Д.Я.Требенко, О.О.Требенко

Використання системи комп'ютерної алгебри Maple при вивченні курсу „Алгебра і теорія чисел"

Рекомендовано Міністерством освіти і науки України
як навчальний посібник для студентів вищих навчальних закладів

2014

ББК 22.14я73+22.13я73
Т66
УДК 512(075.8)+511(075.8)

Гриф надано Міністерством освіти і науки України, лист № 1/11-7622 *від* 25.04.2013

Требенко Д.Я., Требенко О.О. Використання системи комп'ютерної алгебри Maple при вивченні курсу „Алгебра і теорія чисел". – К.: НПУ імені М.П.Драгоманова, 2014. – 532 с.

У навчальному посібнику розглядаються можливості використання системи комп'ютерної алгебри Maple для супроводу навчання вищої алгебри в університеті.

Зміст посібника повністю відповідає діючій програмі курсу „Алгебра і теорія чисел" для математичних спеціальностей педагогічних університетів. Посібник містить початкові відомості про Maple, типові задачі курсу, вміння розв'язувати які є необхідною умовою свідомого опанування теоретичного матеріалу курсу, показником сформованості базових навичок. Основні теоретичні відомості, винесені на початок кожного параграфу, допомагають виділити головне, найсуттєвіше в темі. Кожний тип завдань супроводжується зразком аналітичного розв'язання (без використання комп'ютера) та зразком перевірки в Maple (із використанням комп'ютера). Наявність 25 варіантів завдань дозволяє індивідуалізувати навчальний процес.

Посібник призначений для студентів математичних спеціальностей вищих педагогічних навчальних закладів. Він також може бути з успіхом використаний при викладанні курсу вищої математики для студентів технічних спеціальностей.

Рецензенти:

Працьовитий М.В.	доктор фіз.-мат. наук, професор, зав. кафедри вищої математики НПУ імені М.П.Драгоманова, Заслужений діяч науки і техніки України
Семко М.М.	доктор фіз.-мат. наук, професор, зав. кафедри вищої математики Національного університету державної податкової служби України

ISBN 978-966-660-936-9

Зміст

Передмова

Одним із перспективних напрямів розвитку і модернізації сучасної вітчизняної освіти є інформатизація – раціоналізація інтелектуальної діяльності за рахунок використання в навчальному процесі сучасних інформаційних і комунікаційних технологій (ІКТ). Як показує практика, використання ІКТ в процесі навчання підвищує мотивацію учнів та студентів до навчання, сприяє розвитку інтелекту і формуванню навичок самостійної роботи з пошуку необхідної інформації, розширює обсяг навчальної інформації, забезпечує індивідуальний підхід у навчанні, підвищує якість контролю знань учнів, забезпечує гнучкість управління навчальним процесом. Результат впровадження ІКТ в навчальний процес безпосередньо залежить від професійних знань, вмінь і навичок вчителя. Вчитель має бути готовим до використання ІКТ в своїй професійній діяльності, володіти навичками організації навчання із використанням ІКТ, знати можливі раціональні і найбільш ефективні способи організації, вміти комбінувати їх та пристосовувати до потреб конкретної учнівської аудиторії, а також знати, як реалізувати принцип особистісно-орієнтованого навчання, як організувати активну творчу діяльність учнів в умовах застосування ІКТ.

На глибоке переконання авторів, для формування ІКТ-компетенції майбутнього вчителя особливо важливо, щоб студент бачив можливості, способи, шляхи використання ІКТ (а не лише був теоретично з ними ознайомлений) в процесі власного навчання, організованого із використанням елементів ІКТ. При цьому особлива роль відводиться інформатизації фундаментальних математичних дисциплін, адже викладати майбутній фахівець буде саме фундаментальну науку.

У даному навчальному посібнику розглядаються можливості використання системи комп'ютерної алгебри Maple для супроводу навчання вищої алгебри в університеті.

Посібник складений відповідно до діючої програми курсу "Алгебра і теорія чисел" для студентів спеціальності 6.040201 "Математика". Головною метою курсу "Алгебра і теорія чисел" є вивчення основ сучасної абстрактної алгебри, її місця в загальній системі математичних знань, зокрема, її взаємозв'язків з теорією чисел, формування загальнонаукового світогляду і виховання алгебраїчної та теоретико-числової культури, необхідної майбутньому вчителю для глибокого розуміння цілей і завдань як основного шкільного курсу математики, так і спеціальних факультативних курсів, і також для проведення наукових досліджень.

Відповідно до програми значну частину часу для вивчення дисципліни відведено на самостійну роботу студентів. Саме систематична самостійна робота є однією із важливих форм ефективного засвоєння навчального матеріалу. З метою її інтенсифікації пропонується виконання індивідуальних домашніх завдань. Відмітимо, що для успішного засвоєння програмового матеріалу необхідно вміти розв'язувати всі задачі, які вміщено до даного посібника.

Ефективність самостійної роботи на стадії формування вмінь і навичок розв'язування задач значною мірою залежить від можливості студента вчасно проконтролювати себе. Помилка, виявлена самим студентом на даному етапі, спонукає його до пошуку причини цієї помилки, більш детального вивчення теоретичного матеріалу.

Для перевірки отриманого розв'язку задачі зручно використовувати спеціальні комп'ютерні програми - системи комп'ютерної алгебри (СКА). Одним із світових лідерів серед СКА є пакет Maple. Серед інших його виділяє ряд переваг: розвинуті графічні засоби, сучасний багатовіконний інтерфейс із можливістю роботи в діалоговому режимі, потужна бібліотека математичних функцій, великий набір додаткових пакетів функцій, деталізована довідкова система із прикладами використання команд, сучасна мова програмування інтерпретуючого типу, наявність засобів підтримки деяких інших мов програмування та інтеграції із широковідомими програмами.

Для розв'язання багатьох алгебраїчних задач в Maple є готові вбудовані функції. Однак, зрозуміло, що якою б досконалою не була система, завжди знайдеться багато спеціалізованих задач, які залишились поза увагою розробників. Для розв'язання таких задач авторами було створено необхідні Maple-процедури та оформлено їх у вигляді бібліотеки процедур. Файл бібліотеки atchlib.m додається до посібника на диску. Дана бібліотека коректно працює із Maple 9.5 і вище. Бібліотека призначена для досить широкої аудиторії: студентів, аспірантів, викладачів, вчених, які для розв'язування алгебраїчних задач використовують пакет Maple.

Всі вихідні тексти процедур, що містяться в бібліотеці, доступні користувачу. До кожної з них наведено детальне пояснення принципу роботи. Це дозволяє використовувати процедури в якості ілюстративного матеріалу при освоєнні програмування в Maple.

Читачу, який не бажає заглиблюватись у принцип роботи авторських процедур, достатньо викликати необхідну команду із бібліотеки. Натомість для тих, хто прагне розібратись із принципом роботи процедур, детальніше

познайомитись із особливостями програмування в системі Maple, наводимо детальне пояснення в секції „Розробка процедур”. Відмітимо, що деякі процедури можна оптимізувати (це не було зроблено авторами саме для того, щоб для тих, хто вперше знайомиться із основами роботи в Maple, освоєння елементів програмування в Maple було якомога простішим). Тому запрошуємо студентів надавати свої варіанти вдосконалення процедур!!!

В посібнику до кожного типу задач наведено приклад із детальним аналітичним розв'язанням та зразком розв'язання в Maple. Для перевірки отриманого розв'язку задачі або результатів проміжних обчислень студенту достатньо відтворити в Maple наведений зразок, підставивши дані відповідно до свого варіанту. Студент може запропонувати власний алгоритм розв'язання (як аналітичного, так і в Maple), вдосконалити процедуру, наведену в посібнику, створити власну процедуру. Творчість, ініціативність особливо вітаються.

На практиці успішно зарекомендувала себе наступна технологія організації самостійної роботи. Протягом семестру (в 2-3 етапи) студент виконує індивідуальну розрахункову роботу, що включає задачі з даного посібника. Розв'язання задач в Maple не є обов'язковим і оцінюється преміальними балами.

Звіт про розв'язання задач в Maple здається на паперовому носії і має наступне оформлення:

Розрахункова робота №_
з курсу "Алгебра і теорія чисел"
студента _ групи
Прізвище І.П.
Варіант №_
Завдання №_ (Формулювання умови)
Розв'язання. (Хід розв'язання).

Стимулом до роботи в Maple, окрім зазначених преміальних балів, є система оцінювання виконаних завдань із індивідуальної розрахункової роботи. Кожне завдання оцінюється за 3-бальною шкалою: виконано повністю – виконано частково – не виконано. Завдання вважається виконаним повністю лише у випадку, якщо в результаті студент отримав правильну відповідь, правильно оформив розв'язання. У випадку механічної описки, несуттєвої помилки тощо завдання вважається виконаним частково. Щоб уникнути таких описок і помилок, доцільно робити перевірку.

Описана технологія застосування Maple сприяє формуванню навичок самоконтролю студента, допомагає зосередити увагу на поняттях і логіці

методів і алгоритмів абстрактної алгебри, формує уявлення про роль, значення, можливості застосування математичних методів. Аналіз запропонованої викладачем процедури, її вдосконалення і розробка власної процедури допомагають студенту краще зрозуміти суть абстрактних алгебраїчних понять, акцентують увагу на межах застосування алгоритмів розв'язування, нюансах означень, їхнього вибору, формулювання.

Посібник адресований викладачам та студентам математичних спеціальностей. Він також може бути з успіхом використаний при викладанні курсу вищої математики для студентів технічних спеціальностей.

Відмітимо, що в посібнику розглядаються лише ті засоби Maple, які необхідні для розв'язання алгебраїчних задач. Для більш детального ознайомлення із можливостями пакету Maple рекомендуємо звернутись на сайт http://www.maplesoft.com компанії-розробника пакету Maple.

Будемо щиро вдячні за всі зауваження та побажання і просимо їх надсилати за адресою: trebenko@npu.edu.ua

Автори

Розділ I

Початкові відомості про MAPLE

1. Коротка характеристика та історія системи Maple

В останні двадцять років активного розвитку набув новий фундаментальний науковий напрям – комп'ютерна математика. Перші системи комп'ютерної математики використовувались лише для чисельних обчислень. Однак їм на зміну швидко прийшли системи символьної математики (або комп'ютерної алгебри – СКА).

Сьогодні СКА застосовуються в багатьох галузях науки (таких як математика, фізика, хімія, інформатика тощо), техніки, технології. Але особлива роль СКА – в освіті: вони дозволяють перевірити результати громіздких математичних обчислень, більше часу приділити не рутинним обчисленням, а аналізу отриманих результатів; за допомогою СКА можна наочно представити складні математичні об'єкти.

Одним із світових лідерів серед СКА є програма Maple. Роботу над створенням системи було розпочато ще в 1980 році. Група дослідників канадського університету Waterloo поставила перед собою задачу створити таку комп'ютерну систему, яка була б ефективною в наукових дослідженнях і, водночас, достатньо простою, щоб її могли використовувати не лише математики і інженери, але й студенти. Систему було названо Maple. На початку 90-х років XX ст. у Maple з'явився графічний інтерфейс користувача, і саме з цього часу Maple стала широко використовуватись в освіті.

На даний час систему використовують більше 5 мільйонів студентів, вчених, дослідників і спеціалістів різних областей. Користувачами Maple є такі провідні університети і науково-дослідницькі інститути як MIT, Cambridge, Oxford, Waterloo. В промисловості її використовують відомі корпорації Boeing, Bosch, Canon, Motorola, NASA, Toyota, Hewlett Packard, Sun Microsystems, Ford, General Electric, Stanford, Daimler Chrysler та ін.

Систему Maple серед інших виділяє ряд переваг: розвинуті графічні за-

соби, сучасний багатовіконний інтерфейс із можливістю роботи в діалоговому режимі, потужна бібліотека математичних функцій, великий набір додаткових пакетів функцій, деталізована довідкова система із прикладами використання команд, сучасна мова програмування інтерпретуючого типу, наявність засобів підтримки деяких інших мов програмування та інтеграції із широковідомими програмами. В Maple також є редактор для підготовки і редагування документів. Пакет Maple реалізує новітню технологію символьних обчислень, числових обчислень із заданою точністю, містить інноваційні Web-компоненти – маплети (Maplets). Маплети – це засоби візуально-орієнтованого програмування інтерфейсу користувача, вони здатні забезпечити покрокове розв'язання математичних задач із демонстрацією проміжних результатів обчислень. Така покрокова детальна візуалізація істотно підвищує значення системи Maple в освіті.

В Maple є понад 3,5 тисячі вбудованих команд, функцій, процедур, тому велику кількість задач система може розв'язувати без програмування. Достатньо розробити алгоритм розв'язання своєї задачі, виділивши окремі етапи, для яких Maple має готові розв'язання. Але користувач має можливість створювати і власні процедури. Це надзвичайно важливо, оскільки, зрозуміло, що якою б досконалою не була система, завжди знайдеться багато спеціалізованих задач, які залишились поза увагою розробників. Процедури можна оформити у вигляді окремого пакету, доповнити довідковою інформацією, логічно приєднати до основної бібліотеки. Слід відмітити, що розробники Maple ведуть активний діалог із користувачами і розроблені користувачами процедури можуть бути включені до нового релізу.

Таким чином, система Maple – не просто потужний високоінтелектуальний калькулятор, який може розв'язати багато задач аналітично, а система, яка розвивається відповідно до потреб користувачів, внесок у розвиток якої роблять як розробники, так і чисельні користувачі.

2. Структура Maple

Основними компонентами системи Maple є:

1) ядро системи (команди, процедури, написані мовою C);

2) основна бібліотека команд, процедур і функцій та ряд додаткових спеціалізованих пакетів (написаних мовою Maple);

Команди, включені до ядра, виконуються надзвичайно швидко. З даної точки зору, до ядра було б вигідно включати якомога більше обчислювальних засобів. Однак це призводить до уповільнення роботи системи через збільшення навантаження на ядро. Тому об'єм ядра обмежують, залишаю-

чи лише команди, які найчастіше використовуються, але до системи додають бібліотеку команд. Крім того, розширення можливостей системи досягається за рахунок використання додаткових пакетів команд (packages).

3) інтерфейс користувача (сукупність апаратних і програмних засобів для роботи ПК із зовнішнім обладнанням і користувачем).

В різних релізах Maple інтерфейс може бути різним. В Maple 13 є декілька інтерфейсів (стандартний і класичний). Стандартний інтерфейс має наступний вигляд:

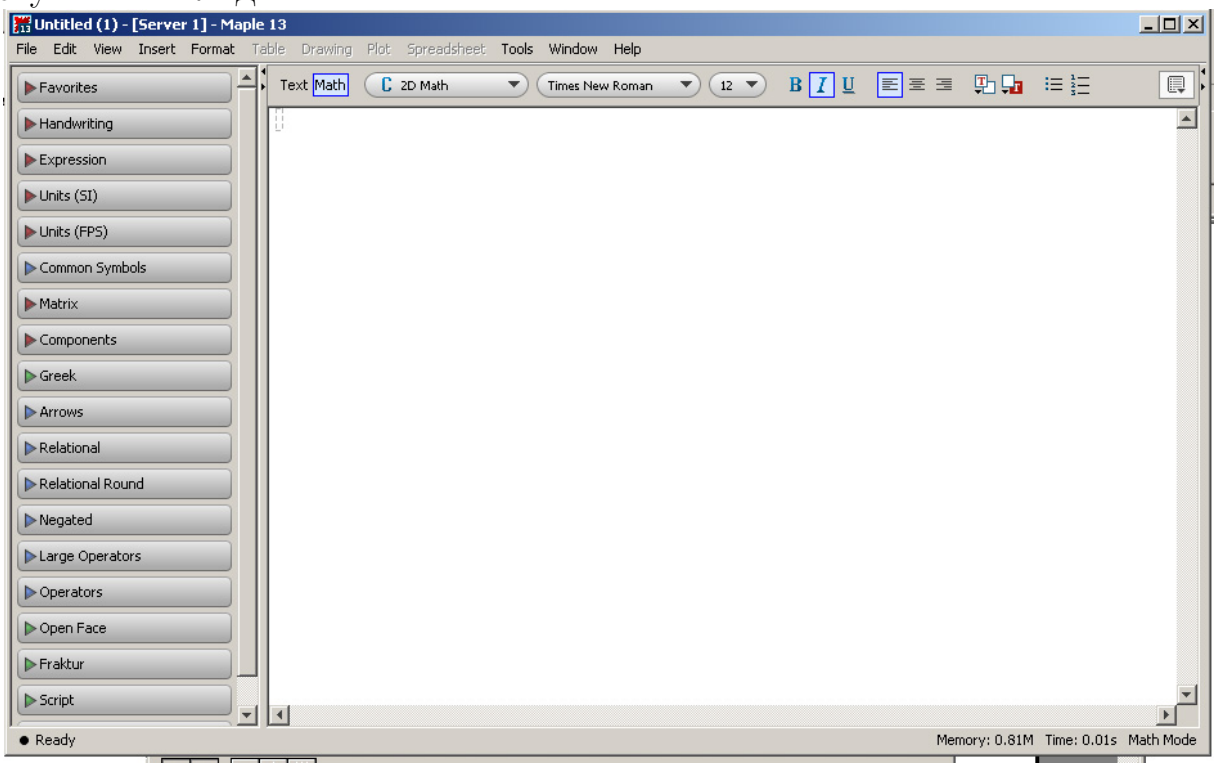


Рис.1

Класичний інтерфейс не змінювався в останніх релізах, починаючи з 4-го:

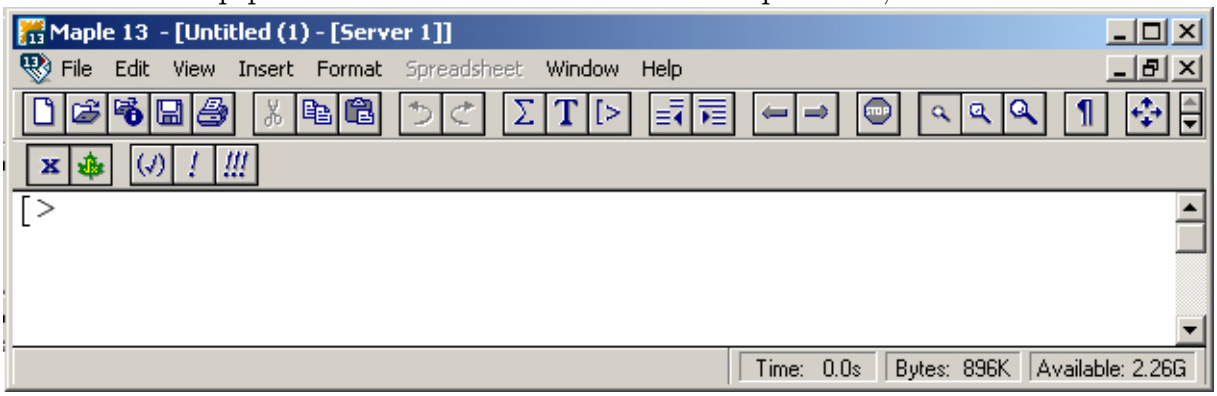


Рис.2

Стандартний інтерфейс – повнофункціональний графічний інтерфейс, використовується для отримання максимальних можливостей системи

Maple. Класичний інтерфейс – базове середовище для малопотужних комп'ютерів, в якому доступні не всі графічні можливості; використання Класичного інтерфейсу вимагає менших затрат пам'яті. Оскільки Класичний інтерфейс доступний ширшому колу користувачів, то в даному посібнику розглядатимемо роботу саме в Класичному інтерфейсі.

Як і в кожній Windows-програмі, інтерфейс Maple має ряд характерних елементів: рядок заголовку (1), рядок головного меню (2), головну панель інструментів (3), контекстну панель інструментів (4), вигляд якої залежить від режиму роботи, робоче поле (5), рядок стану (6), а також лінійки і смуги прокрутки.

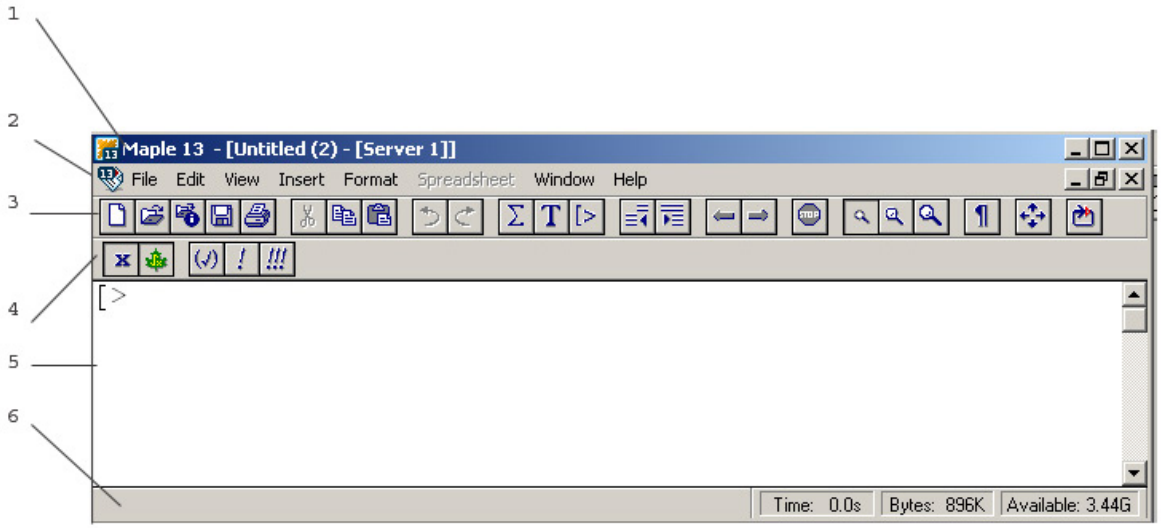


Рис.3

Розглянемо пункти головного меню:

File – містить стандартний набір команд для роботи з файлами, наприклад, зберегти файл, відкрити файл і т.д.

Edit – містить стандартний набір команд для редагування тексту, наприклад, копіювання, видалення виділеного тексту в буфер обміну, відміна команди і т.д.

View – містить стандартний набір команд для управління вікном Maple.

Insert – служить для вставки полів різних типів: математичних, текстових рядків, графічних зображень, гіперпосилань тощо.

Format – містить команди оформлення документу, наприклад, установка типу, розміру і стилю шрифта.

Spreadsheets – служить для роботи із таблицями.

Window – служить для переходу з даного робочого листа на інший.

Help – містить довідкову інформацію про Maple.

Головне меню є контекстно-залежним, тобто його вигляд може змінюватись в залежності від поточного стану (контексту) системи. Наприклад,

якщо всі документи закрито, то головне меню містить лише два пункти: **File** і **Help**. При цьому місце для вікон порожнє і має сірий колір. Вигляд меню також може змінюватись в залежності від того, які об'єкти в документі виділено. Тоді активні пункти меню прописуються чорними буквами, неактивні – сірими.

Призначення пунктів головного меню зрозуміле більшості Windows-користувачів, тому зупинимось лише на пункті **Help**. При виклику пункту **Help/Introduction** з'являється вікно довідкової системи:

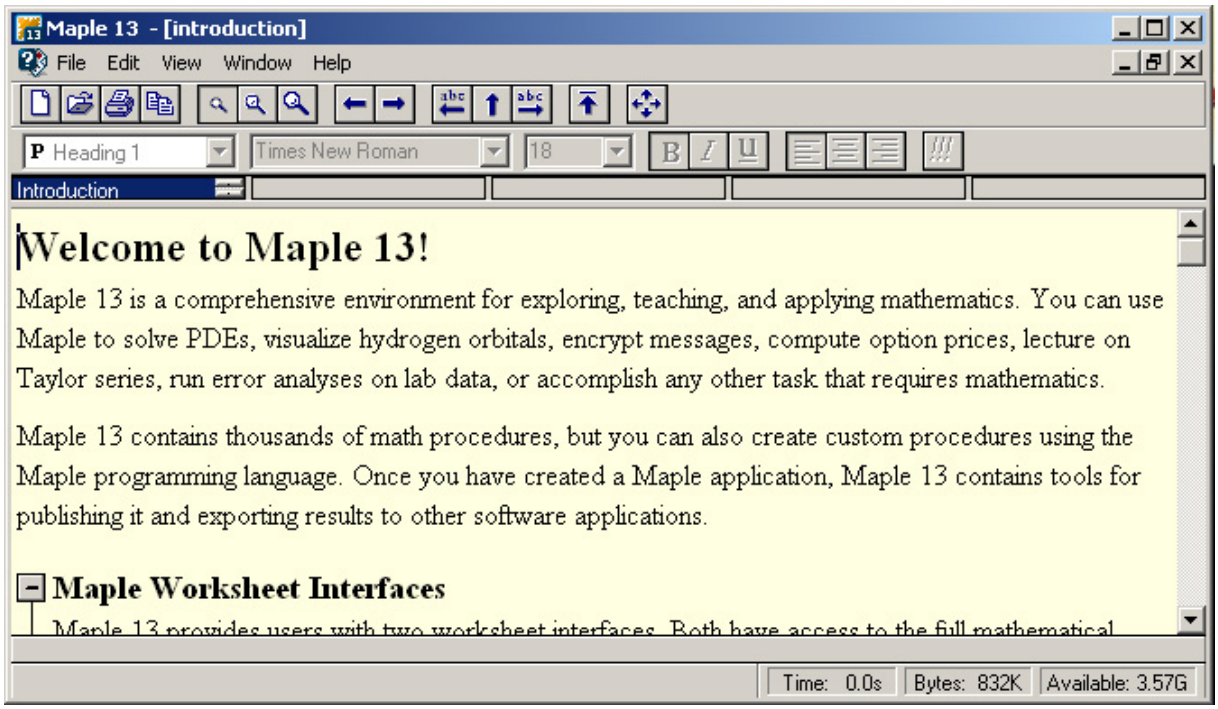


Рис.4

Довідкова система побудована за принципом: розділ/ підрозділ/ підпідрозділ і т.д. Наприклад, для того, щоб побачити довідку про команду **solve**, необхідно викликати **Mathematics/Factorization and Solving Equations/ solve/ Overview**.

Важлива особливість цієї системи – наявність ілюстративних прикладів до кожної із команд. Ці приклади можна скопіювати в свій документ, замінити дані і виконати.

