуль-многочлен кільця $R[x_1, \ldots, x_n]$ позначатимемо просто 0.

***Означення**. Степенем члена $Ax_1^{k_1} \ldots x_n^{k_n}$ многочлена називається сума $k_1+\ldots+k_n$. Число k_i ($i = 1, 2, \ldots, n$) називають степенем даного члена відносно x_i. Найбільший із степенів*

членів називається степенем многочлена, а член з найбільшим степенем називається старшим членом многочлена.

Многочлени нульового степеня є відмінні від 0 елементи кільця $R[x_1, ..., x_n]$. Їх разом з елементами 0 називатимемо *константами*. Степінь многочлена $f(x_1, ..., x_n)$ позначатимемо *deg f* як і у випадку многочленів від однієї змінної.

Якщо всі члени многочлена мають той самий степінь l, то многочлен називається *однорідним многочленом* або формою степеня l. Очевидно, що *будь-який многочлен можна подати як суму скінченної кількості однорідних многочленів різних степенів.*

***Теорема**. Якщо $f(x_1,...,x_n)$ і $g(x_1,...,x_n)$ – відмінні від нуля многочлени з $R[x_1, ..., x_n]$, де R – область цілісності, то $deg\,(fg) = deg\,f + deg\,g$.*

Наслідок. *У кільці R $[x_1,..., x_n]$ дільниками одиниці можуть бути лише відмінні від нуля константи.*

Для многочленів від багатьох змінних поняття степеня члена вже недостатнє для встановлення єдиного порядку розміщення членів, як це було для многочленів від однієї змінної. Найбільш поширений в алгебрі є так званий *лексикографічний* принцип упорядкування членів многочлена – за словником. У випадку членів многочлена роль першої, другої і т. д. букв виконують відповідно $x_1, x_2, ...$, алфавітному ж принципу впорядкування i-ї букви відповідає упорядкування за степенями змінної x_i.

Розглянемо будь-які два члени многочлена $T_1 = Ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n}$, $T_2 = Bx_1^{l_1}x_2^{l_2} \dots x_n^{l_n}$. Якщо ці члени не подібні, то не всі відповідні степені k_i і l_i рівні між собою, тобто існує принаймні одне таке натуральне число p $(1 \le p \le n)$, що $k_i = l_i$ при $i = 1, 2, ..., p\text{-}1$, але $k_p \ne l_p$ Якщо $k_p > l_p$, то член (T_1) називається *вищим*, ніж член (T_2). Якщо ж $k_p < l_p$, то член (T_1) називається *нижчим*, ніж член (T_2).

Як бачимо, з будь-яких двох неподібних членів многочлена один вищий, ніж другий. Очевидно, далі, що коли член T_1 вищий за член T_2, а член T_2 вищий за член T_3, то T_1 вищий за T_3. Звідси зрозуміло, що завжди можна так розмістити члени в канонічній формі многочлена, щоб вищі члени передували нижчим. Таке розміщення і

називається *лексикографічним*.

Наприклад, під час лексикографічного розміщення многочлен можна записати так:

$$f(x_1, x_2, x_3) = x_1^4 x_2 x_3 - 2x_1^3 - x_1^2 x_2^3 + 2x_1^2 x_2 x_3 + \\ + x_1^2 x_2 x_3 + 2x_1 x_2^3 x_3^2 + x_1 x_{3.}^2$$

Називатимемо перший по порядку член многочлена у лексикографічному розміщенні *вищим членом* многочлена.

Лема*. Вищий член добутку двох многочленів дорівнює добутку вищих членів цих многочленів.*

Крім лексикографічного розміщення членів многочлена досить часто доводиться користуватися розміщенням членів за степенями однієї змінної, тобто зображенням типу (9.2). У цьому випадку многочлен $f(x_1,\dots\ x_n)$ над кільцем R можна записати у вигляді:

$$f(x_1, x_2, \dots, x_n) = A_s\left(x_1, x_2, \dots, x_{p-1}, x_{p+1}, \dots x_n\right)x_p^n + \\ + A_{s-1}\left(x_1, x_2, \dots, x_{p-1}, x_{p+1}, \dots x_n\right)x_p^{n-1} + \dots + \\ + A_0\left(x_1, x_2, \dots, x_{p-1}, x_{p+1}, \dots x_n\right),$$

де коефіцієнти $A_i\left(x_1, x_2, \dots, x_{p-1}, x_{p+1}, \dots x_n\right)$, $i = 0,\ 1,\ \dots,\ s$ є многочленами від n - 1 змінних $x_1, x_2, \dots, x_{p-1}, x_{p+1} \dots x_n$ над кільцем R.

Функціональне тлумачення многочленів

Як і у випадку многочленів та раціональних дробів від однієї змінної, природно поставити питання про можливість тлумачити многочлени $f(x_1,\dots\ x_n)$ як функції від n змінних і про зв'язок між алгебраїчним і функціональним підходами.

Кожному многочлену $f(x_1,\dots\ x_n) \in R[x_1,\dots x_n]$ поставимо у відповідність функцію

$$\varphi_f\colon R^n \to R. \qquad (12.3)$$

значення якої визначаються умовою: для будь-яких

$$\alpha_1, \alpha_2, \dots, \alpha_n \in R\ \ \varphi_f\colon (\alpha_1, \alpha_2, \dots, \alpha_n) = f(\alpha_1, \alpha_2, \dots, \alpha_n), \qquad (12.4)$$

де $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ – елемент кільця R, який отримуємо, підставивши у вираз для многочлена $f(x_1,\dots\ x_n)$ замість x_i

елемент $\alpha_i \in R$ і виконавши відповідні дії множення і додавання (в розумінні операцій, заданих в R).

Теорема. *Якщо R – область цілісності характеристики* 0, *то кільце* $R[x_1 \ldots x_n]$ *ізоморфне сукупності усіх функцій* φ_f, *визначених умовами* (12.3) – (12.4).

З теореми випливає, що для випадку областей цілісності R з одиницею, характеристика яких дорівнює 0 (зокрема, для всіх числових полів), алгебраїчне і функціональне тлумачення многочленів з $R[x_1, x_2, \ldots, x_n]$ цілком рівноправні. Це і є обґрунтування використання алгебраїчних властивостей многочленів від кількох змінних в аналізі і теорії функцій.

Подільність у кільці многочленів від кількох змінних

Досі ми розглядали переважно такі властивості многочленів від багатьох змінних, які повторюють (з природним узагальненням) відповідні властивості многочленів від однієї змінної. Розглянемо питання, в яких проявляється специфіка многочленів від кількох змінних.

Звичайно, означення подільності, дільника, загальні властивості відношення подільності, поняття і властивості незвідних многочленів переноситься на кільце многочленів від n змінних без усяких змін, оскільки вони властиві будь-якій області цілісності, зокрема й $R[x_1, x_2, \ldots, x_n]$. Вважатимемо, що основна область цілісності R є поле, яке позначатимемо P.

Означення. *Вважатимемо, що многочлен $f \in P_n$ ділиться на многочлен $g \in P_n$, відмінний від нуля, і записуватимемо $f \vdots g$, якщо існує такий многочлен $s \in P$, що $f = g \cdot s$. При цьому g називають дільником многочлена f.*

Відношення подільності многочленів в P_n має такі ж властивості, що й многочлени від однієї змінної.

Дільниками 1 в P_n можуть бути лише відмінні від нуля константи.

Асоційованими многочленами в кільці P_n є такі і тільки такі многочлени, які відрізняються множником, що є відмінною від нуля константою.

***Означення**. Многочлен $p \in P_n$ називається незвідним у полі P, якщо deg p≥1, для будь-яких u, v $\in P_n$, p=uv→deg u=0 або deg v=0.*

Многочлен $q \in P_n$ називається звідним у полі P, якщо

$$deg\ q \geq 1\ i\ \exists(u, v \in P_n):$$
$$[q = uv \wedge deg\ u \geq 1\ i\ \ deg\ v \geq 1].$$

Найпростішими *властивостями* незвідних многочленів є такі:

1. *Якщо p незвідний у P, то і будь-який асоційований з ним многочлен cp незвідний у P.*
2. *Якщо p, q незвідні у P многочлени і p/q, то p і q – асоційовані.*
3. *Будь-який многочлен $p \in P_n$ першого степеня незвідний у P.*

На цьому по суті закінчується аналогія теорії подільності в кільцях $P[x]$ і $P[x_1 \ldots x_n]$ *при* $n \geq 2$. Специфіка останнього полягає в тому, що $P[x_1, x_2, \ldots, x_n]$ і для $n \geq 2$ *не є кільцем головних ідеалів* і (тим більше) *евклідовим кільцем.* Тому безпосереднє перенесення на це кільце результатів попередніх тем неможливе.