Довідкову інформацію про певну команду можна отримати різними способами:

I спосіб: встановити курсор в будь-яке місце команди і натиснути клавішу **F1**;

II спосіб: в області введення (див.нижче) поставити символ ? і (без пропуску) написати назву команди, після чого натиснути клавішу **Enter**. На рис.5 показано, як отримати довідкову інформацію про команду **solve**:

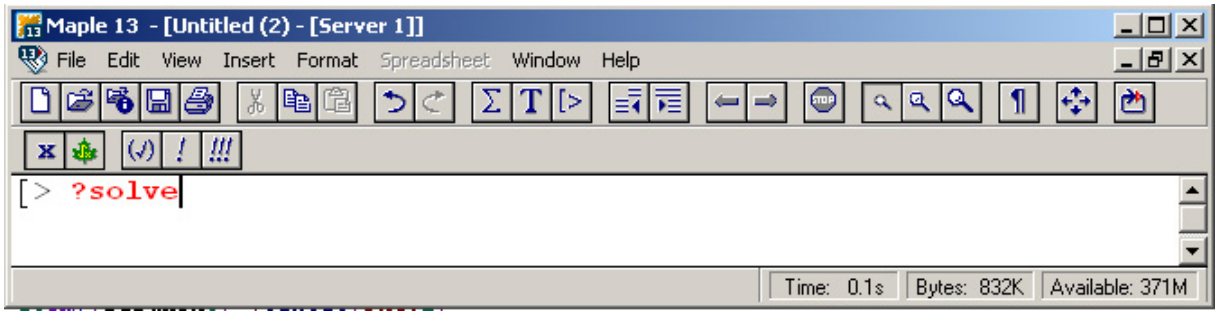


Рис.5

Досить корисний елемент інтерфейсу - підказки, що спливають. Вони з'являються, якщо навести курсор миші на певний елемент інтерфейсу. Підказка має вигляд прямокутної хмаринки, яка розташована біля вказаного елементу. Підказки досить зручні при ознайомленні із призначенням кнопок палітр і панелей інструментів, а також позицій меню.

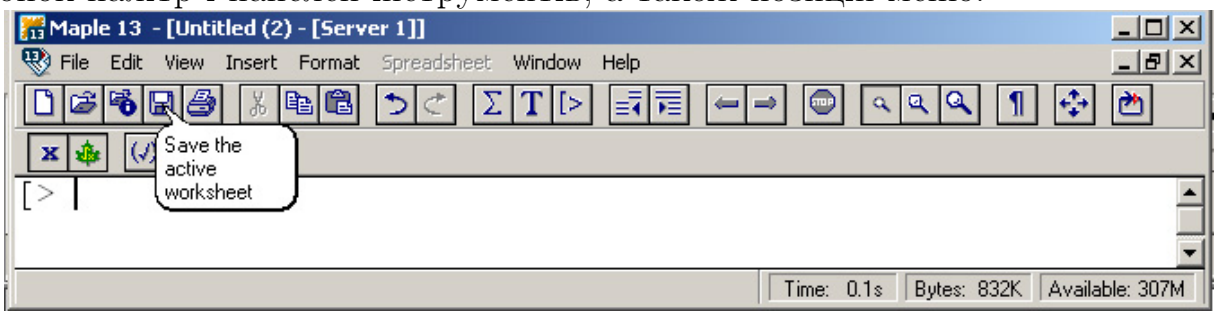


Рис.6

3. Початок роботи

Одразу після завантаження система готова до роботи. Сеанс роботи називають сесією. Робота в Maple відбувається в діалоговому режимі: користувач задає запитання (вводить команди, вирази, процедури), система відповідає (сприймає введені команди, обробляє, виводить на екран результат). Запитання і відповідь на нього виділяються в лівій частині робочого поля квадратними дужками.

Робоче поле має 3 області: область введення, область виведення, область текстових коментарів.

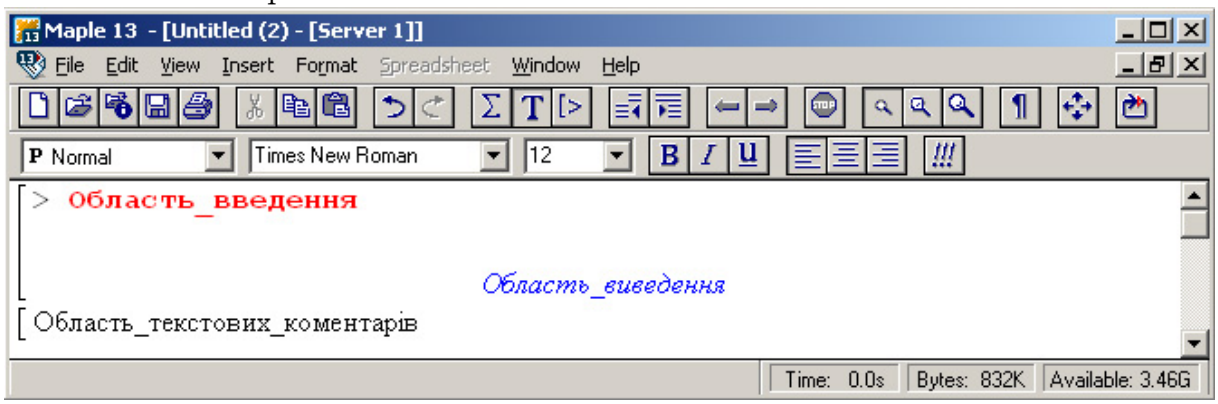


Рис.7

Область введення складається із командних рядків („рядків запитань”). Кожний командний рядок починається із символу „>”, містить Maple-команди, закінчується символом „;” (крапка з комою) або символом „:” (двокрапка). Знак „;” вказує на те, що результат виконання команди необхідно вивести на екран. Якщо ж використовується знак „:”, то команда обробляється системою, але результат на екран не виводиться (цей знак зручно використовувати при проміжних обчисленнях). Колір шрифта – червоний.

Область виведення містить результати виконання введених команд у вигляді аналітичних виразів, графічних об’єктів або повідомлень про помилку. Колір шрифта – синій.

Область текстових коментарів може містити будь-яку текстову інформацію, яка пояснює роботу, використовується для забезпечення наочності Maple-документів. Текстові рядки Maple не сприймає і не обробляє. Колір шрифта – чорний.

На рис.8 наведено приклад роботи в Maple: у відповідь на введену команду **solve(2*x=5);** отримано результат $\frac{5}{2}$; відсутність знаку ; або : призводить до помилки:

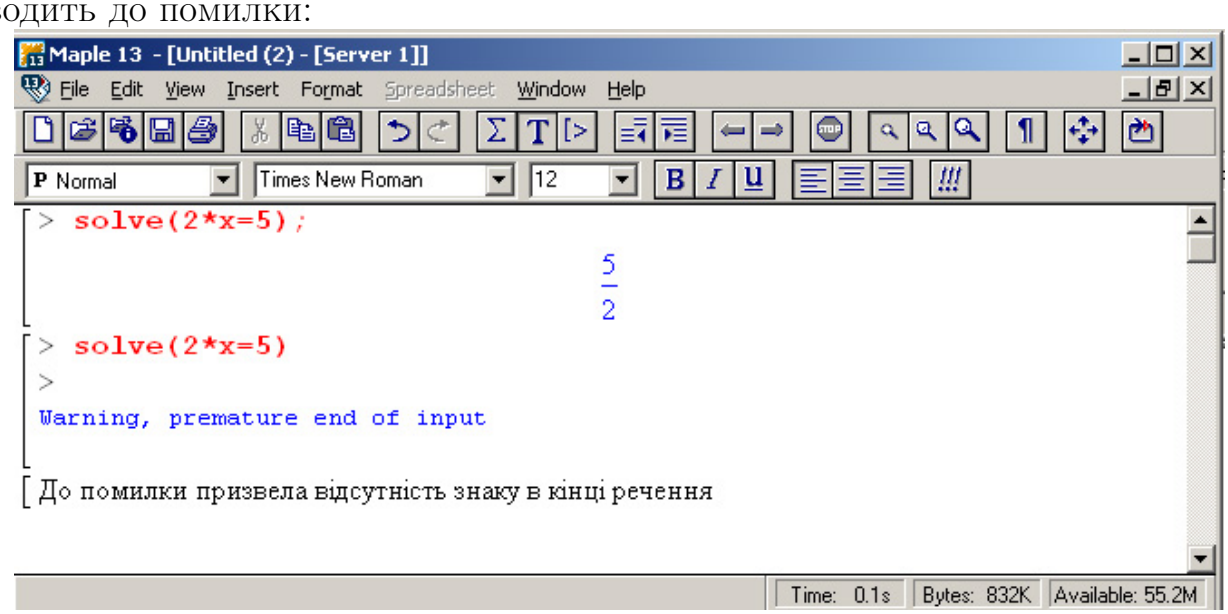


Рис.8

Для переходу до області текстових коментарів треба на Панелі інструментів натиснути кнопку  . Щоб повернутись назад до командного режиму, треба натиснути кнопку  .

4. Maple-мова

Кожна розмовна мова містить такі основні елементи як символи, слова, словосполучення і речення. Мова програмування Maple (Maple-мова)

також має аналогічні структурні елементи. Описати мову означає описати всі її структурні елементи. При цьому опис символів полягає в перерахуванні допустимих символів мови, під описом слів, словосполучень і речень розуміють правила їхнього утворення. Опис кожного елемента мови задається його синтаксисом і семантикою. Синтаксис – це правила побудови елементів мови, семантика – смисл і правила використання елементів мови.

Синтаксис Maple-мови схожий на синтаксис таких відомих мов програмування як C, FORTRAN, BASIC і PASCAL. Тому користувачу, який знайомий із цими мовами і з програмуванням взагалі, нескладно освоїти і Maple-мову.

Алфавіт Maple-мови

Символи мови – це елементарні знаки, які використовуються для запису слів. Набір всіх символів називають алфавітом мови.

Алфавіт Maple-мови містить 26 малих і 26 великих букв латинського алфавіту, 10 арабських цифр (від 0 до 9), 32 спеціальні символи (арифметичні оператори +,-,*,/, знак піднесення до степеня ^та ін.)

Для введення символів використовують клавіатуру і палітри (**View/Pallettes**). Відмітимо, що вигляд виразу може залежати від режиму. Наприклад, в режимі введення вираз e^x матиме запис **exp(x)**, а в режимі виведення на екрані відобразиться $\mathbf{e^x}$.

Серед спеціальних символів виділимо наступні:

- знаки пунктуації: *одиночні* : і ; і *парні* (круглі дужки (і) для групування слів у виразах, кутові дужки < і > для певного групування виразів, фігурні дужки { і } для позначення даних типу *множина*, квадратні дужки [і] для позначення даних типу *список*, подвійні лапки "для позначення даних типу *рядок*);

- знак % – системна змінна, що зберігає результат попередньої операції;

- знак # – вказівник програмного коментаря (Коментар – це текст, розміщений в рядку справа від даного знаку, призначений для внесення пояснень до тексту. Наявність коментарів робить записи зрозумілішими. Коментарі ігноруються системою і не впливають на її роботу. Для запису коментаря можна використовувати будь-які символи із клавіатури, зокрема букви кирилиці);

- знак \ (backslash) має декілька значень в залежності від контексту.

Із окремих символів утворюються слова, що мають певний смисл. Між словами ставлять пропуск або знак пунктуації. Якщо між словами стоїть знак пунктуації, то пропуск можна ставити і до, і після знака пунктуації, а можна взагалі не ставити. Між словами дозволяється ставити декілька пропусків. Всередині слів пропуски ставити не можна!

Пропуски також не можна ставити всередині таких комбінацій символів: := (оператор присвоювання), :: (вказівник типу змінної), <>, <=, >= (знаки $\neq$, $\leqslant$, $\geqslant$ відповідно).

Слова в Maple

Слова – це мінімальні одиниці мови, що мають самостійне значення. В залежності від призначення слова поділяються на: ключові слова, ідентифікатори (імена), оператори, рядки і натуральні числа.

Ключові слова – зарезервовані вирази, які мають фіксоване значення: використовуються для конструювання умовних виразів (if, fi, elif, else, then), циклічних конструкцій (do, by, od, while, to, for, from, in), процедур (description, global, local, proc, option, end) або команди керування (done, quit, stop, return, export, use, try та ін.).

Ідентифікатор – це ім'я об'єкта (константи, змінної, типу, команди, процедури, функції). В Maple-мові розглядають два види імен: стандартні і створені користувачем. Стандартні ідентифікатори – імена, які використовуються для математичних функцій (такі як **sin** і **cos**), вбудованих Maple-команд (наприклад, **expand**, **simplify**), для назв типів (**integer**, **list**). Користувач може створювати нові ідентифікатори, при цьому:

- не можна використовувати ключові слова і стандартні ідентифікатори (наприклад, не можна позначити змінну іменем **begin**); імена бібліотечних Maple-команд використовувати можна, але не бажано, оскільки відповідна команда перестає працювати;
- в якості ідентифікатора можна використовувати будь-яку послідовність символів латинського алфавіту, цифр і знаків підкреслення _), довжина якої не перевищує 524275 символів;
- ідентифікатор не може містити пропуски і спеціальні символи алфавіту (зокрема, знаки пунктуації);
- ідентифікатор повинен починатись або із букви, або із символа підкреслення (ідентифікатори, що починаються із знаку підкреслення, використовуються для ідентифікації глобальних змінних).

Важливо відмітити, що система Maple чутлива до регістру, тобто ідентифікатори NaMe, NAME, name і namE всі будуть сприйняті як різні ідентифі-

катори. Наприклад, для того, щоб розкрити дужки у виразі $(x+2)(x-1)$, треба ввести наступне:

```
> expand((x+2)*(x-1));
```

$$x^2 + x - 2$$

Запис команди великими літерами призводить до такого результату.

```
> EXPAND((x+2)*(x-1));
```

$$\mathrm{EXPAND}((x+2)\,(x-1))$$

Ідентифікатор намагаються підбирати в такий спосіб, щоб він відображав суть об'єкта. Наприклад, для позначення дати краще використати ідентифікатор Date, ніж просто букву D. Для більш зручного читання доцільно використовувати різні регістри: наприклад, для позначення кореня рівняння замість equationroot використати ідентифікатор EquationRoot, відділивши прописними буквами смислові частини.

Оператори – знаки або комбінації знаків, які використовуються для позначення операцій над даними (операндами). Операнди можуть бути числами, константами, змінними, виразами. Наприклад, у виразі (2+4)-5 є 2 оператори: + і -. Для оператора + операндами є числа 2 і 4, для оператора - операндами є вираз (2+4) і константа 5.

В математичних виразах оператори мають стандартний пріоритет (тобто порядок виконання операцій стандартний). Останніми виконуються операції додавання і віднімання. Більш високий пріоритет мають операції множення і ділення, потім операція піднесення до степеня, логічні операції і т.д. Для зміни порядку використовуються круглі дужки: вираз в дужках, незалежно від пріоритету операторів, що входять до його складу, виконується в першу чергу:

```
> 2+3/5;
```

$$\frac{13}{5}$$

```
> (2+3)/5;
```

$$1$$

В залежності від кількості операндів оператори поділяються на: бінарні, унарні та нульарні.

Бінарні оператори мають 2 операнди, які зазвичай розміщені по обидва боки від оператора. Основні з них представлено в наступній таблиці:

Оператор	Смислове навантаження	Оператор	Смислове навантаження
+	додавання	<	менше ніж
-	віднімання	>	більше ніж
*	множення	<=	менше ніж або дорівнює
/	ділення	>=	більше ніж або дорівнює
** або ^	піднесення до степеня	=	дорівнює
mod	остача від ділення	<>	не дорівнює
:=	присвоєння	::	означення типу
$	оператор послідовності	->	функціональний оператор
@	оператор композиції	and,or,...	логічні оператори і, або, ...

Розглянемо приклади:

```
> 3+4;
```

$$7$$

```
> 2^3;
```

$$8$$

```
> 8 mod 3;
```

$$2$$

```
> x@x;
```

$$x^{(2)}$$

```
> (sin@cos)(x);
```

$$\sin(\cos(x))$$

```
> x$3;
```

$$x,\ x,\ x$$

Важливо, розуміти різницю між операторами = і :=. Оператор присвоєння := використовується для надання змінним конкретних значень. Наприклад, запис `a:=3` означає, що змінній a надано значення 3. В подальших обчисленнях замість числа 3 можна використовувати змінну a:

```
> a:=3;
```

$$a := 3$$

```
> 2+a;
```

$$5$$

Оператор рівності = використовується для запису рівнянь, логічних умов (див. далі про логічні оператори), для задання параметрів команд (наприклад, color="Chocolate"для задання шоколадного кольору ліній графіка). Він не надає значень змінним:

```
> a=3;
```

$$a = 3$$

```
> 2+a;
```

$$2 + a$$

Унарні оператори мають 1 операнд. Вони можуть бути префіксними (стояти перед операндом) і постфіксними (стояти після операнда). Всього є 7 унарних операторів:

Оператор	Смислове навантаження
+	унарний плюс (префіксний)
-	унарний мінус (префіксний)
!	факторіал (постфіксний)
not	логічне заперечення (префіксний)
.	десяткова крапка (префіксний або потсфіксний)
$	оператор посідовності (префіксний)
&string	нейтральний оператор

Приклади застосування операторів:

```
> +3;
```

$$3$$

```
> -2;
```

$$-2$$

```
> 25!;
```

$$15511210043330985984000000$$

```
> $2..6;
```

$$2,\ 3,\ 4,\ 5,\ 6$$

```
> .234;
```

$$0.234$$

Нульарними операторами є: %, %%, %%% (1, 2, 3 знаки відсотка). Оператор % забезпечує підстановку в рядку введення останнього обчисленого результату, оператор %% – передостаннього, а оператор %%% – передпередостаннього. Наприклад, обчислимо значення виразу $(\frac{2}{3}+\frac{7}{49})\cdot 21$ послідовно:

```
> 2/3+7/49;
```

$$\frac{17}{21}$$

Щоб помножити отриманий результат на 21, достатньо ввести наступне:

```
> %*21;
```

$$17$$

Два знаки відсотка, написані поруч, використовуються для виклику передостаннього результату:

```
> 2+3;
```

$$5$$

```
> 4-2;
```

$$2$$

```
> %%;
```

$$5$$

Логічні оператори (або булеві) вказують на зв'язок між величинами. До них відносять бінарні оператори: <, <=, >, >=, =, <>, and, or та унарний оператор not. Конструкції з логічними операторами часто використовуються у програмуванні в комбінації з командою **evalb**, яка повертає значення **true**, якщо твердження істинне (умова виконується), і **false**, якщо хибне (умова не виконується). Якщо система не може визначити, істинним є твердження, чи хибним, то повертається значення FAIL:

```
> evalb(2>3);
```

$$false$$

```
> evalb(2<3);
```

$$true$$

```
> evalb(2<>3);
```

$$true$$

```
> evalb(2>3 and 2<3);
```

$$false$$

```
> evalb(2>3 or 2<3);
```

$$true$$

Функціональний оператор використовують для реалізації підстановок і для задання функцій користувача. Наприклад, запис x− > x^2 означає, що замість x необхідно підставити x^2.

Користувач має можливість створювати нові оператори із наперед вказаними властивостями. Для цього використовується команда **define(opname, property1, property2, ...)**, де opname – ім'я оператора, property1, property2, ... – властивості. Можна вказати наступні властивості: unary (унарний), binary (бінарний), diff (оператор диференціювання), linear (лінійний), flat (асоціативний), orderless (комутативний), antisymmetric (антисиметричний), zero (нульовий), identity (одиничний) та ін.

Задамо, наприклад, комутативний оператор f:

```
> define(f,orderless);
```

Перевіримо, чи є рівними результати $f(2,3)$ і $f(3,2)$:

```
> evalb(f(2,3)=f(3,2));
```

$$true$$

Рядок – це деяка послідовність символів, яка записується в подвійних лапках:

```
> "This is рядок";
```

$$\text{“This is рядок”}$$

Рядки використовуються для створення текстових коментарів, імен змінних і символьних виразів. В рядках можна використовувати будь-які символи (зокрема і букви кирилиці, але гарантії в правильності обробки таких символів немає: все ж таки Maple – англомовна програма і має обмежену підтримку інших мов).

До рядка може входити будь-який математичний вираз, його значення не обчислюється:

```
> "2+3";
```

$$\text{“2+3”}$$

Дуже важливо, не плутати подвійні лапки із одинарними: подвійні лапки "використовуються для запису рядків, ліва одинарна лапка ‘ для ідентифікаторів (вираз, обмежений лівими одинарними лапками з двох боків сприймається як один символ), права одинарна лапка ’ (апостроф) – щоб вираз не було обчислено. Розглянемо приклади: введемо змінну ‘one symbol‘, значення якої 3.

```
> ‘one symbol‘:=3;
```

$$one\ symbol := 3$$

```
> 5+‘one symbol‘;
```

$$8$$

Використання апострофів в такому випадку призводить до помилки:

```
> ’one symbol’:=3;
```

```
Error, missing operator or ‘;‘
```

Рядку присвоїти значення також не можна:

```
> "one symbol":=3;
```

```
Error, invalid left hand side of assignment
```

Апостроф використовується, якщо необхідно записати вираз із змінною, якій раніше було надано певного значення:

```
> a:=1; 2+’a’;
```

$$a := 1$$

$$2 + a$$

```
> a:=1; 2+a;
```

$$a := 1$$

$$3$$

Натуральне число в Maple – це слово із десяткових цифр:

```
> 00123456789012;
```

$$123456789012$$

5. Типи даних

Для обробки даних на ЕОМ дуже важливою є класифікація їх за типом. Тип визначає: спосіб внутрішнього представлення об'єкту, тобто обсяг пам'яті, необхідний для зберігання даного об'єкту, множину значень, яких може набувати об'єкт, і операції, які можна виконувати над об'єктом. Наприклад, над числами типу real (дійсні) можна виконувати операції +, -, * і /, але не можна виконувати операцію mod, яка застосовна до чисел типу integer (цілі).

Типи бувають прості і структуровані.

Прості типи даних

В Maple розглядають наступні основні типи *числових* даних: integer (ціле), rational (раціональне), fraction (дріб), float (число з плаваючою комою) і complex (комплексне). Щоб визначити тип числа a, використовують команду **whattype(a)**:

```
> whattype(32);
```

integer

```
> whattype(1/5);
```

fraction

Число a має тип fraction, якщо воно належить до типу rational, але не належить до типу integer.

```
> whattype(0.2);
```

float

Під числом типу integer розуміють будь-яку послідовність десяткових цифр із знаками + або - на початку (знак + можна не ставити). Якщо в правому кінці числа типу integer поставити знак десяткової крапки, то система сприйматиме запис як число типу float.

```
> whattype(32.);
```

float

Відмітимо, що для відокремлення цілої частини від дробової при введенні числа типу float використовується крапка (а не кома!).

Для переведення числа a в інший тип t використовують команду **convert(a,t)**:

```
> convert(1/5,float);
```

$$0.2000000000$$

```
> convert(0.2,fraction);
```

$$\frac{1}{5}$$

```
> convert(0.2,integer);
```

```
Error, unrecognized conversion
```

Число 0,2 не є цілим, тому система повідомила про помилку.

Для переведення числа a в тип float можна також використовувати команду **evalf(a)**:

```
> evalf(1/5);
```

$$0.2000000000$$

```
> evalf(1/3);
```

$$0.3333333333$$

Кількістю десяткових цифр можна управляти, задаючи значення системної змінної Digits:

```
> Digits:=4: evalf(1/3);
```

$$0.3333$$

За замовчуванням Digits дорівнює 10.

Як бачимо, для запису раціонального числа можливі декілька варіантів: у вигляді звичайного дробу із використанням оператора ділення, наприклад: **15/36** (тип fraction); у вигляді десяткового дробу, наприклад: **5.3** (тип float); крім того, можливий запис в показниковій формі, наприклад, запис

```
> 2,67213*10^(-5)
```

означає $2,67213 * 10^{-5}$. Вибір форми запису визначається із урахуванням операцій і команд, які будуть використовувати введене число.

Комплексне число $z = a + bi$, $a, b \in \mathbb{R}$, записується у вигляді z:=a+b*I (уявну одиницю i позначають через I):

```
> 2+3*I;
```

$$2 + 3\,I$$

```
> (3+4*I)+(2-3*I);
```

$$5 + I$$

Результат операції над числами можна отримати із будь-якою необхідною кількістю точних цифр:

```
> 25!;
```

$$15511210043330985984000000$$

```
> 2012!/2000!;
```

$$42585549549920231315554292243155727616 00$$

```
> 2^100-2^99;
```

$$633825300114114700748351602688$$

Однак якщо у виразі зутрічаються дані різних типів, то ця властивість може бути втрачена:

```
> 2^100-2^99.;
```

$$0.6342\,10^{30}$$

В цьому випадку показник степеня було задано як число типу float, тому в результаті отримано також число типу float.

Розробники системи Maple стверджують, що, в принципі, можливі обчислення із мільйоном точних цифр, на практиці така точність майже не потрібна.

Структуровані типи даних

До структурованих типів даних відносять послідовності, списки, множини, масиви і таблиці.

Послідовність (exprseq, від.англ. sequence of expressions) – декілька Maple-виразів, записаних через кому.

Найпростіший спосіб задати послідовність – просто ввести всі її елементи:

```
> a:=1,3,7;
```

$$a := 1,\ 3,\ 7$$

```
> b:=Monday, Tuesday, Wednesday, Thursday, Friday, Saturday,
Sunday;
```

$$b := \mathit{Monday},\ \mathit{Tuesday},\ \mathit{Wednesday},\ \mathit{Thursday},\ \mathit{Friday},\ \mathit{Saturday},\ \mathit{Sunday}$$

Важливою особливістю даного типу є те, що якщо елементи послідовності, в свою чергу, самі є послідовностями, то результатом є єдина послідовність:

```
> a:=1,2,3: b:=x,y,z:  c:=2,4:
  d:=a,4,5,6,b,c;
```

$$d := 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ x,\ y,\ z,\ 2,\ 4$$

Є ще два способи створення послідовностей:

а) використовують оператор послідовності $ (один або разом із оператором діапазона ..):

```
> a$5;
```

$$a,\ a,\ a,\ a,\ a$$

```
> $4..10;
```

$$4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10$$

```
> x[i]$i=3..7;
```

$$x_3,\ x_4,\ x_5,\ x_6,\ x_7$$

```
> 2*i$i=1..4;
```

$$2,\ 4,\ 6,\ 8$$

```
> f(x)$x=5..13;
```

$$f(5),\ f(6),\ f(7),\ f(8),\ f(9),\ f(10),\ f(11),\ f(12),\ f(13)$$

б) використовують команду seq:

```
> seq(i,i=4..10);
```

$$4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10$$

```
> seq(x[i],i=3..7);
```

$$x_3,\ x_4,\ x_5,\ x_6,\ x_7$$

```
> seq(2*i,i=1..4);
```

$$2,\ 4,\ 6,\ 8$$

```
> seq(f(x),x=5..13);
```

$$f(5),\ f(6),\ f(7),\ f(8),\ f(9),\ f(10),\ f(11),\ f(12),\ f(13)$$

Команда **seq** працює швидше.

Список (list) – впорядкована сукупність виразів. Задається у вигляді **[a1,a2,...,an]**, де ai – будь-який Maple-вираз.

Довжина списку – кількість його елементів. Її можна знайти за допомогою команди nops:

```
> d:=[1,3,7,9];
```

$$d := [1,\ 3,\ 7,\ 9]$$

```
> nops(d);
```

$$4$$

Два списки [a1,a2,...,am] і [b1,b2,...,bn] вважаються рівними, якщо вони мають рівні довжини ($m = n$) і рівні відповідні елементи ($a_i = b_i$ для всіх $= 1, 2, ..., n$).

```
> a:=[1,2]; b:=[3-2,2];
```

$$a := [1,\ 2]$$
$$b := [1,\ 2]$$

```
> evalb(a=b);
```

$$true$$

Отримати i-ий елемент списку c:=[a1,a2,...,an] можна, ввівши **c[i]**:

```
> c:=[2,3,5,7,11];
```

$$c := [2,\ 3,\ 5,\ 7,\ 11]$$

```
> c[2];
```

$$3$$

Заміна i-го елемента списку c виконується через присвоєння елементу c[i] нового значення:

```
> c[4]:=6;
```

$$c_4 := 6$$

Тепер список c виглядатиме наступним чином:

```
> c;
```

$$[2,\ 3,\ 5,\ 6,\ 11]$$

Для видалення i-го елемента необхідно ввести subsop(i=NULL,c)

```
> subsop(4=NULL,c);
```

$$[2,\ 3,\ 5,\ 11]$$

Множина (set) – невпорядкована сукупність виразів. Задається у вигляді **{a1,a2,...,an}**, де ai – будь-який Maple-вираз:

```
> m:={2,3,5,7,11};
```

$$m := \{2,\ 3,\ 5,\ 7,\ 11\}$$

```
> {a,23,book};
```

$$\{23,\ a,\ book\}$$

Елементи, які повторюються, не записуються:

```
> {2,1,3,1,4,1};
```

$$\{1,\ 2,\ 3,\ 4\}$$

```
> {50/2,5^2,25};
```

$$\{25\}$$

Як видно із прикладів, порядок, в якому Maple сприймає елементи множини, не завжди збігається із порядком, в якому користувач їх вводить (числа записуються в порядку зростання, а символи і рядки в алфавітному порядку).

Кількість елементів скінченної множини та i-ий елемент множини (для порядку елементів, в якому множину було сприйнято системою) можна отримати аналогічно як і для наборів:

```
> m:={2,5,7,1,8,3};
```

$$m := \{1, 2, 3, 5, 7, 8\}$$

```
> nops(m);
```

$$6$$

```
> m[4];
```

$$5$$

Maple підтримує ряд операцій над множинами: об'єднання (**union**), різниця (**minus**) і перетин (**intersect**) множин, наприклад:

```
> a:={2,3,4,5}: b:={2,3,6,7}:
> a union b;
```

$$\{2, 3, 4, 5, 6, 7\}$$

```
> a minus b;
```

$$\{4, 5\}$$

```
> a intersect b;
```

$$\{2, 3\}$$

Порожня множина задається у вигляді:

```
> {};
```

$$\{\}$$

```
> nops({});
```

$$0$$

Масив (array) – сукупність елементів одного типу даних, впорядкованих за індексами (наборами індексів), які визначають положення елемента в масиві. Масив може бути одновимірним (один індекс) та багатовимірним (набір індексів).

Загальний формат масиву наступний: **array(prop,dim,datas)**, де prop – певна властивість масиву (наприклад, властивість symmetric бути симетричним відносно головної діагоналі), dim – розмірність, яка задається у вигляді діапазонів за кожним із індексів, datas – дані (елементи масиву).

Найчастіше використовуються такі формати:

array(a..b,s1) – для задання одновимірного списку з індексами від a до b і елементами, що задаються за допомогою s1;

array(a..b,c..d,s2) – для задання двовимірного списку з номерами рядків від a до b, номерами стовпців від c до d і елементами, що задаються за

допомогою списку списків s2.

Наприклад, задамо двовимірний масив, в якому 3 рядки і 2 стовпці. Елементи масиву вводяться у вигляді списку списків: кожний рядок є списком, масив є списком, елементами якого є списки-рядки:

```
> m:=array(1..3,1..2,[[a,b],[c,d],[e,f]]);
```

$$m := \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix}$$

Щоб отримати елемент масиву, вказують набір індексів, який відповідає даному елементу. Викличемо елемент, що міститься в 2-му рядку, 1-му стовпці:

```
> m[2,1];
```

$$c$$

Якщо елементи масиву початково не задано, то їх можна задати за допомогою оператора присвоєння :=. Щоб вивести на екран масив, необхідно застосувати команду **print** (взагалі, дана команда використовується для виведення на екран результату певної дії). Наприклад, створимо двовимірний масив C, в якому 3 рядки і 2 стовпці, і заповнимо його поелементно:

```
> C:=array(1..3,1..2);
```

$$C := \mathrm{array}(1..3,\ 1..2,\ [])$$

```
> C[1,1]:=a: C[1,2]:=b: C[2,1]:=m: C[2,2]:=n:
  C[3,1]:=u:
  C[3,2]:=v:
> print(C);
```

$$\begin{bmatrix} a & b \\ m & n \\ u & v \end{bmatrix}$$

Структуру **array** можна використовувати для задання векторів і матриць. Вектор задається як одновимірний масив, матриця як двовимірний масив; нумерація їхніх рядків і стовпців повинна здійснюватись, починаючи з одиниці. В попередньому прикладі якраз і було задано матрицю розмірності 3×2. Задамо вектор-рядок:

```
> r:=array(1..4,[2,5,7,9]);
```

$$r := [2,\ 5,\ 7,\ 9]$$

Для векторів і матриць є й інші способи задання. Для створення матриць можна використовувати функцію-конструктор матриці **Matrix(r, c, init, ro, sym, sc, sh, st, o, dt, f, a)** з набором необов'язкових параметрів.

```
> m:=Matrix(3,2,[[a,b],[c,d],[e,f]]);
```

$$m := \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix}$$

Аналогічно для створення векторів існує конструктор вектора **Vector[o](d, init, ro, sh, st, dt, f, a, o)**:

```
> r:=Vector[row]([2,5,7,9]);
```

$$r := [2,\ 5,\ 7,\ 9]$$

Вектори і матриці можна також задавати за допомогою кутових дужок:

```
> r:=<2,5,7,9>;
```

$$r := \begin{bmatrix} 2 \\ 5 \\ 7 \\ 9 \end{bmatrix}$$

Спосіб задання вектора і матриці залежить від того, які дії необхідно буде виконувати над даними об'єктами. Наприклад, для того, щоб застосовувати команди пакету LinearAlgebra, необхідно, щоб дані об'єкти було задано за допомогою функцій Vector і Matrix відповідно.

6. Змінні і константи

Константи – це найпростіші іменовані об'єкти, що мають наперед визначені значення (числові чи символьні). Числова константа – це число будь-якого із числових типів. Наприклад, у виразі 5-cos(1.23) числа 5 і 1.23 є константами: 5 – типу integer, 1.23 – типу float. В Maple є ряд вбудованих констант, їхній перелік можна отримати ввівши команду constants:

Pi	число $\pi = 3,1415928535...$
I	уявна одиниця i
infinity	∞
true, false, FAIL	логічні константи

Імена вбудованих констант захищені атрибутом protected, тому ці імена не можна використовувати в якості нових ідентифікаторів:

```
> Pi;
```

$$\pi$$

```
> Pi:=1;
```

```
Error, attempting to assign to `Pi` which is protected
```

Користувач має можливість створювати власні константи і вводити їх до списку констант:

```
> type(M,constant);
```

$$false$$

```
> constants:=constants,M;
```

$$constants := false,\ \gamma,\ \infty,\ true,\ Catalan,\ FAIL,\ \pi,\ g,\ M$$

```
> type(M,constant);
```

$$true$$

M не належить до числа вбудованих констант, тому на запит, чи має M тип constant спочатку система дає негативну відповідь, коли ж до списку констант її було додано, відповідь позитивна.

Змінні – це об'єкти, значення яких може змінюватись в процесі виконання документа. Змінні бувають глобальні (доступні для модифікації значень в будь-якому місці документа) і локальні (використовуються при описі процедур, заданні функцій, див. §7). Тип змінної визначається за тим значенням, яке було їй присвоєно (наприклад, integer, rational, float, complex,string, symbol та ін).

Якщо змінній не надано конкретного значення, вважається, що вона має тип symbol. Після того, як їй буде присвоєне певне значення, вона може змінити тип:

```
> whattype(x);
```

$$symbol$$

```
> x:=2;
```

$$x := 2$$

```
> whattype(x);
```

$$integer$$

```
> x:=2.5;
```

$$x := 2.5$$

```
> whattype(x);
```

$$float$$

Щоб явно вказати тип змінної, використовують конструкцію `name::type`, де name – ім'я (ідентифікатор) змінної, type – тип змінної. Наприклад, запис a::integer означає, що змінна a може набувати лише цілочисельних значень.

Система пам'ятає лише останнє присвоєне змінній значення. Наприклад, якщо спочатку змінній присвоїти значення 5, а потім 7, то в подальших обчисленнях використовуватиметься лише 7:

```
> x:=5;
```

$$x := 5$$

```
> x:=7;
```

$$x := 7$$

```
> x^2+1;
```

$$50$$

Якщо змінну, якій було надано конкретного значення, необхідно використати як невизначену змінну, то необхідно відмінити присвоєння. Розглянемо приклад:

```
> x:=2;
```

$$x := 2$$

```
> diff(x^3,x);

Error, invalid input: diff received 2, which is not valid for its
2nd argument
```

Похідну функції знайти не вдалось, оскільки x – визначена (має значення 2), а аргументом команди **diff** має бути невизначена змінна. Щоб відмінити присвоєння, необхідно ввести:

```
> x:='x';
```

$$x := x$$

(використовується знак апострофа '). Тепер можна знаходити похідну:

```
> diff(x^3,x);
```

$$3\,x^2$$

Щоб відмінити присвоєння значень одночасно всім змінним, які використовувались в ході сесії, використовують команду restart.

```
> x:=2;
```

$$x := 2$$

```
> x^3;
```

$$8$$

```
> restart;
> x^3;
```

$$x^3$$

Відмітимо, що Maple зберігає в пам'яті всі присвоєння, які було зроблено протягом Maple-сесії (з часу запуску програми), навіть якщо робота проводилась в декількох документах. Тому результати обчислень можуть залежати від присвоювань в інших документах. Щоб уникнути цього, при переході до розв'язування нового завдання доцільно використовувати команду restart.

7. Maple-команди

Синтаксис команд

Важливим поняттям системи Maple є поняття команди. Команда повертає результат деякого перетворення вхідних даних (аргументів команди) за певним правилом (представленим у вигляді функції або процедури).

Стандартна команда Maple задається за допомогою свого ідентифікатора (імені) command і послідовності параметрів: p1,p2,...,pn, які вказуються в круглих дужках: **command(p1, p2, ...,pn)**. Якщо Maple-команду введено без помилок, Maple проводить обчислення і переводить курсор на наступний командний рядок робочого листа (створює цей рядок, якщо його немає). В кінці кожної команди необхідно ставити знак ; або :.

Наприклад, щоб розв'язати рівняння $x^2 - 5x + 6 = 0$, треба застосувати команду **solve(eq,var)**, параметрами якої є рівняння eq і змінна var відносно якої треба розв'язати рівняння. Для цього вводимо:

```
> solve(x^2-5*x+6=0,x);
```

$$3,\ 2$$

Отже, розв'язками заданого рівняння є числа 3 і 2. Якщо ввести попередню команду із знаком ": одержимо наступне:

```
> solve(x^2-5*x+6=0,x):
```

Незважаючи на те, що результат не з'явився на екрані, обчислення було проведено і результат запам'ятовано. Така форма запису дуже зручна при проведенні проміжних обчислень (хоча краще все ж таки ставити знак ; оскільки це дає змогу вчасно проконтролювати правильність введення команд).

Якщо в кінці Maple-команди не поставити знаки ; або : то Maple не виконує команду і на екрані з'являється попереджувальне повідомлення:

```
> solve(x^2-5*x+6=0,x)

Warning, premature end of input
```

(Увага, незакінчене твердження)

В якості параметрів команд можуть виступати константи, змінні, послідовності, списки, множини і набори; існують команди, що не мають жодного параметра. Параметром команди може бути інша команда, наприклад:

```
> ifactor(sqrt(36));
```

(2) (3)

Спочатку команда sqrt повертає результат $\sqrt{36} = 6$, а потім команда ifactor повертає канонічний розклад натурального числа 6.

Деякі команди мають обмеження на тип даних, що використовуються в якості параметрів. Наприклад, при спробі застосувати команду ifactor до числа 2,3 отримуємо повідомлення про помилку:

```
> ifactor(2.3);
```

```
Error, (in ifactor) invalid arguments
```

Тип даних для кожного параметра окремо зазначається при описі команди.

Порядок параметрів також важливий, наприклад, при зміні параметрів в команді solve отримаємо:

```
> solve(x,x^2-5*x+6=0);
```

```
Error, invalid input: too many and/or wrong type of arguments passed
to solve; first unused argument is x^2-5*x+6 = 0
```

Команда може мати окрім обов'язкових параметрів, ще й необов'язкові.

Як уже зазначалось, в Maple є понад 3,5 тисячі команд, що зберігаються в ядрі Maple, основній бібліотеці і тематичних пакетах. Назви команд було вибрано в такий спосіб, щоб вони якнайвлучніше відображали суть дії і водночас були якомога короткими. Наприклад, команда **sqrt(a)**, яка для заданого параметра **a** повертає значення квадратного кореня із **a**, походить від англійського словосполучення square root (квадратний корінь). Більшість назв команд записується за допомогою малих букв, але деякі команди мають аналоги, які починаються із великої букви. Оскільки Maple чутлива до регістру, то слід звертати увагу не лише на правильність запису послідовності введених символів, але й на регістр.

Виклик команд

Виклик команди залежить від того, чи належить вона до ядра, чи до основної бібліотеки, чи до спеціалізованого пакету. Команди ядра і основної бібліотеки завантажуються автоматично. Якщо ж при виклику деякої команди із основної бібліотеки в рядку виведення просто повторюється

введений запис, а сама команда не виконується, то це означає, що в імені команди допущено помилку. Наприклад,

```
> ifaktor(36);
```

ifaktor(36)

В такому випадку необхідно перевірити по буквах, чи правильно записано ім'я команди, включаючи відповідність верхнього і нижнього регістрів.

Команди, що містяться в спеціалізованих пакетах (наприклад, пакетах linalg, numtheory), автоматично не завантажуються. Існує 2 способи виклику команди із спеціалізованого пакету.

Спосіб I: завантаження всього пакету package командою **with(package)**. Для виклику команди в такому випадку достатньо ввести її назву та параметри. Наприклад, викличемо команду **divisors(a)** із пакету numtheory, яка для заданого числа a повертає множину всіх натуральних дільників числа a:

```
> divisors(12);
```

divisors(12)

Виклик команди без попереднього завантаження пакету numtheory не призвів до обробки даної команди. Завантажимо пакет і знову викличемо команду:

```
> with(numtheory): divisors(12);
```

$$\{1, 2, 3, 4, 6, 12\}$$

Отже, натуральними дільниками числа 12 є 1,2,3,4,6,12.

Щоб побачити перелік всіх команд пакету package, необхідно в кінці речення with(package) поставити знак ;

```
> with(numtheory);
```

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, *fermat*, *imagunit*, *index*, *integral_basis*, *invcfrac*, *invphi*, *iscyclotomic*, *issqrfree*, *ithrational*, *jacobi*, *kronecker*, λ, *legendre*, *mcombine*, *mersenne*, *migcdex*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*, *nthconver*, *nthdenom*, *nthnumer*, *nthpow*, *order*, *pdexpand*, ϕ, π, *pprimroot*, *primroot*, *quadres*, *rootsunity*, *safeprime*, σ, *sq2factor*, *sum2sqr*, τ, *thue*]

Якщо необхідна лише одна команда пакету або невелика кількість команд, то можна не завантажувати пакет повністю (оскільки це може призвести до надлишкових затрат пам'яті), а завантажити лише конкретну команду (набір команд). Для цього вводимо **with(package,c1,c2,...)**, де package – назва пакету, c1,c2,... – назви команд.

```
> with(numtheory,divisors):
> divisors(12);
```

$$\{1, 2, 3, 4, 6, 12\}$$

Завантажити пакет (або деяку команду із пакету) достатньо один раз протягом поточної Maple-сесії.

Спосіб II: не завантажуючи весь пакет package, команду command можна викликати у форматі **package[command](p1,p2,...,pn)**:

```
> numtheory[divisors](12);
```

$$\{1, 2, 3, 4, 6, 12\}$$

Деякі стандартні Maple-команди

В даному пункті розглянемо лише команди із ядра Maple та основної бібліотеки, які використовуються найчастіше. Багато інших команд, які використовуються при розв'язуванні алгебраїчних задач, буде розглянуто в Розділах II-VIII.

Дії над числами

До складу системи Maple входить графічний калькулятор. Однак обчислення зручно виконувати і в режимі документу. Для арифметичних операцій використовують бінарні оператори +, -, *, / (див. §4). Операція піднесення до степеня a^b записується у вигляді a**b або у вигляді a^ b. Зауважимо, що для арифметичних операцій Maple розпізнає лише круглі дужки, а при спробі використання квадратних або фігурних дужок просто виводить на екран введений вираз:

```
> 2^[3*(1+7)];
```

$$2^{[24]}$$

Але

```
> 2^(3*(1+7));
```

$$16777216$$

Операція добування кореня з комплексного числа z може бути здійснена в декілька способів. Найпростіший випадок – добування квадратного кореня. В такому випадку найзручніше використовувати команду **sqrt(z)**. Нижче наведено результати застосування даної команди до числа 3.

Для отримання точного результату вводимо:

```
> sqrt(3);
```

$$\sqrt{3}$$

```
> sqrt(4);
```

$$2$$

```
> sqrt(12);
```

$$2\sqrt{3}$$

```
> sqrt(-4);
```

$$2\,I$$

```
> sqrt(3+4*I);
```

$$2+I$$

```
> sqrt(4+2*sqrt(3));
```

$$\sqrt{3}+1$$

Щоб одержати наближене значення квадратного кореня з числа 3, його необхідно ввести як число типу float:

```
> sqrt(3.0);
```

$$1.732050808$$

Можна також застосувати команду evalf(z) (при цьому за замовчуванням на екран виводиться 10 знаків.)

```
> evalf(sqrt(3));
```

$$1.732050808$$

Щоб одержати іншу кількість десяткових знаків, необхідно цю кількість додатково вказати. Наприклад, щоб отримати 20 десяткових знаків, вводимо:

```
> evalf(sqrt(3),20);
```

$$1.7320508075688772935$$

У випадку кореня довільного натурального степеня n використовується команда **root(z,n)** або **root[n](z)**.

```
> root(3.0,3);
```

$$1.442249570$$

```
> root[3](3.0);
```

$$1.442249570$$

```
> root(3,3);
```

$$3^{(1/3)}$$

```
> root(8,3);
```

$$2$$

```
> root[3](8);
```

$$2$$

```
> root(24,3);
```

$$2\,3^{(1/3)}$$

```
> root(-8,3);
```

$$2\,(-1)^{(1/3)}$$

```
> root(-8.0,3);
```

$$1.000000000 + 1.732050807\,I$$

```
> root[3](3+4*I);
```

$$(3 + 4\,I)^{(1/3)}$$

```
> root[3](3.0+4.0*I);
```

$$1.628937146 + 0.5201745022\,I$$

Також операцію добування кореня натурального степеня n можна здійснити за допомогою команди **surd(z,n)**. Покажемо відмінність між результатами команд ^, **root**, і **surd**:

```
> (8)^(1/3); root(8, 3); surd(8, 3);
```

$$8^{(1/3)}$$

$$2$$

$$2$$

```
> (8.0)^(1/3); root(8.0, 3); surd(8.0, 3);
```

$$2.000000000$$

$$2.000000000$$

$$2.000000000$$

```
> (-8)^(1/3); root(-8, 3); surd(-8, 3);
```

$$(-8)^{(1/3)}$$

$$2\,(-1)^{(1/3)}$$

$$-2$$

```
> (-8.0)^(1/3); root(-8.0, 3); surd(-8.0, 3);
```

$$1.000000000 + 1.732050807\,I$$

$$1.000000000 + 1.732050807\,I$$

$$-2.000000000$$

Алгебраїчні перетворення

Серед Maple-команд, які використовуються для перетворення алгебраїчних виразів, виділимо наступні:

simplify(expr) – спрощення виразу **expr**;

expand(expr) – розкриття дужок у виразі **expr**;
factor(expr) – розклад на множники виразу **expr**.
Розглянемо приклади:

```
> simplify((x^3-27)/(x^2+3*x+9));
```

$$x - 3$$

```
> expand((x^2+4)*(x-1)*(x+6));
```

$$x^4 + 5\,x^3 - 2\,x^2 + 20\,x - 24$$

Розкладемо отриманий вираз на множники:

```
> factor(%);
```

$$(x^2 + 4)\,(x - 1)\,(x + 6)$$

Для команди **simplify** в якості (необов'язкового) параметру можна вказати додаткову умову (умови), тоді буде відбуватись перетворення лише тих частин виразу, що задовольняють вказану умову. Наприклад, при виклику команди **simplify(expr,ln)** буде відбуватись спрощення лише тих частин виразу, що містять натуральні логарифми. Серед таких додаткових умов: **trig** – для перетворення тригонометричних виразів, **power** – для степеневих перетворень, **radical** (або **sqrt**) – для перетворення радикалів. Використання додаткових параметрів значно підвищує ефективність команди **simplify**.

Скоротити дріб **expr** можна також за допомогою команди **normal(expr)**.

```
> normal((x^3-27)/(x^2+3*x+9));
```

$$x - 3$$

Для зведення подібних доданків у виразі expr використовується команда **collect(expr,var)**, де var – ім'я змінної, відносно якої потрібно зводити подібні доданки.

```
> f := a^3*x-x+a^3+a;
```

$$f := a^3\,x - x + a^3 + a$$

```
> collect(f,x);
```

$$(a^3 - 1)\,x + a^3 + a$$

В Maple є можливість – smart-спосіб – замість того, щоб набирати вручну часто використовувані стандартні команди, використати контекстне меню. Для цього вводимо вираз, виводимо його Maple-результат, виділяємо результат і натискаємо праву клавішу миші. З'являється контекстне меню. Далі вибираємо необхідну команду.

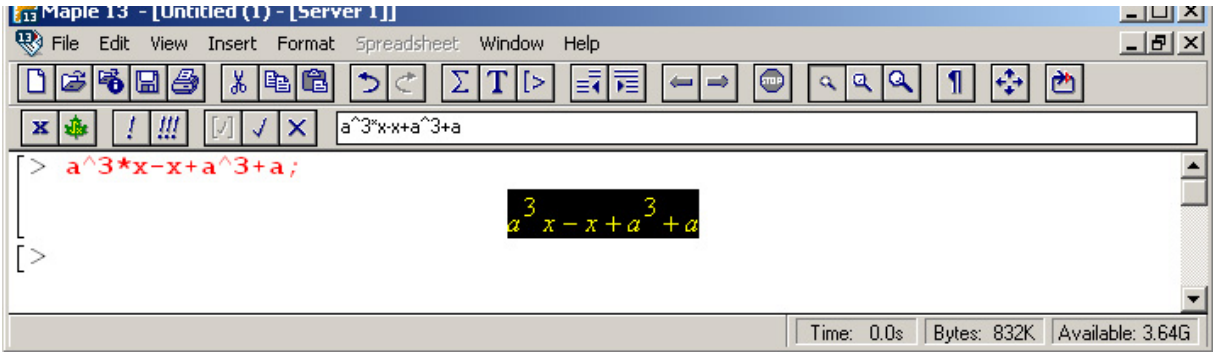


Рис.9

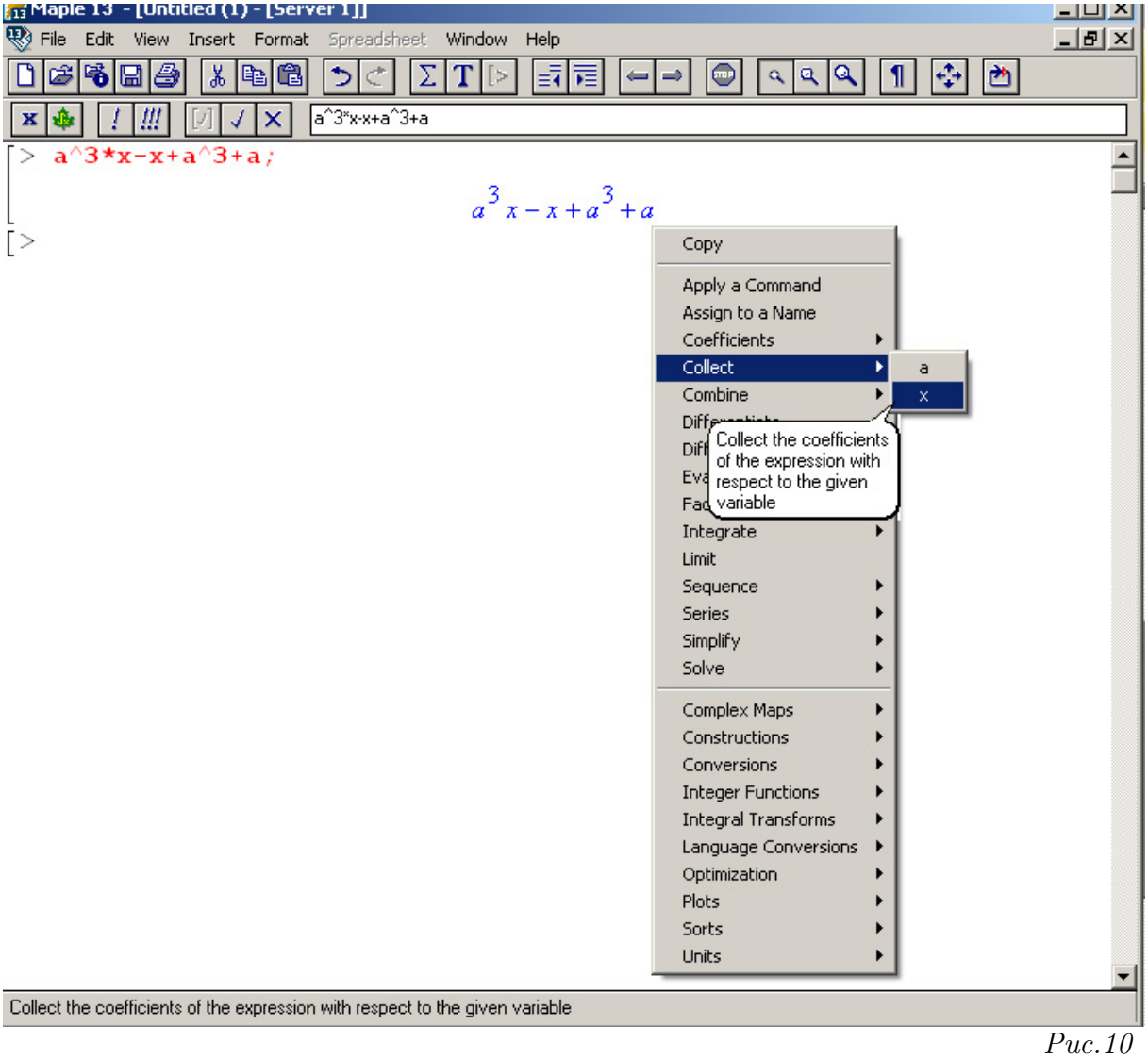


Рис.10

При спрощенні виразу інколи необхідно вказати певні умови, що накладаються на змінні, які входять до складу виразу (наприклад, вказати, яких значень можуть набувати змінні). (Напр., якщо $x \geqslant 0$ при спрощенні виразу $\sqrt{x^2}$ отримаємо x, а якщо $x < 0$, отримаємо $-x$.) Для задання властивості prop змінної v використовується команда **assume(v,prop)**. Розглянемо приклад. Нехай $x > 0$:

```
> assume(x,positive);
```

Тоді при спрощенні виразу $\sqrt{x^2}$ матимемо:

```
> simplify(sqrt(x^2));
```

$$x^{\sim}$$

Знак тільда $\sim$ вказує на особливий статус змінної x (тобто, що змінна задовольняє певні умови). Якщо до переліку попередньо заданих властивостей необхідно додати нові, то використовують команду **additionally(prop2)**. Про властивості змінної x можна дізнатись за допомогою команди **about(x)**:

```
> assume(a,nonpositive);
> additionally(a>=0);
> about(a);
Originally a, renamed a~:

  is assumed to be: 0
```

Спочатку змінну a було задано як таку, що може набувати лише недодатних значень. Потім додатково задано властивість $a \geqslant 0$. В результаті про змінну a відомо, що a може набувати лише значення 0.