Це означає, що алгоритм Евкліда і його численні наслідки не поширюються на випадок многочленів від кількох змінних. Проте один з основних результатів теорії подільності в кільці $P[x]$, а саме – *можливість і єдиність розкладу многочлена у добуток незвідних множників* – залишається в силі і в кільці $P[x_1, x_2, \ldots, x_n]$ *для* $n \geq 2$.

***Теорема**. Будь-який многочлен $f(x_1, x_2, \ldots, x_n)$ над полем P ненульового степеня можна подати як добуток многочленів, незвідних у полі P.*

***Теорема**. Якщо S – область цілісності з одиницею, в якій кожний елемент, відмінний від нуля і від дільника одиниці, однозначно розкладається в добуток простих елементів, то кільце $S[x]$ многочленів над S має такі самі властивості.*

Наслідок. *Будь-який многочлен $f(x_1, x_2, \ldots, x_n) \in P[x_1, x_2, \ldots, x_n]$ ненульового степеня розкладається на незвідні множники єдиним способом* (з точністю до сталих множників і порядку співмножників).

Основна ідея доведення полягає в тому, щоб «вкласти» область цілісності *S* у поле відношень *T,* що завжди

можливо, а далі скористатися тим відомим фактом, що кільце многочленів від однієї змінної над полем є кільцем головних ідеалів і тому в ньому розклад на незвідні множники єдиний. Всюди далі в цьому пункті S позначає область цілісності з одиницею, в якій кожний елемент, відмінний від нуля та від дільника одиниці, однозначно розкладається на прості множники.

***Лема 1**. Для будь-якої скінченної системи елементів a_1, a_2, ..., $a_k \in S$, відмінних від нуля, існує єдиний* (з точністю до дільників одиниці) *найбільший спільний дільник.*

***Означення**. Многочлен $f(x) \in S[x]$, відмінний від нуля, називається примітивним* (відносно S), *якщо* НСД *його коефіцієнтів дорівнює* 1.

***Лема 2**. Добуток двох примітивних многочленів з S $[x]$ є знову примітивний многочлен.*

Нехай тепер T – поле відношень області цілісності S. Розглянемо кільце $T[x]$ многочленів над полем T, тобто многочленів, які можна подати у формі

$$\varphi(x) = \frac{a_n}{b_n}x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots, + \frac{a_0}{b_0},\ a_i, b_i \in S,\ i=0,1,\ldots,n. \quad (12.5)$$

У кільці $T[x]$, згідно з теоремою, розклад на незвідні множники однозначний. Щоб перейти від T $[x]$ до нашого кільця S $[x]$, поставимо кожному многочлену $\varphi(x) \in T$ $[x]$ у відповідність деякий примітивний многочлен f_φ $(x) \in S$ $[x]$ згідно з таким правилом.

Нехай φ (x) – ненульовий многочлен з $T[x]$, поданий у формі (12.5). Помноживши $\varphi(x)$ на елемент $b = b_0b_1 \ldots b_{n-1}b_n \in S$, маємо многочлен $b\varphi(x)$ з кільця $S[x]$. Позначимо через a НСД коефіцієнтів многочлена $b\varphi(x)$ у кільці S. Тоді многочлен $f_\varphi(x) = \frac{b\varphi(x)}{a}$ є примітивним многочленом у кільці $S[x]$ і називається *відповідним многочленом* $\varphi(x) \in T$ $[x]$.

***Лема 3**. Відповідність $\varphi(x) \to f_\varphi(x)$ взаємно однозначна з точністю до дільників одиниці.* Точніше: *для кожного відмінного від нуля многочлена $\varphi(x) \in T[x]$ відповідний примітивний многочлен $f_\varphi(x) \in S[x]$ єдиний з точністю до дільників одиниці кільця S; два многочлени $\varphi(x)$, $\psi(x) \in T[x]$, яким відповідає той самий примітивний многочлен*

$f_\varphi(x)=f_\psi(x) \in S[x]$, *збігаються з точністю до дільників одиниці кільця* $T[x]$.

Лема 4*. Многочлен* $w(x) \in T\,[x]$ *звідний в* T *тоді і тільки тоді, коли многочлен* $f_w(x) \in S[x]$ *звідний в* S, *причому* $w(x)=\varphi(x)\psi(x) \leftrightarrow f_w(x)=f_\varphi(x)f_\psi(x)$ (з точністю до відповідних дільників одиниці). *Многочлен* $w(x) \in T\,[x]$ *незвідний в* T *тоді і тільки тоді, коли многочлен* $f_w\,(x)$ *незвідний в* S.

Симетричні многочлени

Важливим класом многочленів від кількох змінних є клас так званих симетричних многочленів.