Властивість можна задавати за допомогою числового проміжка:

Проміжок	Формат задання
$[a, b]$	RealRange(a, b)
$(-\infty, b]$	RealRange(-infinity, b)
$[a, \infty)$	RealRange(a, infinity)
$(a, b]$	RealRange(Open(a), b)

Для деяких числових проміжків зручно використовувати стандартну назву:

скорочена назва	формат виводу на екран	значення
realcons	AndProp(real,constant)	дійсне число
negative	RealRange(-infinity,Open(0))	від'мне дійсне число
nonnegative	RealRange(0,infinity)	невід'ємне дійсне число
positive	RealRange(Open(0),infinity)	додатне дійсне число
natural	AndProp(integer, RealRange(1,infinity))	натуральне число
posint	AndProp(integer, RealRange(1,infinity))	натуральне число
odd	LinearProp(2,integer,1)	непарне ціле число
even	LinearProp(2,integer,0)	парне ціле число

Для задання властивостей можна використовувати And, Or, Non - конструкції:

AndProp(a, b, ...)	об'єкт володіє і властивістю a, і властивістю b,...
OrProp(a, b, ...)	об'єкт володіє принаймні однією із властивостей a, або b, або ...
Non(a)	об'єкт не володіє властивістю a

Для введення виразу a, що містить радикали, використовують ті ж команди, що й для чисел: **sqrt(a)** і **root(a)**.

```
> sqrt(x);
```

$$\sqrt{x}$$

```
> sqrt(-9*x^2*y);
```

$$3\sqrt{-x^2\,y}$$

Як бачимо, в цьому випадку спрощення виразу не відбувається. Можна ввести додатковий параметр symbolic, тоді отримаємо:

```
> sqrt(-9*x^2*y,symbolic);
```

$$3\,x\sqrt{-y}$$

Отриманий результат не є коректним: правильна відповідь $3|x|\sqrt{-y}$. Тому при спрощенні виразів, що містять радикали, необхідно задавати область допустимих значень змінних:

```
> assume(x>0);
> sqrt(-9*x^2*y);
```

$$3\,x\tilde{}\,\sqrt{-y}$$

```
> assume(x<0);
> sqrt(-9*x^2*y);
```

$$-3\,x\tilde{}\,\sqrt{-y}$$

Аналогічно для команди root:

```
> root[3](x);
```

$$x^{(1/3)}$$

```
> root[3](16*x^3*y);
```

$$2\,2^{(1/3)}\,(x^3\,y)^{(1/3)}$$

```
> root[4](-16*x^4*y);
```

$$2\,(-x^4\,y)^{(1/4)}$$

```
> root[3](16*x^3*y,symbolic);
```

$$2\,x\,2^{(1/3)}\,y^{(1/3)}$$

```
> root[4](-16*x^4*y,symbolic);
```

$$2\,x\,(-y)^{(1/4)}$$

```
> assume(x>0);
> root[3](16*x^3*y);
```

$$2\,x\tilde{}\,2^{(1/3)}\,y^{(1/3)}$$

```
> root[4](-16*x^4*y);
```

$$2\,x\tilde{}\,(-y)^{(1/4)}$$

Розв'язування рівнянь

Для розв'язування рівнянь в Maple використовується команда **solve(eq,x)**, де x – невідоме, відносно якого необхідно розв'язати рівняння eq. В результаті виконання команди в рядку виведення з'являться розв'язок.

```
> solve(a+b*x=c,x);
```

$$-\frac{a-c}{b}$$

Якщо рівняння має декілька розв'язків, то вони в рядку виведення записуються через кому:

```
> solve(x^3-5*x^2+4*x=0,x);
```

$$0,\ 4,\ 1$$

Якщо права частина рівняння 0 (тобто рівняння має вигляд $f(x) = 0$), то формат команди можна дещо спростити: залишити лише один параметр – ліву частину $f(x)$.

```
> solve(x^3-5*x^2+4*x);
```

$$0,\ 4,\ 1$$

Команда solve повертає результат у вигляді множини елементів. Якщо цю множину позначити деяким символом (набором символів), наприклад, mnojina:

```
> mnojina:=solve(x^3-5*x^2+4*x);
```

$$mnojina := 0,\ 4,\ 1$$

то до елементів цієї множини можна буде звертатись. Наприклад, щоб одержати третій елемент множини mnojina, треба ввести наступне:

```
> mnojina[3];
```

$$1$$

Команда **solve** використовується і для розв'язування систем рівнянь. В такому випадку вона має формат **solve({eq1,eq2,...},{x,y,...})**, де перший параметр – множина $\{eq1, eq2, ...\}$ рівнянь, другий параметр – множина $\{x, y, ...\}$ невідомих:

```
> solve({x+y=3,x-y=1},{x,y});
```

$$\{x = 2,\ y = 1\}$$

Відмітимо, що в результаті застосування команди solve невідомим значення не присвоюються:

```
> x;
```

$$x$$

```
> y;
```

$$y$$

Для того, щоб x і y набули значень 2 і 1 відповідно, необхідно застосувати команду assign:

```
> assign(solve({x+y=3,x-y=1},{x,y}));
> x;
```

$$2$$

```
> y;
```

$$1$$

8. Елементи програмування

Для розв'язування багатьох алгебраїчних задач в Maple є готові вбудовані команди і функції, однак якою б досконалою не була система, завжди знайдеться багато спеціалізованих задач, які залишились поза увагою розробників. Для розв'язування таких задач необхідно вміти створювати команди і функції. Відмітимо, що мова програмування Maple дуже схожа на традиційні мови програмування.

Задання математичних функцій

Для задання математичних функцій в Maple є декілька способів.

Спосіб I. Задання функції за допомогою оператору присвоєння:

```
> f:=x^3;
```

$$f := x^3$$

В такому випадку стандартний функціональний запис $f(2)$ незрозумілий для Maple.

```
> f(2);
```

$$\mathrm{x}(2)^3$$

Обчислити значення функції f в конкретно заданій точці можна задавши це значення x. Наприклад, щоб обчислити значення функції f із попереднього прикладу в точці $x = 5$, треба записати:

```
> f:=x^3;
```

$$f := x^3$$

```
> x:=5;
```

$$x := 5$$

```
> f;
```

$$125$$

Після виконання цих команд змінна x матиме конкретне задане значення 5. Щоб не надавати змінній x конкретного значення, зручніше використовувати команду підстановки **subs(x1=a1, x2=a2,..., ,f)**, де в фігурних дужках вказуються змінні xi і їхні відповідні значення ai (i=1,2,...). Наприклад,

```
> f:=x^3;
```

$$f := x^3$$

```
> subs({x=5},f);
```

$$125$$

Спосіб II. Задання функції за допомогою функціонального оператора -> (комбінація символів „мінус" і „більше", див. §4). Для задання функції $f(x_1, x_2, ..., x_n) = expr$, яка набору змінних (x1,x2,...,xn) ставить у відповідність вираз expr використовується наступна конструкція: **f:=(x1,x2,...,xn)->expr**. Для функції $f(x) = x^3$ матимемо:

```
> f:=x->x^3;
```

$$f := x \to x^3$$

Перевага такого методу – можливість використання стандартного запису, на зразок $f(2)$, для обчислення значення функції в точці.

```
> f(2);
```

$$8$$

Для функції $f(x, y) = x + y$ маємо:

```
> f:=(x,y)->x+y;
```

$$f := (x, y) \to x + y$$

```
> f(2,3);
```

$$5$$

Змінні, вказані в списку формальних параметрів, є локальними (тобто при підстановці на їх місце фактичних параметрів вони зберігають значення лише в тілі функції. За межами цієї функції змінні з цими іменами є або невизначеними, або мають значення, які їм було присвоєно раніше.

```
> f:=(x,y)->x+y;
```

$$f := (x, y) \to x + y$$

```
> f(2,3);
```

$$5$$

```
> x:=0;y:=0;
```

$$x := 0$$
$$y := 0$$

```
> f:=(x,y)->sqrt(x+y);
```

$$f := (x,\, y) \to \sqrt{x+y}$$

```
> f(2,7);
```

$$3$$

```
> x; y;
```

$$0$$
$$0$$

При обчисленні значення функції $f(x, y) = \sqrt{x+y}$ в точці $(2, 7)$ змінним x і y було надано значення 2 і 7 відповідно, але за межами дії функції ці змінні мають нульові значення, які їм було надано спочатку.

Типи програм

За своєю структурою виділяють наступні типи програм: лінійні, розгалужені і циклічні. В лінійних програмах всі дії виконуються строго послідовно одна за одною (наприклад, програма обчислення суми двох матриць однакової розмірності: послідовно знаходимо елементи матриці-суми як суму відповідних елементів матриць доданків).

В розгалужених програмах для конкретних вихідних даних виконуються не всі вказані дії. Але які саме дії необхідно виконувати, визначається в залежності від отриманих в процесі роботи результатів і певних умов. Прикладом такої програми є програма обчислення значення функції в точці, коли функція кусково-задана:

$$f(x) = \begin{cases} -x, & \text{якщо } x \geqslant 0; \\ x+1, & \text{якщо } x < 0. \end{cases}$$

Результат залежить від значення a аргументу. Якщо аргумент невід'ємний, то значення знаходимо за правилом $f(a) = -a$; якщо додатний, то за правилом $f(a) = a + 1$: $f(2) = 2 + 1 = 3$, $f(-4) = -(-4) = 4$.

Циклічною програмою називають таку програму, в якій можна виділити багатократно повторювану послідовність дій (її називають циклом). Для таких програм характерною є наявність параметра циклу. На початку циклу цей параметр має певне значення, яке в ході виконання циклу

змінюється. Цикл завершується, якщо виконується певна умова. Прикладом циклічної програми є програма для відшукання найбільшого спільного дільника за алгоритмом Евкліда: ділення з остачею виконується, поки не отримаємо рівну нулю остачу.

В реальних задачах, як правило, зустрічаються всі 3 типи програм. Розглянемо опис таких програм Maple-мовою.

Умовні речення

Найпростішу конструкцію розгалужених програм в Maple-мові задає оператор умови if, який має наступний синтаксис:

if <умова 1> then <команда 1, команда 2, ...>
|elif <умова 2> then <команда 1′, команда 2′, ...>|
...
|elif <умова n> then <команда n1, команда n2, ...>|
|else <команда k1, команда k2, ...>|
end if;

Вертикальними рисками обмежено необов'язкові елементи даної конструкції. Вираз **end if** вказує на кінець конструкції. На практиці найчастіше використовуються такі дві форми:

if <умова 1> then <команда 1, команда 2, ...> end if: якщо умова 1 задовольняється, то виконуються команда 1, команда 2,..., в іншому випадку нічого не виконується;

if <умова 1> then <команда 1, команда 2, ...> else <команда k1, команда k2, ...> end if: якщо умова 1 задовольняється, то виконуються команда 1, команда 2,..., в іншому випадку виконуються команда k1, команда k2, ...

При заданні умов можна використовувати будь-які логічні вирази, до складу яких входять оператори порівняння >, >=, <, <=, =, <> і логічні оператори and, or, not. Розглянемо наступний приклад:

```
> x:=3:
> if x>0 then print(‘positive‘) end if;
```

positive

```
> x:=-3:
```

В даному прикладі аналізується значення x. У випадку, коли воно додатне, на екран виводиться повідомлення „positive”; якщо x не є додатним, то нічого не виводиться.

Доповнимо конструкцію рядком else:

```
> x:=3:
> if x>0 then print(‘positive‘)
  else print(‘nonpositive‘)
  end if;
```

positive

```
> x:=-3:
> if x>0 then print(‘positive‘)
  else print(‘nonpositive‘)
  end if;
```

nonpositive

Тепер якщо умова $x > 0$ виконується, то виводиться повідомлення „positive”; якщо не виконується, то виводиться повідомлення „nonpositive”.

Для того, щоб зменшити кількість різних **if**-конструкцій, зручно вводити рядок elif. Слово elif розшифровується як else if (тобто „в іншому разі, якщо”). Рядків elif може бути довільна кількість (або не бути жодного). В попередньому прикладі додамо рядок elif (x<0) then print('negative'), який у випадку від'ємного числа x, виводитиме на екран повідомлення „negative”, якщо ж жодна із умов (x<0) і (x>0) не виконується, то виводиться повідомлення „zero”:

```
> x:=3:
> if x>0 then print(‘positive‘)
  elif x<0 then print('negative')
  else print(‘zero‘)
  end if;
```

positive

```
> x:=-3:
> if x>0 then print(‘positive‘)
  elif x<0 then print('negative')
  else print(‘zero‘)
  end if;
```

negative

```
> x:=0:
> if x>0 then print(‘positive‘)
  elif x<0 then print('negative')
  else print(‘zero‘)
  end if;
```

zero

Розглянемо інший приклад. Нехай задано два числа x, y:

```
> x:=2006/2007:
  y:=2007/2008:
```

Потрібно визначити, яке з чисел більше.

```
> if x>y then print(x)
  elif y>x then print(y)
  else print(‘equal‘)
  end if;
```

$$\frac{2007}{2008}$$

Умова (x>y) не є справедливою, але справедлива умова (y>x), тому виконується команда **print(y)**. Якщо ж ввести два рівні числа x і y, то одержимо наступне:

```
> x:=2006/2007: y:=2006/2007:
> if x>y then print(x)
  elif y>x then print(y)
  else print(‘equal‘)
  end if;
```

equal

Циклічні структури

Загальна конструкція циклу в Maple виглядає наступним чином:
| for <name> | | from <expr1> | | by <expr2> | | to <expr3> | | while <expr4>| do <statement sequence> end do;

Тут **name** – ім'я параметру циклу, **expr1**, **expr2** і **expr3** – вирази, що задають початкове значення, кінцеве значення і крок зміни параметру name, **expr4** – вираз, який задає умову, поки цикл (послідовність команд <statement sequence>, розміщена між словами do і end do) буде виконуватись.

В ході виконання циклу значення параметру name змінюється від expr1 до expr3 з кроком expr2. Якщо блок by <expr2> відсутній, то значення параметру змінюється з кроком +1. Розглянемо приклади:

```
> for i from 0 by 2 to 7 do print(i) end do;
```

0
2
4
6

```
> for i from 0 to 7 do print(i) end do;
```

0
1
2

3
4
5
6
7

Допустимим є від'ємний крок:

```
> for i from 6 by -2 to 1 do print(i) end do;
```

6
4
2

Межі зміни значення параметру можна задавати арифметичними виразами:

```
> for i from 3/(1+2) to 3+1 do print(i) end do;
```

1
2
3
4

Перервати цикл можна за допомогою блоку while <expr4>: цикл буде виконуватись до кінця або поки умова expr4 істинна:

```
> for i from 1 to 10 while i<=6 do print(i) end do;
```

1
2
3
4
5
6

Блок for <name> також необов'язковий: цикл може записуватись у спрощеній формі наступним чином:

while <expr> do <statement sequence> end do;

Цикл буде виконуватись, поки умова expr справедлива. Таку форму зручно використовувати, коли наперед невідомо, скільки разів необхідно повторити цикл. Слід відмітити, що застосування такої форми вимагає введення параметру поза межами циклу та зміна його значення всередині циклу вручну. Наприклад, для виведення на екран чисел від 1 до 5 задамо параметр i:

```
> i:=1:
```

Кожне наступне виведене на екран число повинно бути на 1 більше за попереднє, тому всередині циклу необхідно буде збільшувати параметр на 1 (при цьому пишуть i:=i+1). Вихід із циклу здійснюватиметься, коли умова $i \leqslant 5$ не виконуватиметься.

```
> while i<=5 do
print(i);
i:=i+1;
end do;
```

$$1$$
$$i := 2$$
$$2$$
$$i := 3$$
$$3$$
$$i := 4$$
$$4$$
$$i := 5$$
$$5$$
$$i := 6$$

Бачимо: спочатку $i = 1$, умова $i \leqslant 5$ виконується, тому цикл починає роботу: на екран виводиться число 1. Далі параметр i збільшено на 1: $i = 2$, умова $i \leqslant 5$ виконується, тому цикл продовжує роботу: на екран виводиться число 2, параметр збільшується на 1: $i = 3$, умова $i \leqslant 5$ виконується, тому цикл продовжує роботу: на екран виводиться число 3, параметр збільшується на 1: $i = 4$, умова $i \leqslant 5$ виконується, тому цикл продовжує роботу: на екран виводиться число 4, параметр збільшується на 1: $i = 5$, умова $i \leqslant 5$ виконується, тому цикл продовжує роботу: на екран виводиться число 5, параметр збільшується на 1: $i = 6$, умова $i \leqslant 5$ не виконується, тому цикл завершує роботу.

Зауважимо, що якщо забути про необхідність зміни параметру, то умова $i <= 5$ ніколи не настане і циклічні обчислення повторюватимуться нескінченно. В цьому випадку кажуть, що відбулось зациклення програми. Виконання програми в середовищі Maple завжди можна перервати шляхом натиснення кнопки STOP на панелі інструментів.

Інколи зручно використовувати більш специфічну конструкцію циклу:

|for <name>| |in <expr1>| | while <expr2>|
do <statement sequence> end do;

Тут expr1 – список значень, яких буде послідовно набувати параметр циклу name, поки список не буде вичерпано або поки не виконуватиметься умова, задана логічним виразом expr2. Розглянемо приклади:

```
> for i in [1,5,-3,2,7,0] do print(i) end do;
```

$$1$$
$$5$$
$$-3$$
$$2$$
$$7$$
$$0$$

```
> for i in [1,5,-3,2,7,0] while i>0 do print(i) end do;
```

$$1$$
$$5$$

Цикли можуть бути вкладеними (тобто всередині одного циклу може міститись інший). Це зручно використовувати, якщо необхідна зміна декілька параметрів. Наприклад, виведемо послідовно на екран елементи матриці

```
> M:=array(1..3,1..2,[[a,b],[c,d],[e,f]]);
```

$$M := \begin{bmatrix} a & b \\ c & d \\ e & f \end{bmatrix}$$

Кожний елемент матриці M характеризується двома параметрами – індексами: номером рядка і номером стовпця, в яких він розташований. Нехай i – номер рядка, j – номер стовпця. Щоб отримати всі елементи першого рядка, необхідно при $i = 1$ послідовно змінити значення параметра j від 1 до 2, потім, щоб отримати елементи другого рядка, при $i = 2$ послідовно змінюємо значення параметра j від 1 до 2, і аналогічно для третього рядка. Отримаємо два цикли: зовнішній із параметром i та внутрішній із параметром j:

```
> for i from 1 to 3 do
    for j from 1 to 2 do print(M[i,j]) end do;
  end do;
```

$$a$$
$$b$$
$$c$$
$$d$$

$$e$$
$$f$$

В результаті отримано спочатку елементи першого рядка, потім другого і нарешті третього.

Оператори пропуску і переривання циклу. Іноді необхідно пропустити декілька значень параметра циклу. Для цього використовується оператор next. Розглянемо приклад: виведемо на екран всі числа від 1 до 5 за винятком числа 3.

```
> for i from 1 to 5 do
     if i=3 then next else print(i) end if;
  end do;
```

$$1$$
$$2$$
$$4$$
$$5$$

Для того, щоб перервати виконання цикла, використовують оператор break:

```
> for i from 1 to 5 do
     if i=3 then break else print(i); end if;
  end do;
```

$$1$$
$$2$$

Щойно параметр набув значення $i = 3$, відбулось завершення роботи циклу, тому на екран було виведено лише два значення: 1 і 2.

Для переривання циклу (і взагалі програми) можна використовувати також оператори quit, stop і done, але при цьому вікно документу закривається.

Процедури в Maple

Означення процедури. Для розв'язання складної задачі її доцільно розбити на окремі підзадачі, що мають відносно невеликі розміри, невисоку складність. Бажано, щоб алгоритм розв'язування кожної підзадачі складався з одного-декількох кроків. Тоді для кожної підзадачі створюють окрему підпрограму (або ще кажуть процедуру). Такий метод програмування називають модульним або структурним.

В Maple теж є можливість створення процедур. На основі процедур написано бібліотеки Maple, процедури служать засобом розширення можливостей Maple користувачем.

Кожна процедура має своє унікальне ім'я і набір параметрів. Найпростіша форма означення процедури з назвою name має вигляд:

name:=proc(par1,par2,...)
<тіло процедури>
end proc;

Перший рядок – це заголовок процедури. Він містить ключове слово proc, після якого в дужках зазначається послідовність формальних параметрів процедури (ця послідовність може бути і порожньою, тобто мінімально допустимий заголовок proc()). Формальні параметри процедури par1,par2,... – це параметри, які використовуються для її означення/опису/ (імена змінних, які фігурують у виразах із <тіло процедури>. наприклад proc(x), proc(a,b,c) тощо).

<тіло процедури> – послідовність Maple-речень, відокремлених оператором ; що відображає алгоритм процедури. Завершується означення процедури комбінацією слів end proc, після якої ставимо знак : або знак ; (якщо використовується знак ; то у випадку, коли синтаксис правильний, на екран буде виведено означення процедури в тому вигляді, в якому його сприйняла система, в іншому випадку з'являється повідомлення про помилку).

Виклик процедур (або кажуть ще, звернення до процедур), як і виклик Maple-команд і функцій, здійснюється шляхом введення назви (ідентифікатора) процедури зі списком фактичних параметрів (конкретних значень):

name(PAR1,PAR2,...).

Команда, що складається з імені процедури, називається командою виклику процедури.

Відмітимо: після введення означення процедури і натиснення клавіші Enter команди, розміщені в тілі процедури не виконуються, в цей час інтерпретатор Maple-мови перевіряє, чи правильним є синтаксис, здійснює всі можливі спрощення в тілі процедури. Команди із тіла процедури виконуються лише в момент її виклику із певним заданим набором її фактичних параметрів PAR1,PAR2,..., при цьому значення фактичних параметрів підставляються на місце відповідних формальних параметрів par1,par2,... За замовчуванням процедура повертає результат останнього виконаного речення (обчисленого виразу) в її тілі. Якщо необхідно, щоб було повернено значення іншого виразу expr, то використовують команду **return(expr)**.

Параметри процедури. В загальному випадку формальний параметр процедури задається у вигляді par::type, де type – тип параметра. При виклику процедури для кожного із фактичних параметрів PAR перевіряється, чи збігається його тип із типом відповідного формального параметра

par. Якщо тип не збігається, то з'являється повідомлення про помилку. Наприклад, запис proc(a::integer) означає, що в якості параметра a може виступати лише ціле число, тому в тілі процедури параметру a можна присвоювати лише цілі значення.

Розглянемо процедуру **power**, що знаходить степінь числа з основою a і показником b:

```
> power:=proc(a::integer,b::integer)
     a^b
  end proc;
```

Після того, як процедуру введено, система її обробляє, визначає, чи не містить вона помилок. Помилок немає, тому в рядку виведення з'являється запис-результат обробки процедури системою:

$$power := \mathbf{proc}(a{::}integer,\ b{::}integer)\ a^b\ \mathbf{end\ proc}$$

Щоб знайти степінь 2^3, тепер достатньо викликати процедуру power, задавши її із фактичними параметрами 2 і 3 (важливо звертати увагу на порядок введення параметрів!).

```
> power(2,3);
```

$$8$$

Натомість обчислити степінь $2,3^4$ таким способом не можна:

```
> power(2.3,4);
```

```
Error, invalid input: power expects its 1st argument, a, to be of
type integer, but received 2.3
```

Система повідомляє про помилку. Причина в тому, що в означенні процедури power вказано тип її першого параметра a як integer (ціле число), а в якості фактичного параметра використано число 2.3 типу float.