Означення. *Многочлен* $f(x_1, x_2,\ldots,x_n)$ *називається симетричним відносно змінних* $x_1, x_2, \ldots, x_n$, *якщо внаслідок довільної перестановки змінних* $x_1, x_2, \ldots, x_n$ *утворюється многочлен, який дорівнює даному.*

Наприклад.

а) многочлени $f_1(x_1, x_2)=x_1^2+x_2^2$, $f_2(x_1, x_2, x_3)=x_1x_2^2+3x_1x_2-2x_1-2x_2+x_1^2x_2+5$ симетричні відносно змінних x_1 і x_2, бо не змінюються від перестановки цих змінних;

б) многочлен $f_2(x_1, x_2, x_3)=2x_2^2+x_1x_2+x_2x_3$ симетричний відносно змінних x_1 і x_3, але не симетричний відносно змінних x_2, x_3 або x_1, x_2, тому він не симетричний і відносно всіх змінних x_1, x_2, x_3.

З важливими прикладами симетричних многочленів ми, власне кажучи, вже зустрічались у формулах Вієта (тема вісім). Якщо позначити через $x_1, x_2,\ldots,x_n$ корені многочлена $f(x)=x^n+a_{n-1}x^{n-1}+\ldots$ за формулами Вієта матимемо:

$$\begin{gathered} x_1 + x_2 + \cdots + x_n = -a_{n-1}, \\ x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + \\ +x_2x_n + \cdots + x_{n-1}x_n = a_{n-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_1x_2 \ldots x_n = (-1)^n a_0\,. \end{gathered} \qquad (12.6)$$

Позначимо ліві частини цих формул відповідно через $\sigma_1, \sigma_2, \ldots, \sigma_n$ тобто

$$\begin{gathered} \sigma_1 = x_1 + x_2 + \cdots + x_n, \\ \sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \sigma_n = x_1x_2 \ldots x_n\,. \end{gathered} \qquad (12.7)$$

Якщо під $x_1, x_2, \ldots x_n$ розуміти незалежні змінні, то $\sigma_1, \sigma_2, \ldots, \sigma_n$ є, очевидно, многочлени, симетричні відносно цих змінних. Многочлени (12.7) називаються *основними симетричними функціями.*

Встановимо тепер деякі елементарні властивості довільних симетричних многочленів.

1. *Сума, різниця і добуток симетричних многочленів над деяким полем P є знову симетричними многочленами над цим полем.*

   Наслідок. *Множина всіх симетричних многочленів над полем P утворює область цілісності з одиницею відносно дій додавання і множення.* Це кільце є підкільцем усіх многочленів над полем *P.*

2. *Якщо симетричний многочлен* $f(x_1, x_2, \ldots, x_n)$ *містить деякий член* $Mx_1^{l_1}x_2^{l_2}\ldots x_i^{l_i}\ldots x_j^{l_j}\ldots x_n^{l_n}$, *то він містить і член, утворений з даного внаслідок будь-якої перестановки показників* $l_1, l_2, \ldots, l_n$.

   Наслідок. *Якщо* $Mx_1^{l_1}x_2^{l_2}\ldots x_i^{l_i}x_{i+1}^{l_{i+1}}\ldots x_n^{l_n}$, *є вищий член симетричного многочлена, то* $l_1 \geq l_2 \geq \ldots \geq l_n$.

Теорема. **(*Основна теорема теорії симетричних многочленів*).** *Всякий симетричний многочлен* $f(x_1, x_2, \ldots, x_n)$ *від n змінних над полем P можна подати у вигляді многочлена від основних симетричних функцій* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *цих змінних, коефіцієнти якого належать тому самому полю P.*

Теорема*. Зображення симетричного многочлена у вигляді многочлена від основних симетричних функцій єдине.*

Теорема*. Якщо* $f(x)$ *– многочлен від однієї змінної над полем P, коренями якого є* $\alpha_1, \alpha_2, \ldots, \alpha_n$ (які можуть не належати *P), то будь-який симетричний многочлен* $g(x_1, x_2, \ldots, x_n)$ *над полем P при* $x_1=\alpha_1, \ldots, x_n = \alpha_n$ *набуває значення, яке є елементом поля P.*

У низці питань доводиться зустрічатися з задачею побудови за даним многочленом $f(x) \in P$ з коренями $x_1, x_2, \ldots, x_n$ такого многочлена $g(y)$, корені якого y_i виражаються через відповідні корені x, за допомогою деякого многочлена $y=\varphi(x)$ над полем P; $y_i=\varphi(x_i)$. Найпростіші задачі такого типу зустрічаються в шкільному курсі алгебри для $P=Q$.

Наприклад. Нехай треба подати симетричний многочлен над полем Q через основні симетричні функції:

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + +x_2^2x_3 + x_2x_3^2 - \\ - 4(x_1^2 + x_2^2 + x_3^2) + 5.$$

Запишемо цей многочлен як суму однорідних многочленів. Отримуємо:

$$f(x_1, x_2, x_3) = \varphi_1(x_1, x_2, x_3) - 4\varphi_2(x_1, x_2, x_3) + 5;$$
$$\varphi_1(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + \\ +x_2^2x_3 + x_2x_3^2;$$
$$\varphi_2(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2.$$

Спочатку $\varphi_1(x_1, x_2, x_3)$ подамо через основні симетричні многочлени. Вищий його член є $x_1^2x_2$. Від $\varphi_1(x_1, x_2, x_3)$ слід відняти многочлен $g(x_1, x_2, x_3) = \sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0 = \sigma_1\sigma_2$, бо система показників у вищому члені є 2, 1, 0. Але немає потреби фактично виконувати це віднімання. Спираючись на можливість і єдиність зображення даного многочлена у вигляді многочлена $\varphi(\sigma_1, \sigma_2, ..., \sigma_n)$, досить визначити можливий вигляд членів φ $(\sigma_1, \sigma_2,...,\sigma_n)$, і скористатися методом невизначених коефіцієнтів.

У різниці φ_1 (x_1, x_2, x_3) - $g(x_1, x_2, x_3)$, зникнуть всі члени виду $Ax_1^{l_1}x_2^{l_2}x_3^{l_3}$ з довільною перестановкою показників 2, 1, 0. Проте одночасно можуть з'явитися члени того самого степеня 3, але з іншою, нижчою системою показників, а саме: 1, 1, 1. Отже, потім треба буде відняти симетричний многочлен $g(x_1, x_2, x_3) = \sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^1 = \sigma_3$. Тому можна записати: $\varphi_1(x_1, x_2, x_3)=\sigma_1\sigma_2+\alpha\sigma_3$, де α – невизначений поки що коефіцієнт, тобто:

$$x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + \\ +x_2^2x_3 + x_2x_3^2=(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + \\ +ax_1x_2x_3.$$

Щоб знайти α, досить надати деяких числових значень змінним x_1, x_2, x_3, наприклад $x_1 = x_2 = x_3 = 1$. Тоді маємо: 6 = 9 + α. Отже, α = -3. Таким чином, $\varphi_1(x_1, x_2, x_3)=\sigma_1\sigma_2-3\sigma_3$.

Аналогічно міркуватимемо відносно многочлена

$$\varphi_2(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3) = \mathrm{x}_1^2 + \mathrm{x}_2^2 + \mathrm{x}_3^2.$$

Можливі системи показників тут будуть 2, 0, 0 і 1, 1, 0. Отже, відніматимемо такі многочлени:

$$g_2(x_1, x_2, x_3) = \sigma_1^{2-0}\sigma_2^{0-0}\sigma_3^0 = \sigma_1^2;$$
$$g_3(x_1, x_2, x_3) = \sigma_1^{1-1}\sigma_2^{1-0}\sigma_3^0 = \sigma_{2.}$$

І далі, аналогічно до попереднього, $\varphi_2(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3) = \sigma_1^2 + + b\sigma_2$ при $x_1 = x_2 = x_3 = 1$, маємо

$3 = 3^2 + b \bullet 3$, тобто $b = -2$ і тому $\varphi_2(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3) = \sigma_1^2 - 2\sigma_2$. Отже, остаточно отримуємо

$$f(x_1, x_2, x_3) = \sigma_1\sigma_2 - 3\sigma_3 - 4(\sigma_1^2 - 2\sigma_2) + 5.$$

Теорія симетричних многочленів має досить широке застосування в алгебрі.

Приклади розв'язування типових завдань

№1. *Розв'язати систему* $\begin{cases} 4(x+y) = 3xy, \\ x + y + x^2 + y^2 = 26. \end{cases}$

Розв'язання. Ліві частини обох рівнянь є симетричними многочленами, тому для розв'язання даної системи доцільно скористатися теоремою про симетричні многочлени від двох змінних (будь-який симетричний многочлен від x та y можна представити у вигляді многочлена від $\sigma_1 = x + y$ та $\sigma_2 = xy$).