Помилка може виникати і у випадку невідповідності кількості фактичних параметрів par1,par,... кількості заявлених формальних параметрів PAR1,PAR2,... Якщо кількість фактичних параметрів менша за кількість формальних параметрів, то з'являється повідомлення на зразок

```
> power(2);
```

```
Error, invalid input: power uses a 2nd argument, b, which is missing
```

(Помилка, неправильне введення: power використовує 2-ий аргумент b, який упущено (тобто не задано))

Якщо ж кількість фактичних параметрів більша за кількість формальних, то повідомлення про помилку не з'являється, а просто зайві фактичні параметри ігноруються.

```
> power(2,3,4);
```

8

Оформлення. При введенні означення процедури допускається перенесення слів з одного рядка на інший, але не можна розривати слова, константи і комбінації символів. Зауважимо, що перехід на новий рядок при введенні означення процедури здійснюється шляхом натиснення комбінації клавіш **Shift**+**Enter**. При натисненні лише клавіши **Enter**, коли означення процедури записане не повністю (не записана комбінація слів **end proc**), система повідомить про помилку:

```
> power:=proc(a::integer,b::integer)
Warning, premature end of input
```

Взагалі рекомендується процедуру записувати в такому вигляді, щоб її легко було читати, для цього використовуються пропуски, порожні рядки і коментарі. Також доцільно смислові частини відокремлювати відступами від початку рядка. Якщо виведення на екран тексту процедури (після обробки її системою) не потрібне, після слів end proc необхідно ставити знак : (а не ;).

Зауважимо також, що для простої однорядкової процедури типу

proc(par1,par2,...)
command(par1,par2,...)
end proc:

яка набору параметрів par1,par2,... ставить у відповідність результат команди command(par1,par2,...), простіше використовувати функціональний оператор:

(par1,par2,...) -> command(par1,par2,...)

Локальні і глобальні змінні. Змінні, як уже було сказано в §6, бувають локальні і глобальні. Глобальні змінні визначені в рамках всього поточного сеансу, їхні значення можна використовувати і змінювати в будь-який момент. Локальні змінні зберігають своє значення лише в межах процедури (або циклу), а поза межами процедури є невизначеними, або мають значення, яке вони мали до застосування процедури. Це яскраво видно на наступному прикладі:

```
> a:=1:
> plus:=proc(a,b) a+b end;
```

$$plus := \mathbf{proc}(a,\, b)\, a + b\, \mathbf{end\ proc}$$

```
> plus(2,3);
```

5

```
> a;
```

$$1$$

Всередині процедури $a = 2$, але поза її межами $a = 1$. Це значення і було виведено на екран.

Задають область дії змінної (тобто вказують, якою є змінна: глобальною чи локальною) за допомогою (необов'язкових) секцій global і local описової частини процедури. Розглянемо процедуру **sumprod**, яка парі чисел (a, b) ставить у відповідність пару чисел (x, y), де $x = a + b$ і $y = xy$. При цьому задамо змінну x як локальну, а змінну y як глобальну:

```
> sumprod:=proc(a,b)
  local x;
  global y;
     x:=a+b;
     y:=a*b;
     return(x,y)
  end proc;
```

$$sumprod := \mathbf{proc}(a,\, b)\, \mathbf{local}\, x;\, \mathbf{global}\, y;\, x := a + b\,;\, y := a * b\,;\ \ \mathbf{return}\ x,\, y\, \mathbf{end\ proc}$$

Знайдемо результат виконання даної процедури для чисел 2 і 3:

```
> sumprod(2,3);
```

$$5,\, 6$$

Виведемо тепер на екран значення x і y:

```
> x;y;
```

$$x$$

$$6$$

Як бачимо, змінна y набула значення 6, воно зберігається і поза межами процедури, натомість змінна x є невизначеною.

Якщо в тілі процедури є операції присвоювання для раніше заданих (глобальних) змінних, то зміна їхніх значень в ході виконання процедури може вплинути на результат інших обчислень. Щоб цього не відбулось, в Maple є вбудовані засоби: зустрівши такі операції присвоювання, система коригує текст процедури, додаючи рядок-оголошення змінних локальними за допомогою ключового слова local і видає повідомлення про це.

Так, якщо в процедурі plus суму $a + b$ позначити через c, отримаємо:

```
> plus:=proc(a,b)
     c:=a+b
  end proc;
```

```
Warning, ‘c‘ is implicitly declared local to procedure ‘plus‘
```

$$plus := \mathbf{proc}(a,\, b)\, \mathbf{local}\, c;\; c := a + b\, \mathbf{end\ proc}$$

Крім того, локальними вважаються змінні, що використовуються в циклах. Решта змінних – глобальні. Рекомендується, все ж таки, явно вказувати глобальні і локальні змінні: це дозволяє не лише уникнути помилок обробки, але й полегшує розуміння структури документа.

Загальна форма задання процедури. До описової частини процедури можна додавати і інші необов'язкові елементи. Загальна форма задання процедури виглядає наступним чином:

name:=**proc**(par1,par2,...)
⎡ **local** l1,l2,...; ⎤
⎢ **global** g1,g2,...; ⎥ описова
⎢ **option** opt1,opt2,...; ⎥ частина
⎢ **description** des1,des2,...; ⎥ процедури
⎣ **uses** package1,package2,... ⎦
<statement sequence>
end proc; (або :)

Тут l1,l2,... – імена локальних змінних, g1,g2,... – імена глобальних змінних. Порядок слідування секцій описової частини змінювати не можна: однак деякі секції можна не зазначати.

Розглянемо призначення інших секцій описової частини.

В секції **uses** вказують назви модулів або пакетів package1,package2,..., команди із яких використовує процедура. Наприклад, якщо серед команд, які входять до тіла процедури, є команди із пакету numtheory, то необхідно до описової частини додати рядок uses numtheory.

Секція **description** – описова, використовується в якості пояснення, коментаря призначення процедури. Має формат: description "comment", де "comment" – будь-який коментар string-типу. Її зміст не впливає на результат виконання процедури. Наприклад,

```
> sumprod:=proc(a,b)
  local x,y;
  description "poshuk sumy i dobutku chisel a i b";
      x:=a+b;
      y:=a*b;
      return(x,y)
  end proc;
```

sumprod := **proc**(*a*, *b*)
local *x*, *y*;
description "poshuk sumy i dobutku chisel a i b";
x := *a* + *b*; *y* := *a* ∗ *b*; **return** *x*, *y*
end proc

```
> sumprod(2,3);
```

5, 6

В секції **option** вказують певні спеціальні опції процедури. Серед них: remember, arrow, autocompile, builtin, cache, call_external, hfloat, inline, operator, remember, system, trace і 'Copyright...'. Така форма дозволяє створювати процедури для розв'язування досить складних задач. Із даними опціями пропонуємо ознайомитись самостійно, використовуючи довідкову систему.

Створення власної бібліотеки процедур

Якщо деяка процедура часто використовується, то її доцільно зберегти в пам'яті. Для цього створюється власна бібліотека процедур. Назвемо бібліотеку atchlib.

Спочатку задамо таблицю під майбутні процедури:

```
> atchlib:=table();
```

atchlib := table([])

Тепер занесемо до бібліотеки власні процедури. Такі процедури мають подвійну назву – спочатку вказується назва бібліотеки, а потім у квадратних дужках назва процедури.

Задамо дві простих процедури із назвами **summa** і **dobutok**, за допомогою яких можна буде знаходити суму і добуток двох заданих чисел:

```
> atchlib[summa]:=proc(x,y) x+y end proc;
```

$$atchlib_{summa} := \mathbf{proc}(x,\, y)\, x + y\, \mathbf{end\ proc}$$

```
> atchlib[dobutok]:=proc(x,y) x*y end proc;
```

$$atchlib_{dobutok} := \mathbf{proc}(x,\, y)\, x * y\, \mathbf{end\ proc}$$

За допомогою команди with можна перевірити, що бібліотека **atchlib** дійсно містить щойно введені в неї процедури. Їх перелік має з'явитись при зверненні **with(atchlib)**:

```
> with(atchlib);
```

[*dobutok*, *summa*]

Тепер необхідно записати цю бібліотеку під своїм ім'ям на диск за допомогою команди save:

```
> save(atchlib, 'd:/atchlib.m');
```

Зверніть увагу на правильне задання повного імені файлу. Зазвичай для вказування місцезнаходження файлу використовується знак \ (backslash). Але в Maple-мові цей знак вживається для продовження рядка. Тому в цьому випадку слід використовувати або подвійний знак \\ , або знак /. В розглянутому прикладі файл записано в корінь диску D. Після цього бажано перевірити, чи, дійсно, бібліотечний файл було записано. Для цього спочатку командою restart знімаємо раніше введені означення процедур.

```
> restart;
```

Команда with показує, що цих означень уже немає:

```
> with(atchlib);
```

```
Error, invalid input: with expects its 1st argument, pname, to be of
type {module, package}, but received atchlib
```

Після цього командою read необхідно завантажити бібліотечний файл:

```
> read('d:/atchlib.m');
```

Ім'я файлу слід вказувати за правилами, які використовувались для команди save. Якщо все виконано правильно, то команда with покаже перелік процедур в бібліотеці atchlib:

```
> with(atchlib);
```

$$[dobutok,\ summa]$$

і можна апробувати роботу створених процедур:

```
> summa(5,6);
```

$$11$$

```
> dobutok(5,6);
```

$$30$$

Розділ II

Теорія чисел

1. Відношення подільності та його властивості. Ділення з остачею

ТЕОРЕТИЧНІ ВІДОМОСТІ

Говорять, що ціле число a ділиться на ціле число b, якщо існує таке ціле число c, що виконується умова: $a = b \cdot c$. Число a при цьому називають діленим або кратним числа b, b – дільником a і c – часткою. Якщо a ділиться на b, то пишуть $a \vdots b$. У цьому випадку кажуть також, що b є дільником a і пишуть $b \mid a$. Запис $a \nvdots b$ означає, що a не ділиться на b, а запис $b \nmid a$ означає, що b не є дільником a.

Нехай a, b, c, a_i, b_i, де $i \in \overline{1,n}$, – довільні цілі числа. Тоді:

1. $a \vdots a,\ a \vdots 1,\ a \vdots (-a),\ a \vdots (-1)$.

2. $0 \vdots a$.

3. Якщо $a \vdots b$ і $b \vdots a$, то $a = b \cdot c$, де $c = \pm 1$ (такі числа a і b називають асоційованими). Зокрема, якщо $a, b \in \mathbb{N}$, то $a = b$.

4. Якщо $a \vdots b$, $b \vdots c$, то $a \vdots c$.

5. Якщо $a \vdots b$, то $a \vdots (-b)$, $(-a) \vdots b$ і $(-a) \vdots (-b)$.

6. Якщо $a \vdots c$ і $b \vdots c$, то $(a \pm b) \vdots c$.

6. Якщо $a \vdots c$, то $ab \vdots c$ для будь-якого $b \in \mathbb{Z}$.

8. Якщо $a_1 \vdots c, a_2 \vdots c, ..., a_n \vdots c$, то $(a_1b_1 \pm a_2b_2 \pm ... \pm a_nb_n) \vdots c$.

9. $a \vdots 0$ тоді і лише тоді, коли $a = 0$.

Розділити ціле число a на ціле число $b \neq 0$ з остачею означає знайти два цілих числа q і r таких, що:

1) $a = bq + r$;
2) $0 \leqslant r < |b|$.

Число a при цьому називають діленим, b – дільником, q – неповною часткою, а r – остачею від ділення a на b.

Теорема (про ділення з остачею)**.** *Для будь-яких цілих чисел a і b, де $b \neq 0$, завжди існує, причому лише одна, пара цілих чисел q і r таких, що $a = bq + r$, де $0 \leqslant r < |b|$.*

Твердження. *Для будь-яких $a, b \in \mathbb{Z}$, $k \in \mathbb{N}$, справедливо:*

$$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + \ldots + (-1)^i a^{2k-i}b^i + \ldots + b^{2k});$$
$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \ldots + a^{k-i}b^{i-1} + \ldots + ab^{k-2} + b^{k-1}).$$

Наслідок 1. *Сума степенів з однаковими непарними натуральними показниками ділиться на суму основ:* $a^{2k+1} + b^{2k+1} \vdots (a+b)$.

Наслідок 2. *Різниця степенів з будь-якими однаковими натуральними показниками ділиться на різницю основ:* $a^k - b^k \vdots (a-b)$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 1. Знайти неповну частку q і остачу r від ділення цілого числа a на ціле число b, якщо:

а) $a = 521$, $b = 15$;
б) $a = -521$, $b = 15$;
в) $a = 521$, $b = -15$;
г) $a = -521$, $b = -15$;
д) $a = 15$, $b = 521$;
е) $a = 15$, $b = -521$;
є) $a = -15$, $b = 521$;
ж) $a = -15$, $b = -521$.

Розв'язання. Спосіб І. Грунтується на першому способі доведення теореми 1 п.2 §1 із [1]. Якщо $b > 0$, то $q = [\frac{a}{b}]$, $r = a - bq$. Якщо $b < 0$, то знаходимо спочатку неповну частку q_1 від ділення числа $a_1 = a$ на число $b_1 = -b > 0$, тобто $q_1 = [\frac{a}{b_1}]$. Тоді $q = -q_1$. А потім знаходимо $r = a - bq$.

Таким чином, маємо:

а) $a = 521$, $b = 15$. Оскільки $b > 0$, то $q = [\frac{521}{15}] = 34$, $r = 521 - 15 \cdot 34 = 11$;

б) $a = -521$, $b = 15 > 0$. Тоді $q = [\frac{-521}{15}] = -35$, $r = -521 - 15 \cdot (-35) = 4$;

в) $a = 521$, $b = -15 < 0$. Тоді $b_1 = -b = 15$, $q_1 = [\frac{a}{b_1}] = [\frac{521}{15}] = 34$, отже, $q = -34$, $r = 521 - (-15) \cdot (-34) = 11$;

г) $a = -521$, $b = -15 < 0$. Тоді $b_1 = -b = 15$, $q_1 = [\frac{a}{b_1}] = [\frac{-521}{15}] = -35$, отже, $q = 35$, $r = -521 - (-15) \cdot 35 = 4$;

д) $a = 15$, $b = 521 > 0$. Тоді $q = [\frac{15}{521}] = 0$, $r = 15 - 521 \cdot 0 = 15$;

е) $a = -15$, $b = 521 > 0$. Тоді $q = [\frac{-15}{521}] = -1$, $r = -15 - 521 \cdot (-1) = 506$;

є) $a = 15$, $b = -521 < 0$. Тоді $b_1 = -b = 521$, $q_1 = [\frac{a}{b_1}] = [\frac{15}{521}] = 0$, отже, $q = 0$, $r = 15 - (-521) \cdot 0 = 15$;

ж) $a = -15$, $b = -521 < 0$. Тоді $b_1 = -b = 521$, $q_1 = [\frac{a}{b_1}] = [\frac{-15}{521}] = -1$, отже, $q = 1$, $r = -15 - (-521) \cdot 1 = 506$.

Спосіб II. Знайдемо найбільше ціле число k, яке кратне b і не перевищує a. Тоді неповну частку q дістанемо як частку від ділення k на b, а остачу r знайдемо як різницю між a та k.

а) $k = 510 = 15 \cdot 34$. Отже, $q = 34$, $r = 521 - 510 = 11$;
б) $k = -525 = 15 \cdot (-35)$. Таким чином, $q = -35$, $r = -521 - (-525) = 4$;
в) $k = 510 = (-15) \cdot (-34)$, звідки $q = -34$, $r = 521 - 510 = 11$;
г) $k = -525 = (-15) \cdot 35$. Отже, $q = 35$, $r = -521 - (-525) = 4$;
д) $k = 0 = 521 \cdot 0$. Значить, $q = 0$, $r = 15 - 0 = 15$;
е) $k = -521 = 521 \cdot (-1)$. Таким чином, $q = -1$, $r = -15 - (-521) = 506$;
є) $k = 0 = (-521) \cdot 0$, значить, $q = 0$, $r = 15 - 0 = 15$;
ж) $k = -521 = (-521) \cdot 1$. Отже, $q = 1$, $r = -15 - (-521) = 506$.

Спосіб III. Із способу I доведення теореми 1 п.2 §1 із [1] випливає, що:

1) у випадку $b > 0$ справедлива умова: $bq \leqslant a < b(q + 1)$, із якої число q визначається однозначно; тоді $r = a - bq$;
2) у випадку $b < 0$: $q = -q_1$, $r = r_1$, де q_1 і r_1 – відповідно неповна частка і остача від ділення числа a на число $b_1 = -b$.

Маємо:

а) $a = 521$, $b = 15$. Оскільки $b > 0$, то справедлива умова: $15q \leqslant 521 < 15(q+1)$, звідки $q \leqslant \frac{521}{15} < q+1$. Єдиним цілим числом, яке задовольняє дану умову є $q = 34$. Тоді $r = 521 - 15 \cdot 34 = 11$;

б) $a = -521$, $b = 15 > 0$. Тоді $15q \leqslant -521 < 15(q + 1)$, звідки $q = -35$, $r = -521 - 15 \cdot (-35) = 4$;

в) $a = 521$, $b = -15 < 0$. Знайдемо неповну частку q_1 і остачу r_1 від ділення числа a на число $b_1 = -b = 15$. З огляду на а), $q_1 = 34$, $r_1 = 11$. Тоді $q = -q_1 = -34$, $r = r_1 = 11$;

г) $a = -521$, $b = -15 < 0$. Тоді $b_1 = -b = 15$ і, з огляду на б), $q_1 = -35$, $r_1 = 4$, значить, $q = -q_1 = 35$, $r = r_1 = 4$;

д) $a = 15$, $b = 521 > 0$. Із умови $521q \leqslant 15 < 521(q + 1)$ визначаємо, що $q = 0$, тоді $r = 15 - 521 \cdot 0 = 15$;

е) $a = -15$, $b = 521 > 0$. Тоді $521q \leqslant -15 < 521(q + 1)$, звідки $q = -1$, значить, $r = -15 - 521 \cdot (-1) = 506$;

є) $a = 15$, $b = -521$. Тоді $b_1 = 521$ і, з огляду на д), $q_1 = 0$, $r_1 = 15$; звідси $q = -q_1 = 0$, $r = r_1 = 15$;

ж) $a = -15$, $b = -521$. Тоді $b_1 = 521$ і, з огляду на е), $q_1 = -1$, $r_1 = 506$. Отже, $q = -q_1 = 1$, $r = r_1 = 506$.

Розробка процедур. Більшість функцій Maple для розв'язування задач теорії чисел знаходиться в бібліотеці **numtheory**. Для її завантаження необхідно ввести

```
> with(numtheory):
```

(див. §7 розд. I), надалі на цьому окремо не наголошується). В цьому пакеті є команди **irem** і **iquo**, що називаються відповідно остачею і неповною часткою. Проте в описі цих команд (зокрема команди irem) зазначається, що якщо m і n – цілі числа, то результатом виконання команди irem(m,n) є число r таке, що $m = nq + r$, де $|r| < |n|$ і $m \cdot r \geqslant 0$. Таке означення „остачі" від ділення одного цілого числа на інше відрізняється від класичного означення в теорії чисед. Це легко бачити на наступному прикладі. Знайдемо за допомогою команди irem „остачу" від ділення числа -25 на 3. Маємо:

```
> irem(-25,3);
```

$$-1$$

Але за означенням остача r не може бути від'ємною.

Тому для перевірки правильності виконання завдання 1 необхідно створити нові команди, які б знаходили неповну частку і остачу від ділення цілого числа a на ціле число b. Для опису відповідних процедур (назвемо їх **quotient** і **remainder**, див.§8 розд.I) використаємо перший спосіб розв'язування даного прикладу. У випадку $b > 0$ числа q і r визначатимемо із умов $q = [\frac{a}{b}]$, $r = a - bq$. У випадку $b < 0$ знайдемо спочатку неповну частку q_1 від ділення числа a на число $b_1 = -b > 0$; тоді $q = -q_1$. А потім знайдемо $r = a - bq$. Якщо ж $b = 0$, то ділення числа a на b з остачею неможливе; в такому випадку система повинна повідомляти про помилку. Це записують наступним чином:

```
if b=0 then error "division by 0"
```

Для опису цієї команди необхідно використати функцію, що знаходить цілу частину дійсного числа x. В Maple такою функцією є функція **floor(x)** із пакету **numtheory**. Нижче наведено опис процедур quotient і remainder.

```
quotient:=proc(a::integer,b::integer)
local q,r,b1,q1;
uses numtheory;
   if b=0 then error "division by 0";
   elif b>0 then q:=floor(a/b); r:=a-b*q;
   else b1:=-b; q1:=quotient(a,b1); q:=-q1; r:=a-b*q;
   end if;
   return(q);
end proc;
```

```
remainder:=proc(a::integer,b::integer)
local q,r,b1,q1;
uses numtheory;
   if b=0 then error "division by 0";
   elif b>0 then q:=floor(a/b); r:=a-b*q;
   else b1:=-b; q1:=quotient(a,b1); q:=-q1; r:=a-b*q;
   end if;
   return(r);
end proc;
```

Виклик процедур здійснюється у форматі quotient(a,b) та remainder(a,b).

Зауважимо, різниця даних процедур полягає лише в тому, який результат виводиться на екран: в процедурі quotient виводимо число q; в процедурі remainder – число r. (Звичайно, в процедурі quotient не обов'язково знаходити число r, така дія не впливає на результат.)

Розв'язання в Maple. Вводимо процедури quotient та remainder, описані вище: (Зверніть увагу: перехід на наступний рядок здійснюється комбінацією клавіш Shift+Enter. Якщо ж натиснути лише клавішу Enter, Maple почне обробляти процедуру і, оскільки процедура введена не до кінця, повідомить про помилку).

```
> quotient:=proc(a::integer,b::integer)
  local q,r,b1,q1;
  uses numtheory;
     if b=0 then error "division by 0";
     elif b>0 then q:=floor(a/b); r:=a-b*q;
     else b1:=-b; q1:=quotient(a,b1); q:=-q1; r:=a-b*q;
     end if;
     return(q);
  end proc;
```

Натискаємо клавішу Enter, в рядку виведення з'являється результат обробки системою даної процедури:

quotient := **proc**(*a*::*integer*, *b*::*integer*)
local *q*, *r*, *b1*, *q1*;
if $b = 0$ **then error** "division by 0"
elif $0 < b$ **then** $q := \text{floor}(a/b)$; $r := a - b * q$
else $b1 := -b$; $q1 := \text{quotient}(a,\ b1)$; $q := -q1$; $r := a - b * q$
end if;
return *q*
end proc

Аналогічно вводимо процедуру remainder:

```
> remainder:=proc(a::integer,b::integer)
  local q,r,b1,q1;
  uses numtheory;
      if b=0 then error "division by 0";
      elif b>0 then q:=floor(a/b); r:=a-b*q;
      else b1:=-b; q1:=quotient(a,b1); q:=-q1; r:=a-b*q;
      end if;
      return(r);
  end proc;
```

remainder := **proc**(*a*::*integer*, *b*::*integer*)
local *q*, *r*, *b1*, *q1*;
if $b = 0$ **then error** "division by 0"
elif $0 < b$ **then** $q := \text{floor}(a/b)$; $r := a - b * q$
else $b1 := -b$; $q1 := \text{quotient}(a,\ b1)$; $q := -q1$; $r := a - b * q$
end if;
return *r*
end proc

Тепер застосовуємо команди **quotient** і **remainder** до заданих чисел:

```
> quotient(521,15); remainder(521,15);
```

$$34$$
$$11$$

```
> quotient(-521,15); remainder(-521,15);
```

$$-35$$
$$4$$

```
> quotient(521,-15); remainder(521,-15);
```

$$-34$$
$$11$$

```
> quotient(-521,-15); remainder(-521,-15);
```

$$35$$
$$4$$

```
> quotient(15,521); remainder(15,521);
```

$$0$$
$$15$$

```
> quotient(-15,521); remainder(-15,521);
```

$$-1$$
$$506$$

```
> quotient(15,-521); remainder(15,-521);
```

$$0$$
$$15$$

```
> quotient(-15,-521); remainder(-15,-521);
```

$$1$$
$$506$$

Зауваження. Досвід використання СКА „Maple" в процесі викладання курсу „Алгебра і теорія чисел" показав, що переважна більшість студентів з великим інтересом сприймає можливість перевірити правильність отриманої відповіді. Однак лише одиниці намагаються вникнути в принцип роботи розроблених авторами процедур (насправді, це цілком природно). Не вникаючи в суть, при наборі тексту процедури можна допустити багато помилок. Крім того, опис процедур часто досить великий, громіздкий, тому для набору тексту процедури необхідно досить багато часу. Тому всі описані в посібнику авторські процедури було оформлено у вигляді бібліотеки (про те, як створити бібліотеку процеду, див. в §8 розд.I). Файл бібліотеки atchlib.m додається до посібника на диску.

Читачу, який не бажає заглиблюватись в принцип роботи процедур, достатньо викликати необхідну команду із даної бібліотеки. Для цього спочатку вказуємо шлях до файлу бібліотеки:

```
> read(‘e:/atchlib.m‘);
```

(якщо дисковод позначений буквою E). Зверніть увагу, що апостроф тут використовується зворотній (клавіша розміщена в лівому верхньому куті клавіатури). Або альтернативно можна ввести рядок:

```
> read("e:/atchlib.m");
```

Далі слід підключити бібліотеку:

```
> with(atchlib):
```

Тепер вводимо команди quotient і remainder:

```
> quotient(521,15); remainder(521,15);
                                34
                                11
```

і т.д.

Натомість для тих, хто прагне розібратись із принципом роботи процедур, детальніше познайомитись із особливостями програмування в системі Maple, наводимо детальне пояснення в секції „Розробка процедур". Відмітимо, що деякі процедури можна оптимізувати (це не було зроблено авторами саме для того, щоб для тих, хто вперше знайомиться із основами роботи в Maple, освоєння елементів програмування в Maple було якомога простішим). Тому запрошуємо студентів надавати свої варіанти вдосконалення процедур!!!

Завдання 1. Знайти неповну частку q і остачу r від ділення цілого числа a на ціле число b, якщо:

1.1. а) $a = 328$, $b = 17$; д) $a = 17$, $b = 328$;
б) $a = -328$, $b = 17$; е) $a = 17$, $b = -328$;
в) $a = 328$, $b = -17$; є) $a = -17$, $b = 328$;
г) $a = -328$, $b = -17$; ж) $a = -17$, $b = -328$.

1.2. а) $a = 147$, $b = 15$; д) $a = 15$, $b = 147$;
б) $a = -147$, $b = 15$; е) $a = 15$, $b = -147$;
в) $a = 147$, $b = -15$; є) $a = -15$, $b = 147$;
г) $a = -147$, $b = -15$; ж) $a = -15$, $b = -147$.