Застосувавши теорему про симетричні многочлени від двох змінних, отримаємо систему: $\begin{cases} 4\sigma_1 = 3\sigma_2, \\ \sigma_1 + {\sigma_1}^2 - 2\sigma_2 = 26. \end{cases}$

Виразивши σ_2 з 1-го рівняння і підставивши в 2-ге рівняння системи отримуємо: $3{\sigma_1}^2 - 5\sigma_1 - 78 = 0$. Розв'язавши квадратне рівняння маємо: $\sigma_{11} = 6$; $\sigma_{12} = -\frac{13}{3}$. Тоді відповідно $\sigma_{21} = 8$; $\sigma_{22} = -\frac{52}{9}$.

Повернувшись до заміни, отримуємо наступні пари розв'язків початкової системи: (4;2), (2;4), $(\frac{-13+\sqrt{377}}{6}; \frac{-13-\sqrt{377}}{6})$; $(\frac{-13-\sqrt{377}}{6}; \frac{-13+\sqrt{377}}{6})$.

Відповідь:

(4; 2), (2; 4), $(\frac{-13+\sqrt{377}}{6}; \frac{-13-\sqrt{377}}{6})$; $(\frac{-13-\sqrt{377}}{6}; \frac{-13+\sqrt{377}}{6})$.

Таблиця 12.1

Вираження степеневої суми

$s_n = x^n + y^n$ через $\sigma_1 = x + y$ та $\sigma_2 = xy$

s_1	σ_1	s_6	$\sigma_1^6 - 6\sigma_1^4\sigma_2 + 9\sigma_1^2\sigma_2^2 - 2\sigma_2^3$
s_2	$\sigma_1^2 - 2\sigma_2$		
s_3	$\sigma_1^3 - 3\sigma_1\sigma_2$	s_7	$\sigma_1^7 - 7\sigma_1^5\sigma_2 + 14\sigma_1^3\sigma_2^2 - 7\sigma_1\sigma_2^3$
s_4	$\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2$		
s_5	$\sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2$	s_8	$\sigma_1^8 - 8\sigma_1^6\sigma_2 + 20\sigma_1^4\sigma_2^2 - 16\sigma_1^2\sigma_2^3 + 2\sigma_2^4$
		s_9	$\sigma_1^9 - 9\sigma_1^7\sigma_2 + 27\sigma_1^5\sigma_2^2 - 30\sigma_1^3\sigma_2^3 + 9\sigma_1\sigma_2^4$
		s_{10}	$\sigma_1^{10} - 10\sigma_1^8\sigma_2 + 35\sigma_1^6\sigma_2^2 - 50\sigma_1^4\sigma_2^3 + 25\sigma_1^2\sigma_2^3 - 2\sigma_2^5$

№2. *Виразити через елементарні симетричні многочлени такі многочлени*: а) $x^3 + 2x^2y + 2xy^2 + y^3$;

б) $x^4 + y^4 + z^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2$.

Розв'язання

а) $x^3 + 2x^2y + 2xy^2 + y^3 = (x+y)^3 - x^2y - xy^2 =$

$= (x+y)^3 - xy(x+y) = \sigma_1^3 - \sigma_1\sigma_2$;

б) $x^4 + y^4 + z^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2 = \sigma_1^4 -$

$- 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 - 2(x^2y^2 + x^2z^2 + y^2z^2) = \sigma_1^4 -$

$- 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 - 2(\sigma_2^2 - 2\sigma_1\sigma_3) = \sigma_1^4 - 4\sigma_1^2\sigma_2 +$

$+ 2\sigma_2^2 + 4\sigma_1\sigma_3 - 2\sigma_2^2 + 4\sigma_1\sigma_3 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 8\sigma_1\sigma_3$.

Відповідь: а) $\sigma_1^3 - \sigma_1\sigma_2$; б) $\sigma_1^4 - 4\sigma_1^2\sigma_2 + 8\sigma_1\sigma_3$.

Завдання для аудиторного заняття

№1. Розв'язати системи рівнянь:

а) $\begin{cases} x^3 + y^3 = 8 \\ x^2 + y^2 = 4 \end{cases}$; б) $\begin{cases} x^3 + y^3 = 35 \\ x + y = 5 \end{cases}$;

в) $\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$; г) $\begin{cases} x^2 - xy + y^2 = 19 \\ x - xy + y = 7 \end{cases}$.

№2. Виразити через елементарні симетричні многочлени такі многочлени:

а) $f(x_1x_2x_3) = x_1^3 + x_2^3 + x_3^3 - x_1 - x_2 - x_3$;

б) $f(x_1x_2x_3) = x_1^5x_2^1x_3 + x_2^5x_1x_3 + x_1x_2x_3^5 + 2x_1x_2x_3$;

в) $f(x_1x_2x_3) = x_1^4x_2^2 + x_2^4x_1^2 + x_3^4x_2^2 + x_3^4x_1^2 + x_1^4x_3^2 + x_2^4x_3^2$;

г) $f(x_1x_2x_3) = x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3$;

д) $f(xyz) = x^5y^2 + x^5z^2 + x^2y^5 + x^2z^5 + y^5z^2 + y^2z^5$;

е) $f(xyz) = (x + y)(x + z)(y + z)$;

є) $f(xyz) = (x^2 + y^2)(x^2 + z^2)(y^2 + z^2)$.

№3. Перевірити подільність многочлена $f(x,y,z,t)=(xy- zt)^5+(zx-yt)^5$ на $g(x,y,z,t)=(y+z)(x-t)$ в кільці $Z[x, y, z, t]$.

№4. Відомо, що $s_2(x,y)=x^2+y^2$. Довести, що $s_2=\delta_1^2-2\delta_2$.

Відповіді: ***№1.*** б) (2; 3), (3; 2); в) (2; 1), (1; 2), $\left(\frac{3}{2}+\frac{\sqrt{19}}{2}i;\ \frac{3}{2}-\frac{\sqrt{19}}{2}i\right), \left(\frac{3}{2}-\frac{\sqrt{19}}{2}i;\ \frac{3}{2}+\frac{\sqrt{19}}{2}i\right)$; г) (1; 1). ***№2.*** *е)* $\sigma_1\sigma_2 - \sigma_3$.

Завдання для самостійного розв'язування

№1. Виразити через основні симетричні многочлени:

а) $f(x_1x_2x_3) = (x_1 - x_2)^2 + (x_1 - x_3)^2 + (x_2 - x_3)^2$;

б) $f(x_1x_2x_3) = (x_1 + x_2 - 5x_3)(x_2 + x_3 - 5x_1)(x_1 + +x_3 - 5x_2)$;

в) $f(x_1x_2x_3) = (x_1^2 - x_2x_3)(x_2^2 - x_1x_3)(x_3^2 - x_1x_2)$;

г) $f(xyz) = (x - y)^2(y - z)^2(z - x)^2$;

д) $f(x_1x_2x_3) = x_1^4 + x_2^4 + x_3^4 - 2x_1^2x_2^2 - 2x_2^2x_3^2 - 2x_3^2x_1^2$.

№2. Виразити через елементарні симетричні многочлени такі многочлени:

а) $f(x_1x_2x_3) = (x_1 - x_2)^2 + (x_1 - x_3)^2 + (x_2 - x_3)^2$;

б) $f(x_1x_2x_3) = (x_1 + x_2 - 5x_3)(x_2 + x_3 - 5x_1)(x_1 + +x_3 - 5x_2)$;

в) $f(x_1x_2x_3) = (x_1^2 - x_2x_3)(x_2^2 - x_1x_3)(x_3^2 - x_1x_2)$.

№3. Розв'язати системи:

1) $\begin{cases} x^2 + xy + y^2 = 4 \\ x + xy + y = 2 \end{cases}$;

5) $\begin{cases} 2(x + y) = 5xy \\ 8(x^3 + y^3) = 65 \end{cases}$;

2) $\begin{cases} x+y=a+b \\ x^2+y^2=a^2+b^2 \end{cases}$;

3) $\begin{cases} x^3+y^3=5a^3 \\ x^2y+xy^2=a^3 \end{cases}$;

4) $\begin{cases} x^4+x^2y^2+y^4=91 \\ x^2-xy+y^2=7 \end{cases}$;

6) $\begin{cases} x+y=1 \\ x^4+y^4=7 \end{cases}$;

7) $\begin{cases} (x^2+1)(y^2+1)=10 \\ (x+y)(xy-1)=3 \end{cases}$;

8) $\begin{cases} x^2+y^2=axy \\ x^4+y^4=bx^2y^2 \end{cases}$.

№4. Відомо, що $s_3(x,y)=x^3+y^3$. Довести, що $s_3=\delta_1^3-3\delta_1\delta_2$.

№5. Відомо, що $s_2(x,y)=x^2+y^2$. Довести, що $s_2=\delta_1^2-2\delta_2$.