1.3. а) $a = 224$, $b = 11$; д) $a = 11$, $b = 224$;
б) $a = -224$, $b = 11$; е) $a = 11$, $b = -224$;
в) $a = 224$, $b = -11$; є) $a = -11$, $b = 224$;
г) $a = -224$, $b = -11$; ж) $a = -11$, $b = -224$.

1.4. а) $a = 305$, $b = 19$; д) $a = 19$, $b = 305$;
б) $a = -305$, $b = 19$; е) $a = 19$, $b = -305$;
в) $a = 305$, $b = -19$; є) $a = -19$, $b = 305$;
г) $a = -305$, $b = -19$; ж) $a = -19$, $b = -305$.

1.5. а) $a = 287$, $b = 13$; д) $a = 13$, $b = 287$;
б) $a = -287$, $b = 13$; е) $a = 13$, $b = -287$;
в) $a = 287$, $b = -13$; є) $a = -13$, $b = 287$;
г) $a = -287$, $b = -13$; ж) $a = -13$, $b = -287$.

1.6. а) $a = 129$, $b = 7$; д) $a = 7$, $b = 129$;
б) $a = -129$, $b = 7$; е) $a = 7$, $b = -129$;
в) $a = 129$, $b = -7$; є) $a = -7$, $b = 129$;
г) $a = -129$, $b = -7$; ж) $a = -7$, $b = -129$.

1.7. а) $a = 344$, $b = 17$; д) $a = 17$, $b = 344$;
б) $a = -344$, $b = 17$; е) $a = 17$, $b = -344$;
в) $a = 344$, $b = -17$; є) $a = -17$, $b = 344$;
г) $a = -344$, $b = -17$; ж) $a = -17$, $b = -344$.

1.8. а) $a = 427$, $b = 15$; д) $a = 15$, $b = 427$;
б) $a = -427$, $b = 15$; е) $a = 15$, $b = -427$;
в) $a = 427$, $b = -15$; є) $a = -15$, $b = 427$;
г) $a = -427$, $b = -15$; ж) $a = -15$, $b = -427$.

1.9. а) $a = 201$, $b = 16$; д) $a = 16$, $b = 201$;
б) $a = -201$, $b = 16$; е) $a = 16$, $b = -201$;
в) $a = 201$, $b = -16$; є) $a = -16$, $b = 201$;
г) $a = -201$, $b = -16$; ж) $a = -16$, $b = -201$.

1.10. а) $a = 322$, $b = 13$; д) $a = 13$, $b = 322$;
б) $a = -322$, $b = 13$; е) $a = 13$, $b = -322$;
в) $a = 322$, $b = -13$; є) $a = -13$, $b = 322$;
г) $a = -322$, $b = -13$; ж) $a = -13$, $b = -322$.

1.11. а) $a = 339$, $b = 7$; д) $a = 7$, $b = 339$;
б) $a = -339$, $b = 7$; е) $a = 7$, $b = -339$;
в) $a = 339$, $b = -7$; є) $a = -7$, $b = 339$;
г) $a = -339$, $b = -7$; ж) $a = -7$, $b = -339$.

1.12. а) $a = 497$, $b = 11$; д) $a = 11$, $b = 497$;
б) $a = -497$, $b = 11$; е) $a = 11$, $b = -497$;
в) $a = 497$, $b = -11$; є) $a = -11$, $b = 497$;
г) $a = -497$, $b = -11$; ж) $a = -11$, $b = -497$.

1.13. а) $a = 265$, $b = 14$; д) $a = 14$, $b = 265$;
б) $a = -265$, $b = 14$; е) $a = 14$, $b = -265$;
в) $a = 265$, $b = -14$; є) $a = -14$, $b = 265$;
г) $a = -265$, $b = -14$; ж) $a = -14$, $b = -265$.

1.14. а) $a = 703$, $b = 15$; д) $a = 15$, $b = 703$;
б) $a = -703$, $b = 15$; е) $a = 15$, $b = -703$;
в) $a = 703$, $b = -15$; є) $a = -15$, $b = 703$;
г) $a = -703$, $b = -15$; ж) $a = -15$, $b = -703$.

1.15. а) $a = 249$, $b = 19$; б) $a = -249$, $b = 19$;

в) $a = 249$, $b = -19$;
г) $a = -249$, $b = -19$;
д) $a = 19$, $b = 249$;
е) $a = 19$, $b = -249$;
є) $a = -19$, $b = 249$;
ж) $a = -19$, $b = -249$.

1.16. а) $a = 523$, $b = 21$;
б) $a = -523$, $b = 21$;
в) $a = 523$, $b = -21$;
г) $a = -523$, $b = -21$;
д) $a = 21$, $b = 523$;
е) $a = 21$, $b = -523$;
є) $a = -21$, $b = 523$;
ж) $a = -21$, $b = -523$.

1.17. а) $a = 594$, $b = 15$;
б) $a = -594$, $b = 15$;
в) $a = 594$, $b = -15$;
г) $a = -594$, $b = -15$;
д) $a = 15$, $b = 594$;
е) $a = 15$, $b = -594$;
є) $a = -15$, $b = 594$;
ж) $a = -15$, $b = -594$.

1.18. а) $a = 237$, $b = 17$;
б) $a = -237$, $b = 17$;
в) $a = 237$, $b = -17$;
г) $a = -237$, $b = -17$;
д) $a = 17$, $b = 237$;
е) $a = 17$, $b = -237$;
є) $a = -17$, $b = 237$;
ж) $a = -175$, $b = -237$.

1.19. а) $a = 525$, $b = 18$;
б) $a = -525$, $b = 18$;
в) $a = 525$, $b = -18$;
г) $a = -525$, $b = -18$;
д) $a = 18$, $b = 525$;
е) $a = 18$, $b = -525$;
є) $a = -18$, $b = 525$;
ж) $a = -18$, $b = -525$.

1.20. а) $a = 703$, $b = 11$;
б) $a = -703$, $b = 11$;
в) $a = 703$, $b = -11$;
г) $a = -703$, $b = -11$;
д) $a = 11$, $b = 703$;
е) $a = 11$, $b = -703$;
є) $a = -11$, $b = 703$;
ж) $a = -11$, $b = -703$.

1.21. а) $a = 534$, $b = 13$;
б) $a = -534$, $b = 13$;
в) $a = 534$, $b = -13$;
г) $a = -534$, $b = -13$;
д) $a = 13$, $b = 534$;
е) $a = 13$, $b = -534$;
є) $a = -13$, $b = 534$;
ж) $a = -13$, $b = -534$.

1.22. а) $a = 479$, $b = 21$;
б) $a = -479$, $b = 21$;
в) $a = 479$, $b = -21$;
г) $a = -479$, $b = -21$;
д) $a = 21$, $b = 479$;
е) $a = 21$, $b = -479$;
є) $a = -21$, $b = 479$;
ж) $a = -21$, $b = -479$.

1.23. а) $a = 281$, $b = 19$;
б) $a = -281$, $b = 19$;
в) $a = 281$, $b = -19$;
г) $a = -281$, $b = -19$;
д) $a = 19$, $b = 281$;
е) $a = 19$, $b = -281$;
є) $a = -19$, $b = 281$;
ж) $a = -19$, $b = -281$.

1.24. а) $a = 770$, $b = 18$;
б) $a = -770$, $b = 18$;
в) $a = 770$, $b = -18$;
г) $a = -770$, $b = -18$;

д) $a = 18$, $b = 770$;
е) $a = 18$, $b = -770$;
є) $a = -18$, $b = 770$;
ж) $a = -18$, $b = -770$.

1.25. а) $a = 371$, $b = 17$;
б) $a = -371$, $b = 17$;
в) $a = 371$, $b = -17$;
г) $a = -371$, $b = -17$;
д) $a = 17$, $b = 371$;
е) $a = 17$, $b = -371$;
є) $a = -17$, $b = 371$;
ж) $a = -17$, $b = -371$.

Приклад 2. При діленні цілого числа a на ціле число $b > 0$ отримали неповну частку q і остачу r. Знайти невідомі, якщо:

а) $a = 371$, $q = 14$; б) $a = 1256$, $r = 35$.

Розв'язання. а) За теоремою про ділення з остачею: $371 = 14 \cdot b + r$, де $0 \leqslant r < b$. Тоді $r = 371 - 14b$, звідки $0 \leqslant 371 - 14b < b$, значить, $14b \leqslant 371 < 15b$. Таким чином, $371 \geqslant 14b$, тобто $b \leqslant \left[\frac{371}{14}\right] = 26$. З іншого боку, $371 < 15b$, тоді $b > \left[\frac{371}{15}\right] = 24$. Таким чином, $24 < b \leqslant 26$, $b \in \mathbb{Z}$. Отже, $b_1 = 25$, $b_2 = 26$. Тоді відповідно $r_1 = 21$, $r_2 = 7$.

б) За теоремою про ділення з остачею

$$1256 = b \cdot q + 35,$$

звідки $b \cdot q = 1221$. Випишемо всі можливі додатні дільники числа 1221: $1, 3, 11, 33, 37, 111, 407, 1221$. Оскільки остача r має задовольняти умову $0 \leqslant r < b$, то число $b > 35$. Отже, b може дорівнювати лише 37, 111, 407, 1221. Таким чином, маємо: $b_1 = 37$, $q_1 = \frac{1221}{37} = 33$; $b_2 = 111$, $q_2 = 11$; $b_3 = 407$, $q_3 = 3$; $b_4 = 1221$, $q_4 = 1$.

Розв'язання в Maple. а) Розв'язання даної задачі зводиться до пошуку цілих розв'язків нерівності $0 \leqslant a - qb < b$. Для цього використовуємо команду **solve** (див. §7, розд.I):

```
> a:=371;q:=14;
```

$$a := 371$$
$$q := 14$$

```
> solve(0 <= a-q*x and a-q*x < x,x);
```

$$\text{RealRange}(\text{Open}(\frac{371}{15}),\ \frac{53}{2})$$

Отриманий результат означає, що число b має належати проміжку $(\frac{371}{15}; \frac{53}{2}]$. Знайдемо всі цілі числа b з даного проміжку.

Для розв'язування рівнянь і нерівностей в цілих числах використовується команда **isolve**. Її формат аналогічний до формату команди solve:

```
> isolve({371/15<x,x<=53/2});
```

$$\{x = 25\},\ \{x = 26\}$$

Отже, такими числами є лише числа $b_1 = 25$, $b_2 = 26$. Тоді відповідно

```
> r1:=a-25*q;
```

$$r1 := 21$$

```
> r2:=a-26*q;
```

$$r2 := 7$$

б) Із умови $a = bq + r$, випливає, що число b є додатним дільником числа $a - r$. Множину M всіх додатних дільників числа n можна знайти за допомогою команди **divisors(n)** з пакету numtheory. Всього таких дільників є $\tau(n)$. В пакеті numtheory є команда для відшукання числа $\tau(n)$, її формат **tau(n)**. Далі серед елементів множини M вибираємо дільники b, які більші за остачу r, і одразу знаходимо відповідну неповну частку q.

```
> a:=1256;
> r := 35;
> a-r;
```

$$1221$$

```
> with(numtheory):
  M:=divisors(a-r);
```

$$M := \{1,\ 3,\ 11,\ 33,\ 37,\ 111,\ 407,\ 1221\}$$

```
> k:=tau(a-r):
  for i from 1 to k do
     if M[i]>r then print(b=M[i]); print(q=(a-r)/M[i]); end if;
  end do;
```

$$b = 37$$
$$q = 33$$
$$b = 111$$
$$q = 11$$
$$b = 407$$
$$q = 3$$
$$b = 1221$$
$$q = 1$$

Завдання 2. При діленні цілого числа a на ціле число $b > 0$ отримали неповну частку q і остачу r. Знайти невідомі, якщо:

2.1. а) $a = 1023$, $q = 17$; б) $a = 461$, $r = 6$.

2.2. а) $a = 975$, $q = 14$; б) $a = 113$, $r = 23$.

2.3. а) $a = 1005$, $q = 24$; б) $a = 291$, $r = 6$.

2.4. а) $a = 963$, $q = 18$; б) $a = 673$, $r = 8$.

2.5. а) $a = 1421$, $q = 26$; б) $a = 380$, $r = 38$.

2.6. а) $a = 1031$, $q = 18$; б) $a = 525$, $r = 15$.

2.7. а) $a = 1245$, $q = 23$; б) $a = 249$, $r = 25$.

2.8. а) $a = 854$, $q = 17$; б) $a = 588$, $r = 61$.

2.9. а) $a = 883$, $q = 49$; б) $a = 161$, $r = 11$.

2.10. а) $a = 1523$, $q = 28$; б) $a = 974$, $r = 5$.

2.11. а) $a = 1033$, $q = 24$; б) $a = 363$, $r = 41$.

2.12. а) $a = 1211$, $q = 29$; б) $a = 304$, $r = 32$.

2.13. а) $a = 989$, $q = 13$; б) $a = 191$, $r = 9$.

2.14. а) $a = 899$, $q = 42$; б) $a = 305$, $r = 32$.

2.15. а) $a = 1529$, $q = 29$; б) $a = 243$, $r = 22$.

2.16. а) $a = 1042$, $q = 19$; б) $a = 202$, $r = 7$.

2.17. а) $a = 937$, $q = 22$; б) $a = 393$, $r = 33$.

2.18. а) $a = 1049$, $q = 24$; б) $a = 280$, $r = 14$.

2.19. а) $a = 972$, $q = 17$; б) $a = 386$, $r = 35$.

2.20. а) $a = 1323$, $q = 16$; б) $a = 405$, $r = 6$.

2.21. а) $a = 1001$, $q = 27$; б) $a = 247$, $r = 13$.

2.22. а) $a = 1713$, $q = 46$; б) $a = 321$, $r = 17$.

2.23. а) $a = 1002$, $q = 31$; б) $a = 279$, $r = 27$.

2.24. а) $a = 957$, $q = 23$; б) $a = 198$, $r = 16$.

2.25. а) $a = 1307$, $q = 43$; б) $a = 303$, $r = 16$.

2. Найбільший спільний дільник та найменше спільне кратне

ТЕОРЕТИЧНІ ВІДОМОСТІ

Ціле число c називається спільним дільником цілих чисел a і b, якщо $a \vdots c$ і $b \vdots c$. Число 0 може бути спільним дільником чисел a і b тоді і лише тоді, коли $a = 0$, $b = 0$. Найбільшим спільним дільником цілих чисел a і b, одночасно не рівних нулю, називається такий їхній додатний спільний дільник, який ділиться на будь-який спільний дільник цих чисел. Якщо d – найбільший спільний дільник цілих чисел a і b, то пишуть $d = (a, b)$ або $d = \text{НСД}(a, b)$.

Властивості найбільшого спільного дільника

Нехай a, b, q, r – довільні цілі числа.

1°. Якщо $a \vdots b$, $b > 0$, то $(a, b) = b$.
2°. Якщо $a = bq + r$, де a, b, r – відмінні від нуля цілі числа, то $(a, b) = (b, r)$.
3°. Для довільного $m \in \mathbb{N}$, $(ma, mb) = m(a, b)$.
4°. Якщо $c > 0$ – спільний дільник a і b, то $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{c}$.
5°. $d = (a, b)$ тоді і лише тоді, коли $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Теорема. *Для будь-яких цілих чисел a і b, одночасно не рівних нулю, найбільший спільний дільник завжди існує і дорівнює останній відмінній від нуля остачі* ***алгоритму Евкліда****.*

Теорема (про лінійне представлення найбільшого спільного дільника)**.** *Якщо d – найбільший спільний дільник двох цілих чисел a і b, то існують цілі числа x і y такі, що*

$$ax + by = d. \tag{II.1}$$

Запис d у вигляді (II.1) називається лінійним представленням найбільшого спільного дільника d цілих чисел a і b.

Цілі числа a і b називаються взаємно простими, якщо $(a, b) = 1$.

Властивості взаємно простих чисел

1♮. (**критерій взаємної простоти двох цілих чисел**). Для того, щоб числа a і b були взаємно простими, необхідно і достатньо, щоб існували цілі числа x і y такі, що $ax + by = 1$.

2♮. Якщо $ab \vdots c$ і $(b, c) = 1$, то $a \vdots c$.

3♮. Якщо $a \vdots b$, $a \vdots c$, причому $(b, c) = 1$, то $a \vdots bc$.

4♮. Якщо $(a, c) = (b, c) = 1$, то $(ab, c) = 1$.

5♮. Якщо $(a_i, b_j) = 1$ для всіх $i \in \overline{1, s}$, $j \in \overline{1, n}$, то $(a_1a_2...a_s, b_1b_2...b_n) = 1$. Зокрема, якщо $(a, b) = 1$, то $(a^m, b^k) = 1$, де $m, k \in \mathbb{N}$.

Ціле число M називається спільним кратним цілих чисел a і b, якщо $M \vdots a$ і $M \vdots b$. Найменшим спільним кратним відмінних від нуля цілих чисел a і b називається таке додатне спільне кратне цих чисел, яке є дільником будь-якого їхнього спільного кратного. Якщо хоча б одне із чисел a або b рівне 0, то найменшим спільним кратним a і b є число 0. Якщо m – найменше спільне кратне чисел a і b, то це записують так: $m = [a, b]$ або $m = \text{НСК}(a, b)$.

Теорема. *Нехай a і b – довільні натуральні числа. Тоді*

$$[a, b] = \frac{ab}{(a, b)}. \tag{II.2}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 3.1. Довести, що $2n^3 - 3n^2 + n \vdots 6$ при довільному $n \in \mathbb{N}$.

Розв'язання. Введемо позначення: нехай $a_n = 2n^3 - 3n^2 + n$.

Спосіб I. Вираз a_n розкладемо на множники:

$$a_n = 2n^3 - 3n^2 + n = n(2n^2 - 3n + 1) = n(2n^2 - 2n - n + 1) = \\ = n(2n(n-1) - (n-1)) = n(n-1)(2n-1).$$

Оскільки або n, або $n-1$ ділиться на 2, то добуток $n(n-1) \vdots 2$, а значить, $a_n \vdots 2$.

Покажемо, що $a_n \vdots 3$. В силу теореми про ділення з остачею, для чисел n і 3 існують цілі числа q і r такі, що $n = 3q + r$, де $0 \leqslant r \leqslant 2$. Вираз a_n запишемо у вигляді:

$$a_n = (3q + r)(3q + r - 1)(6q + 2r - 1).$$

Якщо $r = 0$, то $a_n = 3q(3q-1)(6q-1) \vdots 3$;
якщо $r = 1$, то $a_n = (3q+1) \cdot 3q \cdot (6q+1) \vdots 3$;
якщо $r = 2$, то $a_n = (3q+2)(3q+1)(6q+3) \vdots 3$.

Таким чином, в будь-якому випадку $a_n \vdots 3$.

Оскільки $a_n \vdots 2$ і $a_n \vdots 3$ і $(2, 3) = 1$, то, в силу властивості $3^\natural$, $a_n \vdots 6$.

Спосіб II. Використаємо метод математичної індукції.

1. При $n = 1$ маємо: $a_1 = 2 \cdot 1 - 3 \cdot 1 + 1 = 0 \vdots 6$.

2. Припустимо, що твердження справедливе при $n = k$, тобто $a_k = 2k^3 - 3k^2 + k \vdots 6$, і покажемо, що воно буде справедливе і при $n = k + 1$, тобто, що $a_{k+1} = 2(k+1)^3 - 3(k+1)^2 + (k+1) \vdots 6$. Маємо:

$$a_{k+1} = 2(k+1)^3 - 3(k+1)^2 + (k+1) = (2k^3 - 3k^2 + k) + 6k^2 = a_k + 6k^2 \vdots 6,$$

оскільки за припущенням $a_k \vdots 6$.

В силу принципу математичної індукції, твердження, що $2n^3-3n^2+n \vdots 6$, справедливе для довільного натурального n.

Зауваження. Для того, щоб довести, що $a_{k+1} \vdots 6$ (за умови, що $a_k \vdots 6$), достатньо показати, що різниця $a_{k+1} - a_k$ ділиться на 6. Розглянемо різницю:

$$a_{k+1} - a_k = 2(k+1)^3 - 3(k+1)^2 + (k+1) - 2k^3 - 3k^2 + k = \\ = 2(3k^2 + 3k + 1) - 3(k+1) + 1 = 6k^2.$$

Оскільки $a_{k+1} - a_k \vdots 6$ і $a_k \vdots 6$, то $a_{k+1} \vdots 6$.

Розв'язання в Maple. Спосіб I. Позначимо $a_n = 2n^3 - 3n^2 + n$. Розкладемо вираз a_n на множники. Для розкладу виразу eq на множники використовується команда **factor(eq)**. Маємо:

```
> a_n:=factor(2*n^3-3*n^2+n);
```

$$a\_n := n\,(2\,n-1)\,(n-1)$$

В силу теореми про ділення з остачею, $n = 3q + r$, де $q, r \in \mathbb{Z}$, причому $0 \leqslant r \leqslant 2$. Підставимо вираз для n в попередню рівність (використовуючи команду **subs**, див. §8, розд.I):

```
> a_n:=subs({n=3*q+r},a_n);
```

$$a\_n := (3\,q+r)\,(6\,q+2\,r-1)\,(3\,q+r-1)$$

Далі розглядаємо випадки для числа r. В кожному із випадків знаходимо вираз a_n і перевіряємо, чи ділиться даний вираз на 3 (для цього знаходимо остачу від ділення a_n на 3 за допомогою оператора **mod**, пишуть a_n mod m, де **m** – дільник. Про оператор mod піде мова дещо пізніше (див. §5)).

```
> r:=0; a_n; (a_n mod 3);
```

$$r := 0$$
$$3\,q\,(6\,q-1)\,(3\,q-1)$$
$$0$$

```
> r:=1; a_n; (a_n mod 3);
```

$$r := 1$$
$$3\,(3\,q+1)\,(6\,q+1)\,q$$
$$0$$

```
> r:=2; a_n; (a_n mod 3);
```

$$r := 2$$
$$(3\,q+2)\,(6\,q+3)\,(3\,q+1)$$

0

Як бачимо, в кожному із випадків остача від ділення a_n на 3 дорівнює 0, отже, $a_n \vdots 3$ для довільного $n \in \mathbb{N}$.

Зручно використати команду **evalb(x)**, результатом якої є відповідь на питання, чи є істинним твердження **x**. Можливі наступні результати: true – твердження істинне, false – твердження хибне, FAIL – неможливо відповісти. Важливо: команда evalb не спрощує виразів. Тому її результатом може бути false для істинного твердження. В такому випадку, необхідно спочатку спростити вирази, а потім використовувати команду evalb.

Перевіримо, наприклад, чи правильно, що при $r = 0$ вираз a_n ділиться на 3.

```
> evalb(subs({r=0},a_n) mod 3=0);
```

$$true$$

Можна одразу здійснити перевірку для всіх можливих остач r, використовуючи цикл **for**.

```
> for i from 0 to 2 do evalb(subs({r=i},a_n) mod 3=0) end do;
```

$$true$$
$$true$$
$$true$$

В кожному із випадків $r = 0$, $r = 1$, $r = 2$ вираз a_n ділиться на 3.

Аналогічно перевіряємо, що $a_n \vdots 2$:

```
> a_n:=factor(2*n^3-3*n^2+n);
```

$$a\_n := n\,(2\,n-1)\,(n-1)$$

```
> a_n:=subs({n=2*q+r},a_n);
```

$$a\_n := (2\,q+r)\,(4\,q+2\,r-1)\,(2\,q+r-1)$$

```
> for i from 0 to 1 do evalb(subs({r=i},a_n) mod 2=0) end do;
```

$$true$$
$$true$$

Спосіб II. Використаємо метод математичної індукції. Заданий вираз позначимо через f (див. §8 розд.I):

```
> f:=n->2*n^3-3*n^2+n;
```

$$f := n \to 2\,n^3 - 3\,n^2 + n$$

Перевіримо, чи виконується твердження при $n = 1$:

```
> evalb(f(1) mod 6=0);
```

true

При $n = 1$ твердження виконується. Припустимо, що твердження справедливе при $n = k$ (тобто $f(k) \vdots 6$). Тоді для того, щоб показати, що воно справедливе і при $n = k + 1$ (тобто $f(k + 1) \vdots 6$), достатньо показати, що різниця $f(k + 1) - f(k)$ ділиться на 6 (дивіться Зауваження). Знайдемо різницю і спростимо її:

```
> simplify(f(k+1)-f(k));
```

$$6\,k^2$$

Залишається перевірити, чи ділиться отриманий вираз на 6 (щоб не вводити отриманий вираз, використаємо нуль-арний оператор %, див. §4, Розд.I):

```
> evalb(% mod 6=0);
```

true

Отже, різниця $a_{k+1} - a_k$ ділиться на 6. Тоді, враховуючи, що, за індуктивним припущенням, $a_k \vdots 6$, матимемо, що і $a_{k+1} \vdots 6$. В силу принципу математичної індукції, твердження $a_n = 2n^3 - 3n^2 + n \vdots 6$ справедливе для довільного натурального n.

Приклад 3.2. Довести, що при будь-якому натуральному n число $11^{n+2} + 12^{2n+1}$ ділиться на 133.

Розв'язання. Введемо позначення: нехай $a_n = 11^{n+2} + 12^{2n+1}$.

Спосіб I. Перетворимо даний вираз:

$$a_n = 11^{n+2} + 12^{2n+1} = 11^n \cdot 121 + 12^{2n} \cdot 12 = (12^{2n} - 11^n) \cdot 12 + 133 \cdot 11^n = \\ = (144^n - 11^n) \cdot 12 + 133 \cdot 11^n.$$

За наслідком 1 §1: $144^n - 11^n \vdots (144 - 11)$, тобто $144^n - 11^n \vdots 133$. Оскільки $133 \cdot 11^n \vdots 133$, то за властивістю 6 §1 $a_n \vdots 133$.

Спосіб II. Використаємо метод математичної індукції.

1. При $n = 1$ твердження справедливе: $a_1 = 11^3 + 12^3 = 3059 \vdots 133$).

2. Припустимо, що твердження справедливе при натуральному n, тобто $a_n = 11^{n+2} + 12^{2n+1} \vdots 133$, і покажемо, що тоді воно справедливе при $n + 1$. Вираз a_{n+1} перетворимо наступним чином:

$$a_{n+1} = 11^{n+3} + 12^{2(n+1)+1} = 11^{n+2} \cdot 11 + 12^{2n+1} \cdot 144 = 11^{n+2} \cdot 11 + \\ + 12^{2n+1} \cdot (11 + 133) = (11^{n+2} + 12^{2n+1}) \cdot 11 + 133 \cdot 12^{2n+1} = 11 \cdot a_n + 133 \cdot 12^{2n+1}.$$

За індуктивним припущенням $a_n \vdots 133$. Доданок $133 \cdot 12^{2k+1}$, очевидно, теж ділиться на 133. Отже, вираз a_{n+1} ділиться на 133.