№6. Нехай x_i – корені многочлена (i=1, 2, 3) $4x^3-x^2+5x-1$. Скласти кубічне рівняння, коренями якого є x_1^2, x_2^3, x_3^2.

Відповіді: ***№1.*** д) $\sigma_1^4+8\sigma_1\sigma_3-4\sigma_1^2\sigma_2$.

СПИСОК ВИКОРИСТАНОЇ І РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Завало С.Т. Курс алгебри. К.: Вища школа. 1985. 503 с.
2. Завало С. Т., Костарчук В.М., Хацет. Б.І. Алгебра і теорія чисел.Ч.1: підручник. К., 1974. 288 с.
3. Завало С. Т., Костарчук В.М., Хацет. Б.І. Алгебра і теорія чисел.Ч.2: підручник. К., 1976. 388 с.
4. Завало С.Т., Левищенко С.С., Пилаєв В.В., Рокицький І.Д. Алгебра і теорія чисел: Практикум. Частина 1. К: Вища школа: Гол. вид-во, 1983. 224 с.
5. Завало С.Т., Левищенко С.С., Пилаєв В.В., Рокицький І.Д. Алгебра і теорія чисел: Практикум. Частина 2. К: Вища школа: Гол. вид-во, 1986. 264 с.
6. Оглобліна О. І., Сушко Т. С., Шрамко Ю. В. Елементи теорії чисел: навч. посіб. Суми: Сумський державний університет, 2015. 186 с
7. Окунєв Л.Я. Вища алгебра. К. Радянська школа, 1950. 254 с.
8. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел. Ч.1. К.: НПУ імені М.П.Драгоманова, 2009. 420 с.
9. Требенко Д.Я., Требенко О.О. Збірник індивідуальних розрахункових завдань з курсу «Алгебра і теорія чисел» Ч.1. К.: НПУ імені М.П.Драгоманова, 2010. 172 с.
10. Требенко Д.Я., Требенко О.О. Збірник індивідуальних розрахункових завдань з курсу «Алгебра і теорія чисел» Ч.2. К.: НПУ імені М.П.Драгоманова, 2011. 110 с.

ГРЕЦЬКИЙ АЛФАВІТ

Буква	*Назва букви*	*Буква*	*Назва букви*
Α α	альфа	**Ν ν**	ню
Β β	бета	**Ξ ξ**	ксі
Γ γ	гамма	**Ο ο**	омікрон
Δ δ	дельта	**Π π**	пі
Ε ε	епсілон	**Ρ ρ**	ро
Ζ ζ	дзета	**Σ σ**	сігма
Η η	ета	**Τ τ**	тау
Θ θ	тета	**Υ υ**	іпсилон
Ι ι	йота	**Φ φ**	фі
Κ κ	каппа	**Χ χ**	хі
Λ λ	лямбда	**Ψ ψ**	псі
Μ μ	мю	**Ω ω**	омега

ЛАТИНСЬКИЙ АЛФАВІТ

Буква	*Назва букви*	*Буква*	*Назва букви*
A a	а	**N n**	ен
B b	бе	**O o**	о
C c	це	**P p**	пе
D d	де	**Q q**	ку
E e	е	**R r**	ер
F f	еф	**S s**	ес
G g	же	**T t**	те
H h	аш	**U u**	у
I i	і	**V v**	ве
J j	жі	**W w**	дубль ве
K k	ка	**X x**	ікс
L l	ель	**Y y**	ігрек
M m	ем	**Z z**	зет

Навчальне видання

ЗАЇКА Оксана Володимирівна
СУХОЙВАНЕНКО Людмила Федорівна
ПРОКОПЕЦЬ Тетяна Олександрівна

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

НАВЧАЛЬНИЙ ПОСІБНИК

Відповідальний за випуск *Л.Ф. Сухойваненко*
Редактор *О.В. Заїка*
Комп'ютерне верстання *С.П. Цьома*

Підп. до друку 18.01.2023.
Формат 60x84/16. Гарнітура Cambria.
Папір офсетний. Друк офсетний. Ум. друк. арк. 15,35.
Ум. фарб.-відб. 15,35. Обл.-вид. арк. 13,78.
Тираж 100 пр. Вид. № 2.

СумДПУ імені А. С. Макаренка
40002, м.Суми, вул.Роменська, 87
Свідоцтво ДК № 231 від 02.11.2000 р.

Видавець і виготовлювач:
ФОП Цьома С.П. 40002, м. Суми, вул. Роменська, 100.
Тел.: 066-293-34-29.