В силу принципу математичної індукції, $11^{n+2} + 12^{2n+1} \vdots 133$ при будь-якому натуральному n.

Зауваження. Зручно, припустивши, що твердження справедливе при $n = k$, тобто $a_n = 11^{n+2} + 12^{2n+1} \vdots 133$, записати a_n у вигляді $a_n = 133s$, де $s \in \mathbb{Z}$. Тоді $11^{n+2} = 133s - 12^{2n+1}$. Звідси, $a_{n+1} = 11^{n+3} + 12^{2(n+1)+1} = 11^{n+2} \cdot 11 + 12^{2n+1} \cdot 144 = (133s - 12^{2n+1}) \cdot 11 + +12^{2n+1} \cdot 144 = 133 \cdot 11s + 133 \cdot 12^{2n+1}$. Кожен із доданків ділиться на 133, а отже, і вираз a_n ділиться на 133.

Розв'язання в Maple. Аналогічно до Прикладу 3.1 (див. спосіб II), матимемо:

```
> f:=n->11^(n+2)+12^(2*n+1);
```

$$f := n \to 11^{(n+2)} + 12^{(2\,n+1)}$$

```
> evalb(f(1) mod 133=0);
```

true

Отже, при $n = 1$ твердження справедливе.

```
> evalb(simplify(f(k+1)-f(k)) mod 133=0);
```

true

Різниця $f(k+1) - f(k)$ ділиться на 133. Тоді у випадку якщо $f(k) \vdots 133$, то і $f(k+1) \vdots 133$. В силу принципу математичної індукції, твердження справедливе для довільного $n \in \mathbb{N}$.

Завдання 3. Довести, що:

3.1. а) $(n^{12} - n^8 - n^4 + 1) \vdots 512$ для довільного непарного цілого числа n;
б) $(5^{n+3} + 11^{3n+1}) \vdots 17$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.2. а) $(3^{3n+2} + 5 \cdot 2^{3n+1}) \vdots 19$ для довільного $n \in \mathbb{N} \cup \{0\}$;
б) $(4^n + 15n - 1) \vdots 9$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.3. а) $(n^3 + 3n^2 - n + 45) \vdots 48$ для довільного непарного цілого числа n;
б) $(50^n - 5^n(2^n + 1) + 1) \vdots 36$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.4. а) $(n + 2)(n^3 - n + 24) \vdots 24$ для довільного $n \in \mathbb{Z}$;
б) $(3^{2n+3} - 24n + 37) \vdots 64$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.5. а) $(n^3 + 3n^2 + 5n) \vdots 3$ для довільного $n \in \mathbb{Z}$;
б) $(5 \cdot 7^n + 6n + 19) \vdots 12$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.6. а) $(5^n + 5^{n+1} + 5^{n+3} + 1965) \vdots 655$ для довільного $n \in \mathbb{N}$;

б) $(4 \cdot 3^{2n+2} + 32n - 36) \vdots 64$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.7. а) $(2n^3 - 3n^2 + n) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(5^{2+n} + 26 \cdot 5^n + 8^{2n+1}) \vdots 59$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.8. а) $(n^4 - 2n^3 - 3n^2 + 2n) \vdots 24$ для довільного $n \in \mathbb{Z}$;
б) $(n \cdot 7^{n+1} - (n-1)7^n - 1) \vdots 6$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.9. а) $(n^3 + 35n) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(3^{3n+3} - 26n - 27) \vdots 169$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.10. а) $(6^{2n} + 3^{3n+2} - 3^n - 9 \cdot 5^n) \vdots 11$ для довільного $n \in \mathbb{N} \cup \{0\}$;
б) $(10^n - 9n + 26) \vdots 27$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.11. а) $(n^3 + (n+1)^3 + (n+2)^3) \vdots 9$ для довільного $n \in \mathbb{Z}$;
б) $(5^n - 4n + 15) \vdots 16$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.12. а) $7^{2n} - 1 \vdots 48$ для довільного $n \in \mathbb{N} \cup \{0\}$;
б) $(5^{n+3} \cdot 2^n - 125) \vdots 45$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.13. а) $n(8n+1)(7n+1) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(2^{2n+3} + 120n + 28) \vdots 36$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.14. а) $(n^3 + 3n^2 + 2n) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}) \vdots 19$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.15. а) $(2n^6 - n^4 - n^2) \vdots 36$ для довільного $n \in \mathbb{Z}$;
б) $(4^n + 6n + 8) \vdots 9$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.16. а) $(n+2)(n^2 + 4n + 9) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(9^{n+1} - 8n + 7) \vdots 16$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.17. а) $(n^5 + 29n) \vdots 30$ для довільного $n \in \mathbb{Z}$;
б) $(10^n + 18n - 28) \vdots 27$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.18. а) $(2^{8n+4} + 1) \vdots 17$ для довільного $n \in \mathbb{N} \cup \{0\}$;
б) $(2^{n+2} \cdot 3^n + 5n - 4) \vdots 25$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.19. а) $(n^2 + 3n + 1)^2 + 23 \vdots 24$ для довільного $n \in \mathbb{Z}$;
б) $(13^n + 4n - 1) \vdots 16$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.20. а) $(2n^3 + 3n^2 + 7n) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(3 \cdot 5^n - 12n + 45) \vdots 48$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.21. а) $(n^7 + 41n) \vdots 42$ для довільного $n \in \mathbb{Z}$;
б) $(5 \cdot 9^n + 24n + 59) \vdots 64$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.22. а) $(6^{10n+1} + 1) \vdots 7$ для довільного $n \in \mathbb{N} \cup \{0\}$;

б) $(4^n + 3n - 1) \vdots 6$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.23. а) $(n^2 - 1)(n^2 + 2n + 12) \vdots 12$ для довільного $n \in \mathbb{Z}$;
б) $(5 \cdot 7^n - 48n + 13) \vdots 18$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.24. а) $(1 + 3^{3n+1} + 9^{3n+1}) \vdots 13$ для довільного $n \in \mathbb{N} \cup \{0\}$;
б) $(2^{2n+1} - 6n + 16) \vdots 18$ для довільного $n \in \mathbb{N} \cup \{0\}$.

3.25. а) $(n^3 + 5n + 12) \vdots 6$ для довільного $n \in \mathbb{Z}$;
б) $(7 \cdot 5^n + 20n + 1) \vdots 8$ для довільного $n \in \mathbb{N} \cup \{0\}$.

Приклад 4.1. За допомогою алгоритму Евкліда знайти:

а) найбільший спільний дільник чисел 548 і -702;
б) лінійне представлення $(548, -702)$;
в) найменше спільне кратне чисел 548 і -702.

Розв'язання. а) Оскільки $(548, -702) = (548, 702)$, то, використовуючи алгоритм Евкліда, знайдемо $d = (548, 633)$. Нехай $a = 702$, $b = 548$. Маємо:

$$
\begin{array}{rrl|l}
a = & 702 & 548 & = b \\
\cline{3-4}
 & 548 & 1 & \\
\cline{2-3}
b = & 548 & 154 & = r_1 \\
\cline{2-3}
 & 462 & 3 & \\
\cline{2-3}
r_1 = & 154 & 86 & = r_2 \\
\cline{2-3}
 & 86 & 1 & \\
\cline{2-3}
r_2 = & 86 & 68 & = r_3 \\
\cline{2-3}
 & 68 & 1 & \\
\cline{2-3}
r_3 = & 68 & 18 & = r_4 \\
\cline{2-3}
 & 54 & 3 & \\
\cline{2-3}
r_4 = & 18 & 14 & = r_5 \\
\cline{2-3}
 & 14 & 1 & \\
\cline{2-3}
r_5 = & 14 & 4 & = r_6 \\
\cline{2-3}
 & 12 & 3 & \\
\cline{2-3}
r_6 = & 4 & 2 & = r_7 \neq 0 \\
\cline{2-3}
 & 4 & 2 & \\
\cline{2-3}
 & 0 & = r_8 &
\end{array}
$$

Таким чином, $r_8 = 0$. Остання відмінна від нуля остача алгоритму Евкліда $r_7 = 2$, значить, $(702, 548) = 2$, а тому і $(-702, 548) = 2$.

б) Знайдемо спочатку лінійне представлення $(702, 548)$. Випишемо рівності, отримані в процесі виконання алгоритму:

$$\begin{aligned}
a &= 1 \cdot b + r_1,\\
b &= 3 \cdot r_1 + r_2,\\
r_1 &= 1 \cdot r_2 + r_3,\\
r_2 &= 1 \cdot r_3 + r_4,\\
r_3 &= 3 \cdot r_4 + r_5,\\
r_4 &= 1 \cdot r_5 + r_6,\\
r_5 &= 3 \cdot r_6 + d, \quad \text{де} \quad d = r_7.
\end{aligned}$$

Виразимо остачі:

$$\begin{aligned}
r_1 &= a - b, && \text{(II.3)}\\
r_2 &= b - 3r_1, && \text{(II.4)}\\
r_3 &= r_1 - r_2, && \text{(II.5)}\\
r_4 &= r_2 - r_3, && \text{(II.6)}\\
r_5 &= r_3 - 3r_4, && \text{(II.7)}\\
r_6 &= r_4 - r_5, && \text{(II.8)}\\
d &= r_5 - 3r_6.
\end{aligned}$$

Підставляючи послідовно в останню рівність замість r_6, r_5, r_4, r_3, r_2 та r_1 їхні представлення (II.3)-(II.8), отримуємо:

$$\begin{aligned}
d = r_5 - 3r_6 &\overset{(II.8)}{=} r_5 - 3(r_4 - r_5) = 4r_5 - 3r_4 \overset{(II.7)}{=} 4(r_3 - 3r_4) - 3r_4 = 4r_3 - 15r_4 \overset{(II.6)}{=}\\
&= 4r_3 - 15(r_2 - r_3) = 19r_3 - 15r_2 \overset{(II.5)}{=} 19(r_1 - r_2) - 15r_2 = 19r_1 - 34r_2 \overset{(II.4)}{=}\\
&= 19r_1 - 34(b - 3r_1) = 121r_1 - 34b \overset{(II.3)}{=} 121(a - b) - 34b = 121a - 155b.
\end{aligned}$$

Таким чином, $d = 121a - 155b$, тобто $2 = 121 \cdot 702 - 155 \cdot 548$. Тоді, очевидно, $2 = (-121)(-702) + (-155) \cdot 548$. Отже, $x = -121$, $y = -155$.

Зауваження. При відшуканні лінійного представлення найбільшого спільного дільника двох цілих чисел бажано робити перевірку. В даному прикладі маємо:

$$121a - 155b = 121 \cdot 702 - 155 \cdot 548 = 84942 - 84240 = 2 = d.$$

в) За формулою (II.2) маємо:

$$[-702, 548] = \frac{|-702| \cdot |548|}{(-702, 548)} = \frac{702 \cdot 548}{2} = 351 \cdot 548 = 192348.$$

Розробка процедур. Для знаходження найбільшого спільного дільника двох цілих чисел a і b використовується команда **igcd(a,b)** із пакету **numtheory**. Але через громіздкість обчислень при розв'язанні даного завдання часто виникають помилки, тому бажано мати процедуру, яка б давала змогу перевірити проміжні обчислення. Створимо власну процедуру відшукання НСД двох чисел на основі алгоритму Евкліда. Обмежимось випадком, коли числа a і b – обидва натуральні. Така процедура буде більш простіша (не потрібно розглядати декілька випадків, використовуючи умовний оператор if), водночас, для перевірки проміжних обчислень її цілком достатньо, адже розв'язання зводиться до пошуку НСД двох натуральних чисел. У випадку, коли числа натуральні, для пошуку їхнього НСД можна використовувати вбудовані команди irem та iquo, про які йшла мова при розв'язанні Прикладу 1 (і не завантажувати додатково розроблені при розв'язанні Прикладу 1 процедури **quotient** і **remainder**).

Нижче наведено текст процедури. Відмітимо, що символ # використовується для коментування дій, що виконуються в межах процедури (це полегшує розуміння структури процедури), тому цей символ і частину рядка, яка розміщена справа від нього набирати не обов'язково. В ході даної процедури:

1) перевіряється, чи виконується умова: $a \vdots b$; якщо так, то найбільший спільний дільник знайдено: $d = b$;

2) в іншому випадку (тобто $a \overline{\vdots} b$) для зручності позначаємо $r_0 = b$, знаходимо неповну частку q_0 і остачу r_1 від ділення a на b;

3) виводимо на екран числа q_0 і r_1;

4) послідовно знаходимо неповні частки і остачі, поки не отримаємо остачу r_i, рівну 0; всі проміжні обчислення виводимо на екран;

5) цикл завершується, коли $r_i = 0$; в силу теореми про алгоритм Евкліда, $d = r_{i-1}$.

Окремо зауважимо, опис змінної q як глобальної, необхідний для того, щоб значення $q_0, q_1, ..., q_n$ (які в такому випадку система запам'ятовує) можна було використовувати для подальших обчислень поза межами процедури, а саме: при відщуканні лінійного представлення НСД чисел a і b. Оскільки в рівності алгоритму Евкліда числові значення підставляють лише для неповних часток $q_0, q_1, q_2, ...$, решту змінних, зокрема і $r_1, r_2, r_3, ...$, оголошуємо локальними.

```
gcdeuclid:=proc(a::posint,b::posint)
local d,i,r;
global q;
uses numtheory;
   if a mod b=0 then d:=b; #1
   else r[0]:=b; #2
      q[0]:=iquo(a,b);
      r[1]:=irem(a,b);
      print(‘ _q‘[0]=q[0],‘ _r‘[1]=r[1]); #3
      i:=1;
      while r[i]<>0 do #4
         q[i]:=iquo(r[i-1],r[i]);
         r[i+1]:=irem(r[i-1],r[i]);
         print(‘_q‘[i]=q[i],‘_r‘[i+1]=r[i+1]);
         i:=i+1;
      end do;
      d:=r[i-1]; #5
   end if;
   return(d);
end proc:
```

Розв'язання в Maple. Для перевірки лише остаточних результатів обчислень:

а) Для відшукання найбільшого спільного дільника використовуємо команду **igcd(a,b)** із пакету **numtheory**.

```
> with(numtheory):
> igcd(-702,548);
```

$$2$$

Отже, $(-702, 548) = 2$.

б) За допомогою команди **igcdex(a,b,'u','v')**, де **a,b** – задані числа, з пакету **numtheory** можна знайти числа u, v із лінійного представлення найбільшого спільного дільника. Числам u, v в результаті виконання команди буде присвоєне певне значення.

```
> with(numtheory):
> igcdex(-702,548,'u','v');
```

$$2$$

```
> u;v;
```

$$-121$$
$$-155$$

Отже, $2 = (-121)(-702) + (-155) \cdot 548$.

в) Для знаходження найменшого спільного кратного двох цілих чисел використовуємо команду **ilcm(a,b)**.

```
> with(numtheory):
> ilcm(-702,548);
```

$$192348$$

Таким чином, $[-702, 548] = 192348$.

Для перевірки проміжних обчислень підключаємо авторську бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Для чисел 702 і 548 матимемо:

```
> gcdeuclid(702,548);
```

$$\begin{gathered} \_q_1 = 1,\ \_r_1 = 154 \\ \_q_2 = 3,\ \_r_2 = 86 \\ \_q_3 = 1,\ \_r_3 = 68 \\ \_q_4 = 1,\ \_r_4 = 18 \\ \_q_5 = 3,\ \_r_5 = 14 \\ \_q_6 = 1,\ \_r_6 = 4 \\ \_q_7 = 3,\ \_r_7 = 2 \\ \_q_8 = 2,\ \_r_8 = 0 \\ 2 \end{gathered}$$

Найбільший спільний дільник заданих чисел дорівнює 2. Виражаємо остачі $r_1, r_2, r_3, ..., d$ (див. рівності (II.3)-(II.8)). Оскільки значення змінних $q_0, q_1, q_2, ...$ зберігається і поза межами процедури (а значить, їхні значення система пам'ятала), то отримаємо:

```
> r[1]:=a-b*q[0];
  r[2]:=b-r[1]*q[1];
  r[3]:=r[1]-r[2]*q[2];
  r[4]:=r[2]-r[3]*q[3];
  r[5]:=r[3]-r[4]*q[4];
  r[6]:=r[4]-r[5]*q[5];
  d:=r[5]-r[6]*q[6];
```

$$\begin{gathered} r_1 := a - b \\ r_2 := 4\,b - 3\,a \\ r_3 := 4\,a - 5\,b \\ r_4 := 9\,b - 7\,a \\ r_5 := 25\,a - 32\,b \end{gathered}$$

$$r_6 := 41\,b - 32\,a$$
$$d := 121\,a - 155\,b$$

В останньому рядку отримали лінійне представлення НСД чисел 702 і 548, яке має збігатись із отриманим при аналітичному розв'язанні.

Завдання 4. За допомогою алгоритму Евкліда знайти:

а) найбільший спільний дільник чисел a і b;
б) лінійне представлення (a, b);
в) найменше спільне кратне чисел a і b.

4.1. $a = 6120,\ b = -504.$

4.2. $a = -2442,\ b = 2370.$

4.3. $a = -6321,\ b = 4013.$

4.4. $a = -4030,\ b = 2315.$

4.5. $a = -7973,\ b = 3344.$

4.6. $a = 3120,\ b = -2325.$

4.7. $a = 2234,\ b = -2135.$

4.8. $a = -5577,\ b = 4031.$

4.9. $a = 2233,\ b = -2130.$

4.10. $a = 3243,\ b = -1224.$

4.11. $a = 2250,\ b = -731.$

4.12. $a = 6251,\ b = -777.$

4.13. $a = 6188,\ b = -2340.$

4.14. $a = -4968,\ b = 4815.$

4.15. $a = 6140,\ b = -6052.$

4.16. $a = 6715,\ b = -6120.$

4.17. $a = 1364,\ b = -1022.$

4.18. $a = 4242,\ b = -3120.$

4.19. $a = 3040,\ b = -1544.$

4.20. $a = -5716,\ b = 5183.$

4.21. $a = -6245,\ b = 6188.$

4.22. $a = -3090,\ b = 1045.$

4.23. $a = -5116,\ b = 2233.$

4.24. $a = 1723,\ b = -1540.$

4.25. $a = -1718,\ b = 1042.$

Приклад 5.1. Знайти натуральні числа a і b такі, що

$$\begin{cases} (a, b) = 26, \\ [a, b] = 4914. \end{cases}$$

Розв'язання. Оскільки $(a, b) = 26$, то існують такі натуральні числа a_1 і b_1, що $a = 26a_1$, $b = 26b_1$, причому $(a_1, b_1) = 1$. За формулою (II.2) маємо:

$$[a, b] = \frac{ab}{(a, b)} = \frac{26a_1 \cdot 26b_1}{26} = 26a_1b_1.$$

Враховуючи другу умову заданої системи, отримуємо: $4914 = 26a_1b_1$, звідки $a_1b_1 = 189$. Оскільки $(a_1, b_1) = 1$, а $189 = 3^3 \cdot 7$, можливі такі випадки:

а) $a_1 = 1$, $b_1 = 189$ або навпаки;
тоді $a = 26a_1 = 26$, $b = 26b_1 = 4914$ або $a = 4914$, $b = 26$;

б) $a_1 = 3^3$, $b_1 = 7$ або навпаки;
тоді $a = 702$, $b = 182$ або $a = 182$, $b = 702$.

Отже, числа a і b дорівнюють відповідно 26 і 4914 або 702 і 182, або навпаки.

Розв'язання в Maple. Розв'язування систем рівнянь такого виду (коли в рівняннях фігурують теоретико числові фуекції) в Maple здійснити не можна. Перевіримо, чи задовольняють умову знайдені при аналітичному розв'язанні пари чисел a і b:

```
> igcd(26,4914); ilcm(26,4914);
```

$$26$$
$$4914$$

```
> igcd(702,182); ilcm(702,182);
```

$$26$$
$$4914$$

Кожна із знайдених пар задовольняє умову. Але це не гарантує повністю правильну відповідь: при розв'язуванні можна було втратити розв'язки. Зробимо покрокову перевірку.

Нехай $d = (a, b)$, $m = [a, b]$, тобто:

```
> d:=26; m:=4914;
```

$$d := 26$$
$$m := 4914$$

Добуток a_1b_1 позначимо через z. Тоді:

```
> z:=m/d;
```

$$z := 189$$

Число z повинно розкладатись в добуток двох взаємнопростих натуральних чисел. Знайдемо всі натуральні дільники числа z:

```
> with(numtheory): M:=divisors(z);
```

$$M := \{1,\ 3,\ 7,\ 9,\ 21,\ 27,\ 63,\ 189\}$$

Елементи цієї множини можна викликати за їхнім номером i у вигляді $M[i]$ (див. §5 розд. I).

Для кожного із дільників $M[i]$ перевіримо, чи є взаємнопростими числа $M[i]$ і $\frac{z}{M[i]}$. Якщо так, то покладемо $a_1 = M[i]$, $b_1 = \frac{z}{M[i]}$ і знайдемо відповідні a і b.

```
> k:=tau(z):
  for i from 1 to k do
     if igcd(M[i],z/M[i])=1 then a1:=M[i]; b1:=z/M[i];
     a:=a1*d; b:=b1*d;
     print(a,b);
     end if;
  end do;
```

26, 4914
182, 702
702, 182
4914, 26

Отже, для чисел a і b можливі варіанти: $a = 26$, $b = 4914$ або навпаки; $a = 182$, $b = 702$ або навпаки.

Приклад 5.2. Знайти натуральні числа a і b такі, що

$$\begin{cases} a + b = 200, \\ (a, b) = 25. \end{cases}$$

Розв'язання. Оскільки $(a, b) = 25$, то існують такі натуральні числа a_1 і b_1, що $a = 25a_1$, $b = 25b_1$, причому $(a_1, b_1) = 1$. Тоді із першої умови заданої системи, отримуємо: $25a_1 + 25b_1 = 200$, звідки $a_1 + b_1 = 8$. Оскільки $(a_1, b_1) = 1$, то можливі лише такі випадки:

а) $a_1 = 1$, $b_1 = 7$ або навпаки;
тоді $a = 25a_1 = 25$, $b = 25b_1 = 175$ або $a = 175$, $b = 25$;

б) $a_1 = 3$, $b_1 = 5$ або навпаки;
тоді $a = 75$, $b = 125$ або $a = 125$, $b = 75$.

Отже, числа a і b дорівнюють відповідно 25 і 175 або 75 і 125, або навпаки.

Розв'язання в Maple. Зробимо покрокову перевірку, аналогічну до Прикладу 5.1.

Нехай $d = (a, b)$, $s = a + b$, тобто:

```
> d:=25; s:=200;
```

$$d := 25$$

$$s := 200$$

Суму $a_1 + b_1$ позначимо через z. Тоді:

```
> z:=s/d;
```

$$z := 8$$

Число z повинно розкладатись в суму двох взаємнопростих натуральних чисел. Переберемо всі такі варіанти: визначимо, чи є числа i та $z-i$ взаємно простими ($i = 1, 2, ..., z$). Якщо так, покладемо $a_1 = i$, $b_1 = z - i$ і знайдемо відповідні a і b.

```
> for i from 1 to z-1 do
    if igcd(i,z-i)=1 then a1:=i; b1:=z-i; a:=a1*d; b:=b1*d;
    print(a,b);
    end if;
  end do;
```

25, 175

75, 125

125, 75

175, 25

Отже, для чисел a і b можливі варіанти: $a = 25$, $b = 175$ або навпаки; $a = 75$, $b = 125$ або навпаки.

Завдання 5. Знайти натуральні числа a і b такі, що:

5.1. $\begin{cases} [a,b] = 390, \\ (a,b) = 15. \end{cases}$

5.2. $\begin{cases} a + b = 110, \\ (a,b) = 22. \end{cases}$

5.3. $\begin{cases} ab = 15750, \\ (a,b) = 15. \end{cases}$

5.4. $\begin{cases} \frac{a}{b} = \frac{7}{3}, \\ (a,b) = 24. \end{cases}$

5.5. $\begin{cases} [a,b] = 468, \\ ab = 5616. \end{cases}$

5.6. $\begin{cases} \frac{a}{(a,b)} + \frac{b}{(a,b)} = 14, \\ [a,b] = 726. \end{cases}$

5.7. $\begin{cases} (a,b) = 32, \\ [a,b] = 480. \end{cases}$

5.8. $\begin{cases} (a,b) = 22, \\ a + b = 176. \end{cases}$

5.9. $\begin{cases} (a,b) = 28, \\ [a,b] = 1428. \end{cases}$

5.10. $\begin{cases} ab = 1575, \\ [a,b] = 315. \end{cases}$

5.11. $\begin{cases} \frac{a}{b} = \frac{17}{20}, \\ (a,b) = 16. \end{cases}$

5.12. $\begin{cases} a + b = 150, \\ (a,b) = 15. \end{cases}$

5.13. $\begin{cases} (a,b)=32, \\ ab=56320. \end{cases}$

5.14. $\begin{cases} [a,b]=1260, \\ (a,b)=12. \end{cases}$

5.15. $\begin{cases} (a,b)=30, \\ a+b=150. \end{cases}$

5.16. $\begin{cases} \frac{b}{a}=\frac{21}{20}, \\ (a,b)=16. \end{cases}$

5.17. $\begin{cases} \frac{a}{(a,b)}+\frac{b}{(a,b)}=10, \\ [a,b]=315. \end{cases}$

5.18. $\begin{cases} (a,b)=21, \\ [a,b]=315. \end{cases}$

5.19. $\begin{cases} a+b=84, \\ [a,b]=12(a,b). \end{cases}$

5.20. $\begin{cases} (a,b)=14, \\ [a,b]=2254. \end{cases}$

5.21. $\begin{cases} ab=13500, \\ [a,b]=900. \end{cases}$

5.22. $\begin{cases} \frac{a}{(a,b)}+\frac{b}{(a,b)}=12, \\ [a,b]=1085. \end{cases}$

5.23. $\begin{cases} \frac{a}{b}=\frac{17}{15}, \\ (a,b)=23. \end{cases}$

5.24. $\begin{cases} a+b=138, \\ (a,b)=23. \end{cases}$

5.25. $\begin{cases} [a,b]=891, \\ ab=24057. \end{cases}$

3. Прості та складені числа

ТЕОРЕТИЧНІ ВІДОМОСТІ

Натуральне число $p \neq 1$ називається простим, якщо воно ділиться лише на ± 1 і $\pm p$. Натуральне число a називається складеним, якщо воно має дільники, відмінні від ± 1, $\pm a$. Якщо a – складене, то існує такий дільник b числа a, що $a = bc$, де $1 < b < a$, $1 < c < a$.

Властивості простих чисел

Нехай p – просте.

1. Якщо $p \vdots a$, $1 \neq a \in \mathbb{N}$, то $p = a$.
2. Для будь-якого $a \in \mathbb{Z}$ справедливо: або $a \vdots p$, або $(a,p)=1$.
3. Якщо $a_1 a_2 \dots a_n \vdots p$, то принаймні один із $a_i \vdots p$, $i \in \overline{1,n}$.
4. Найменший відмінний від одиниці дільник натурального числа $a > 1$ є простим.
5. Найменший простий дільник складеного числа a не більший за $\sqrt{a}$.

Із властивості 5 випливає, що якщо натуральне число $a \neq 1$ не ділиться на жодне просте число p таке, що $p \leqslant \sqrt{a}$, то a – просте; в іншому випадку, a – складене.

Для складання таблиці простих чисел, що не перевищують даного натурального числа a, використовують спосіб, який називається **решетом Ератосфена**. Він полягає в послідовному вилученні з ряду $1, 2, \dots, a$ числа 1, потім всіх чисел, кратних 2 (крім 2), потім – кратних 3 (крім 3) і т.д. (підкреслюють всі числа, кратні простим числам $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\dots$, $p_k \leqslant \sqrt{a}$, крім самих чисел p_i, $i \in \overline{1,k}$) (див. Приклад 6). Числа, що залишились непідкресленими, є простими.

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

Теорема (основна теорема арифметики)**.** *Будь-яке натуральне число $n > 1$ або є простим числом, або його можна записати, причому єдиним чином, у вигляді добутку простих чисел.*

Зауваження. Два добутки чисел, що відрізняються лише порядком запису співмножників, будемо вважати однаковими.

Якщо в розкладі натурального числа на прості множники об'єднати однакові множники, то дістанемо канонічний розклад (або канонічну форму) числа n :

$$n = p_1^{k_1} p_2^{k_2} ... p_m^{k_m}, \tag{II.9}$$

де $k_i \in \mathbb{N}$, $p_i \neq p_j$ при $i \neq j$ для всіх $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant m$. Всі дільники d цього числа вичерпуються числами виду:

$$d = p_1^{l_1} p_2^{l_2} ... p_m^{l_m}, \tag{II.10}$$

де $0 \leqslant l_i \leqslant k_i$ для всіх $i = 1, 2, ..., m$. Запис (II.10) називають узагальненим канонічним розкладом числа d (показники степенів можуть бути рівні нулю).

Якщо натуральні числа a і b мають узагальнені канонічні розклади

$$a = p_1^{k_1} p_2^{k_2} ... p_s^{k_s},\ b = p_1^{t_1} p_2^{t_2} ... p_s^{t_s},$$

$(k_i \geqslant 0, t_i \geqslant 0)$, то:

$$\begin{aligned} (a, b) &= p_1^{r_1} p_2^{r_2} ... p_s^{r_s},\ \text{де } r_i = \min_{1 \leqslant i \leqslant s} (k_i, t_i), \\ [a, b] &= p_1^{m_1} p_2^{m_2} ... p_s^{m_s},\ \text{де } m_i = \max_{1 \leqslant i \leqslant s} (k_i, t_i). \end{aligned} \tag{II.11}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 6. Знайти всі прості числа, які містяться між числами 1820 і 1880.

Розв'язання. Числа 1820 і 1880, а також всі парні числа, що містяться між ними, є складеними, тому випишемо лише всі непарні числа між 1820 і 1880:

$$\begin{aligned} &1821, 1823, 1825, 1827, 1829, 1831, 1833, 1835, 1837, 1839, \\ &1841, 1843, 1845, 1847, 1849, 1851, 1853, 1855, 1857, 1859, \\ &1861, 1863, 1865, 1867, 1869, 1871, 1873, 1875, 1877, 1879. \end{aligned} \tag{II.12}$$

Число цього ряду є простим, якщо воно не ділиться на жодне просте число (крім самого себе), яке не перевищує $\sqrt{1879}$. Оскільки $43 < \sqrt{1879} < 44$, випишемо всі прості числа, які більші за 2 і не перевищують 43. Ними є:

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.$$

Підкреслимо числа ряду (II.12), кратні 3:

$$\underline{1821}, 1823, 1825, \underline{1827}, 1829, 1831, \underline{1833}, 1835, 1837, \underline{1839},$$
$$1841, 1843, \underline{1845}, 1847, 1849, \underline{1851}, 1853, 1855, \underline{1857}, 1859,$$
$$1861, \underline{1863}, 1865, 1867, \underline{1869}, 1871, 1873, \underline{1875}, 1877, 1879.$$

Потім серед тих, що залишились непідкресленими, шукаємо числа, кратні 5. Це числа: 1825, 1835, 1855, 1865. Підкреслимо їх:

$$\underline{1821}, 1823, \underline{1825}, \underline{1827}, 1829, 1831, \underline{1833}, \underline{1835}, 1837, \underline{1839},$$
$$1841, 1843, \underline{1845}, 1847, 1849, \underline{1851}, 1853, \underline{1855}, \underline{1857}, 1859,$$
$$1861, \underline{1863}, \underline{1865}, 1867, \underline{1869}, 1871, 1873, \underline{1875}, 1877, 1879.$$

Далі серед непідкреслених визначаємо числа, кратні 7. Таким є лише число 1841. Підкреслимо його. На число 11 діляться числа 1837, 1859. Підкреслимо їх. Маємо:

$$\underline{1821}, 1823, \underline{1825}, \underline{1827}, 1829, 1831, \underline{1833}, \underline{1835}, \underline{1837}, \underline{1839},$$
$$\underline{1841}, 1843, \underline{1845}, 1847, 1849, \underline{1851}, 1853, \underline{1855}, \underline{1857}, \underline{1859},$$
$$1861, \underline{1863}, \underline{1865}, 1867, \underline{1869}, 1871, 1873, \underline{1875}, 1877, 1879.$$

Непідкреслених чисел, кратних 13, немає, на 17 ділиться число 1853, а на 19 – число 1843. Чисел, кратних 23 і 29, немає. Далі, на 31 ділиться число 1829, а кратних 37 і 41 немає. І на 43 ділиться число 1849. Підкреслюємо і ці числа. Остаточно маємо:

$$\underline{1821}, 1823, \underline{1825}, \underline{1827}, \underline{1829}, 1831, \underline{1833}, \underline{1835}, \underline{1837}, \underline{1839},$$
$$\underline{1841}, \underline{1843}, \underline{1845}, 1847, \underline{1849}, \underline{1851}, \underline{1853}, \underline{1855}, \underline{1857}, \underline{1859},$$
$$1861, \underline{1863}, \underline{1865}, 1867, \underline{1869}, 1871, 1873, \underline{1875}, 1877, 1879.$$

Числа, що залишились непідкресленими, є простими. Таким чином, простими числами, що містяться між числами 1820 і 1880 є: 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879.

Розробка процедур. Для перевірки числа a на простоту використовується команда **isprime(a)**, результатом якої є **true**, якщо число просте, і **false**, якщо складене. Створимо процедуру **sieve** для відшукання простих чисел на проміжку $[a, b]$. В результаті виконання циклу for кожне число від a до b підлягатиме перевірці на простоту: якщо число просте, то воно виводиться на екран.

```
sieve:=proc(a::posint,b::posint)
local d,i,r;
global q;
uses numtheory;
   for i from a to b do
      if isprime(i)=true then print(i) end if;
   end do;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку **atchlib**

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо команду **sieve**:

```
> sieve(1820,1880);
```

1823
1831
1847
1861
1867
1871
1873
1877
1879

Завдання 6. Знайти всі прості числа, які містяться між числами:

6.1. 1200 і 1250.

6.2. 2020 і 2070.

6.3. 2202 і 2262.

6.4. 2905 і 2965.

6.5. 1808 і 1868.

6.6. 1470 і 1520.

6.7. 3015 і 3075.

6.8. 1300 і 1350.

6.9. 2034 і 2094.

6.10. 1907 і 1972.

6.11. 2412 і 2462.

6.12. 2813 і 2873.

6.13. 1314 і 1380.

6.14. 2031 і 2091.

6.15. 1458 і 1512.

6.16. 1011 і 1100.

6.17. 2354 і 2404.

6.18. 1400 і 1450.

6.19. 2953 і 3003.

6.20. 2315 і 2375.

6.21. 1112 і 1172.

6.22. 2770 і 2823.

6.23. 1220 і 1280.

6.24. 2703 і 2783.

6.25. 1999 і 2061.

Приклад 7. Використовуючи канонічні розклади, знайти найбільший спільний дільник і найменше спільне кратне чисел 3780 і 4950.

Розв'язання. Розкладемо кожне із цих чисел на прості множники. Оскільки $3780 = 2 \cdot 1890$, $1890 = 2 \cdot 945$, $945 = 3 \cdot 315$, $315 = 3 \cdot 105$, $105 = 3 \cdot 35$, $35 = 5 \cdot 7$, то $3780 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7$. Скорочено цей процес записують наступним чином:

3780	2
1890	2
945	3
315	3
105	3
35	5
7	7
1	

Аналогічно знаходимо розклад числа 4950:

4950	2
2475	3
825	3
275	5
55	5
11	11
1	

Канонічні розклади даних чисел мають вигляд:

$$\begin{aligned} 3780 &= 2^2 \cdot 3^3 \cdot 5 \cdot 7, \\ 4950 &= 2 \cdot 3^2 \cdot 5^2 \cdot 11, \end{aligned}$$

а узагальнені канонічні розклади:

$$\begin{aligned} 3780 &= 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^0, \\ 4950 &= 2^1 \cdot 3^2 \cdot 5^2 \cdot 7^0 \cdot 11^1. \end{aligned}$$

За формулами (II.11)

$$\begin{aligned}(3780, 4950) &= 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^0 = 90;\\ [3780, 4950] &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot 11^1 = 207900.\end{aligned}$$

Зауваження. Шукаючи канонічний розклад числа виду $m \cdot 10^k$, можна спочатку знайти канонічний розклад числа m і помножити отриманий результат на $2^k \cdot 5^k$. В даному прикладі $3780 = 378 \cdot 10$. Оскільки $378 = 2 \cdot 3^3 \cdot 7$, то $3780 = 2 \cdot 3^3 \cdot 7 \cdot (2 \cdot 5) = 2^2 \cdot 3^3 \cdot 5 \cdot 7$.

Розв'язання в Maple. Для перевірки лише остаточного результату достатньо використати команди igcd та ilcm (див. Приклад 4.1). Виконаємо покрокову перевірку.

Для розкладу числа a на прості множники використовуються команди **ifactor(a)** і **ifactors(a)**. Перша з них повертає результат у вигляді добутку степенів простих чисел, друга – у вигляді списку простих чисел і показників степенів. Канонічні розклади kr1 і kr2 чисел 3780 і 4950 матимуть вигляд:

```
> with(numtheory):
> kr1:=ifactor(3780);
```

$$kr1 := (2)^2\ (3)^3\ (5)\ (7)$$

```
> kr2:=ifactor(4950);
```

$$kr2 := (2)\ (3)^2\ (5)^2\ (11)$$

Тепер, щоб знайти найбільший спільний дільник і найменше спільне кратне чисел a і b, використовуємо не команду igcd(a,b), а більш загальну команду gcd(a,b).

Причина в тому, що параметрами команди igcd мають бути цілі числа, а вирази виду $(2)(3)^2(5)^2(11)$ система цілим числом не вважає (це лише форма запису, такий вираз має тип *):

```
> type(kr1,integer);
```

$$false$$

```
> whattype(kr1);
```

$$*$$

Знаходимо канонічні розклади найбільшого спільного дільника і найменшого спільного кратного:

```
> gcd(kr1,kr2);
```

$$(2)\ (3)^2\ (5)$$

```
> lcm(kr1,kr2);
```

$$(2)^2\ (3)^3\ (7)\ (5)^2\ (11)$$

Обчислимо отримані добутки. Щоб не вводити самі добутки, застосуємо нульарний оператор %%:

```
> expand(%%);
```

$$90$$

```
> expand(%%);
```

$$207900$$

Таким чином, $(3780, 4950) = 90$, $[3780, 4950] = 207900$.

Завдання 7. Використовуючи канонічні розклади, знайти найбільший спільний дільник і найменше спільне кратне чисел a і b, якщо:

7.1. $a = 5940, \quad b = 3234.$

7.2. $a = 1960, \quad b = 4550.$

7.3. $a = 7605, \quad b = 728.$

7.4. $a = 10800, \quad b = 9100.$

7.5. $a = 8064, \quad b = 6480.$

7.6. $a = 8460, \quad b = 26460.$

7.7. $a = 6762, \quad b = 20475.$

7.8. $a = 7800, \quad b = 20592.$

7.9. $a = 78624, \quad b = 4900.$

7.10. $a = 10752, \quad b = 5236.$

7.11. $a = 1728, \quad b = 5880.$

7.12. $a = 84525, \quad b = 2160.$

7.13. $a = 11424, \quad b = 6175.$

7.14. $a = 4550, \quad b = 6048.$

7.15. $a = 14553, \quad b = 5508.$

7.16. $a = 5040, \quad b = 29376.$

7.17. $a = 3024, \quad b = 4480.$

7.18. $a = 3672, \quad b = 218700.$

7.19. $a; = 1152, \quad b = 5355.$

7.20. $a = 9702, \quad b = 145800.$

7.21. $a = 15525, \quad b = 6435.$

7.22. $a = 5376, \quad b = 9216.$

7.23. $a = 5880, \quad b = 14400.$

7.24. $a = 1848, \quad b = 4704.$

7.25. $a = 58995, \quad b = 2025.$

4. Числові функції

ТЕОРЕТИЧНІ ВІДОМОСТІ

Функцію $f(x)$ називають **числовою**, якщо вона визначена при всіх натуральних значеннях аргументу x.

Через $\tau(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює числу всіх його натуральних дільників.

Через $\sigma(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює сумі всіх його натуральних дільників.

Через $\varphi(n)$ позначають числову функцію, значення якої для будь-якого натурального числа n дорівнює кількості натуральних чисел, взаємно простих з n, які не перевищують n. Функцію $\varphi(n)$ називають функцією Ойлера.

Через $[x]$ (читається „антьє від x") позначають числову функцію, значення якої для будь-якого дійсного числа x дорівнює найбільшому цілому числу, що не перевищує x. Функцію $[x]$ називають цілою частиною від x.

Через $\{x\}$ позначають числову функцію, значення якої для будь-якого дійсного числа x дорівнює різниці $x - [x]$. Функція $\{x\}$ називається дробовою частиною від x.

Числова функція $f(n)$ називається **мультиплікативною**, якщо:

1) для деякого натурального n_0 $f(n_0) \neq 0$;
2) для довільних натуральних взаємно простих n_1 і n_2 справедлива рівність: $f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2)$.

Властивості мультиплікативних функцій:

1. $f(1) = 1$.
2. Добуток мультиплікативних функцій є мультиплікативною функцією.
3. Якщо $n_1, n_2, ..., n_k$ – попарно взаємно прості числа, то $f(n_1 \cdot n_2 \cdot ... \cdot n_k) = f(n_1) \cdot f(n_2) \cdot ... \cdot f(n_k)$.
4. Якщо $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$ – канонічна форма натурального числа n, то $f(n) = f(p_1^{k_1}) \cdot f(p_2^{k_2}) \cdot ... \cdot f(p_s^{k_s})$.

Числові функції $\tau(n)$, $\sigma(n)$, $\varphi(n)$ – мультиплікативні.

Якщо $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$ – канонічний розклад натурального числа n, то:

$$\tau(n) = (k_1 + 1)(k_2 + 1)...(k_s + 1), \tag{II.13}$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot ... \cdot \frac{p_s^{k_s+1} - 1}{p_s - 1}, \tag{II.14}$$

$$\begin{aligned} \varphi(n) &= n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)...\left(1 - \tfrac{1}{p_s}\right) = \\ &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)...\left(p_s^{k_s} - p_s^{k_s-1}\right). \end{aligned} \tag{II.15}$$

Зокрема, якщо p – просте число, $k \in \mathbb{N}$, то $\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$, $\varphi(p) = p - 1$.

Нехай $x, y \in \mathbb{R}$, $k \in \mathbb{Z}$, $n \in \mathbb{N}$. Тоді:

1♯. $[x + k] = [x] + k$.
2♯. $[x + y] \geqslant [x] + [y]$.
3♯. Якщо $[x] = [y]$, то $-1 < x - y < 1$.
4♯. Якщо $x > 0$, то натуральних чисел, які не перевищують x і діляться на n, буде рівно $\left[\frac{x}{n}\right]$.
5♯. $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

Показник k простого числа p, яке входить до канонічного розкладу натурального числа $n!$, обчислюється за формулою

$$k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... + \left[\frac{n}{p^s}\right], \quad \text{де} \quad p^s \leqslant n < p^{s+1}. \tag{II.16}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 8.1. Знайти натуральне число n, якщо n має тільки два різних простих дільники, $\tau(n) = 12$, $\sigma(n) = 504$.

Розв'язання. Оскільки число n має лише два різних простих дільники, то його канонічний розклад має вигляд

$$n = p_1^{k_1} p_2^{k_2}, \quad \text{де} \quad k_1, k_2 \geqslant 1.$$

Тоді $k_1 + 1 \geqslant 2$, $k_2 + 1 \geqslant 2$. За формулами (II.13) і (II.14) маємо:

$$\begin{cases} (k_1+1)(k_2+1) = 12, \\ \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} = 504. \end{cases} \tag{II.17}$$

Нехай $k_1 \leqslant k_2$.

Спосіб І. Із умов $k_1 + 1 \geqslant 2$, $k_2 + 1 \geqslant 2$ Можливі наступні випадки:

1) $\begin{cases} 1 + k_1 = 2, \\ 1 + k_2 = 6; \end{cases}$ тобто $\begin{cases} k_1 = 1, \\ k_2 = 5. \end{cases}$

2) $\begin{cases} 1 + k_1 = 3, \\ 1 + k_2 = 4; \end{cases}$ тобто $\begin{cases} k_1 = 2, \\ k_2 = 3. \end{cases}$

Розглянемо їх.

Випадок 1): $\begin{cases} k_1 = 1, \\ k_2 = 5. \end{cases}$. Підставимо ці значення в другу рівність системи (II.17). Маємо: $\frac{p_1^2-1}{p_1-1} \cdot \frac{p_2^6-1}{p_2-1} = 504$ або після спрощення:

$$(p_1 + 1)(p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1) = 504. \tag{II.18}$$

Оскільки $p_1 \geqslant 2$, то вираз $p_2^5+p_2^4+p_2^3+p_2^2+p_2+1 \geqslant 2^5+2^4+2^3+2^2+2+1 = 63$. Тоді перший множник $(p_1 + 1)$ не перевищує числа $\left[\frac{504}{63}\right] = 8$. Знайдемо всі можливі дільники числа 504, які не перевищують 8. Ними є: 2, 3, 4, 6, 7, 8. Оскільки p_1 – просте число, то $(p_1 + 1)$ може набувати лише значень 3, 4, 6, 8, тобто $p_1 \in \{2; 3; 5; 7\}$. Дослідимо кожне із значень.

Нехай $p_1 = 2$. Підставляючи в рівність (II.24), маємо:

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 168$$

або

$$p_2(p_2^4 + p_2^3 + p_2^2 + p_2 + 1) = 167, \tag{II.19}$$

звідки $p_2 | \, 167$. Проте 167 – просте, тому рівність (II.19) можлива лише у випадку $p_2 = 167$, але тоді множник $(p_2^4 + p_2^3 + p_2^2 + p_2 + 1)$ дорівнює 1, що неможливо.

Нехай $p_1 = 3$. Із рівності (II.24) маємо:

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 126$$

або

$$p_2(p_2^4 + p_2^3 + p_2^2 + p_2 + 1) = 125.$$

Оскільки p_2 – простий дільник числа 125, то це можливо лише у випадку

$$\begin{cases} p_2 = 5, \\ p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 25. \end{cases}$$

Проте дана система несумісна.

Нехай $p_1 = 5$. Із рівності (II.24) отримуємо:

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 84$$

або

$$p_2(p_2^4 + p_2^3 + p_2^2 + p_2 + 1) = 83,$$

Оскільки 83 – просте число і в добуток нетривіальних множників не розкладається, то таке рівняння розв'язків в простих числах не має.

Залишається розглянути випадок $p_1 = 7$. Підставимо в рівність (II.24):

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 63$$

або

$$p_2(p_2^4 + p_2^3 + p_2^2 + p_2 + 1) = 62. \tag{II.20}$$

Число 62 має 2 прості дільники: 2 і 31. Оскільки, $p_2 < (p_2^4 + p_2^3 + p_2^2 + p_2 + 1)$, то рівняння (II.20) має розв'язок (який є простим числом) лише тоді, коли

$$\begin{cases} p_2 = 2, \\ p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 31. \end{cases}$$

Дана система сумісна, отже, $p_2 = 2$, $p_1 = 7$, а шукане число $n = 7^1 \cdot 2^5$.

Тепер розглянемо **випадок 2)**: $\begin{cases} k_1 = 2, \\ k_2 = 3. \end{cases}$ Підставимо ці значення в другу рівність системи (II.17). Маємо: $\frac{p_1^3-1}{p_1-1} \cdot \frac{p_2^4-1}{p_2-1} = 504$ або після спрощення:

$$(p_1^2 + p_1 + 1)(p_2^3 + p_2^2 + p_2 + 1) = 504. \qquad \text{(II.21)}$$

Безпосередньо переконуємось, що p_2 не може дорівнювати 2. Отже, $p_2 \geqslant 3$. Але тоді $p_2^3 + p_2^2 + p_2 + 1 \geqslant 3^3 + 3^2 + 3 + 1 = 40$, звідки перший множник не може перевищувати числа $\left[\frac{504}{40}\right] = 12$. Отже,

$$p_1^2 + p_1 + 1 \leqslant 12.$$

Таким простим числом може бути лише число 2. Підставимо значення $p_1 = 2$ в рівність (II.21). Матимемо: $p_2^3 + p_2^2 + p_2 + 1 = 72$ або

$$p_2(p_2^2 + p_2 + 1) = 71. \qquad \text{(II.22)}$$

Оскільки число 71 – просте, то, очевидно, рівняння (II.22) розв'язків в простих числах не має.

Всі випадки розглянуто. Єдиним числом, що задовольняє умову, є число $n = 7 \cdot 2^5$.

Спосіб II. Як раніше було показано, $n = p_1^{k_1} p_2^{k_2}$ і справедливі формули (II.17). Нехай $1 \leqslant k_1 \leqslant k_2$. Тоді $k_1+1 \geqslant 2$, $k_2+1 \geqslant 2$. З умови $(k_1+1)(k_2+1) = 12$ випливає, що можливі такі випадки: $k_1+1 = 2$, $k_2+1 = 6$; або $k_1+1 = 3$, $k_2 + 1 = 4$. Тоді: 1) $k_1 = 1$, $k_2 = 5$; 2) $k_1 = 2$, $k_2 = 3$.

Випадок 1): Нехай $k_1 = 1$, $k_2 = 5$. Підставимо ці значення в друге рівняння системи (II.17):

$$\frac{p_1^2 - 1}{p_1 - 1} \cdot \frac{p_2^6 - 1}{p_2 - 1} = 504$$

або після спрощення:

$$(p_1 + 1)(p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1) = 504. \qquad \text{(II.23)}$$

Нехай $p_2 = 2$. Тоді

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 32 + 16 + 8 + 4 + 2 + 1 = 63,$$

значить, $p_1 + 1 = 504 : 63 = 8$. Звідси $p_1 = 7$. Таким чином, $n = p_1^{k_1} p_2^{k_2} = 7^1 \cdot 2^5 = 224$.

Нехай $p_2 = 3$. Тоді

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 = 243 + 81 + 27 + 9 + 3 + 1 = 364.$$

Оскільки $364 \nmid 504$, то p_2 не може дорівнювати 3.

Якщо $p_2 \geqslant 5$, то

$$p_2^5 + p_2^4 + p_2^3 + p_2^2 + p_2 + 1 \geqslant 5^5 + 5^4 + 5^3 + 5^2 + 5 + 1 > 504,$$

що неможливо.

Випадок 2): Нехай $k_1 = 2$, $k_2 = 3$. Тоді

$$\frac{p_1^3 - 1}{p_1 - 1} \cdot \frac{p_2^4 - 1}{p_2 - 1} = 504$$

або після спрощення:

$$(p_1^2 + p_1 + 1)(p_2^3 + p_2^2 + p_2 + 1) = 504. \qquad \text{(II.24)}$$

Якщо $p_2 = 2$, то

$$p_2^3 + p_2^2 + p_2 + 1 = 8 + 4 + 2 + 1 = 15.$$

Оскільки $15 \nmid 504$, то p_2 не може дорівнювати 2.

Якщо $p_2 = 3$, то $p_2^3 + p_2^2 + p_2 + 1 = 27 + 9 + 3 + 1 = 40 \nmid 504$;
якщо $p_2 = 5$, то $p_2^3 + p_2^2 + p_2 + 1 = 125 + 25 + 5 + 1 = 156 \nmid 504$;
якщо $p_2 = 7$, то $p_2^3 + p_2^2 + p_2 + 1 = 343 + 49 + 7 + 1 = 400 \nmid 504$.

Якщо $p_2 \geqslant 11$, то

$$p_2^3 + p_2^2 + p_2 + 1 \geqslant 11^3 + 11^2 + 11 + 1 > 504,$$

що неможливо.

Отже, єдиним числом, що задовольняє умову задачі, є число $n = 224$.

Розв'язання в Maple. Перевіримо, чи задовольняє умову $n = 224$. Знайдемо $\tau(n)$ і $\sigma(n)$:

```
> with(numtheory):
> tau(7*2^5);
```

12

```
> sigma(7*2^5);
```

504

Отже, число 224 задовольняє умову. Але чи немає інших чисел, що задовольняють умову?

Повторимо міркування в Maple. Використаємо спосіб II розв'язання. Знайдемо натуральні числа k_1 і k_2, що задовольняють умову $(k_1+1)(k_2+1)=12$. Для цього знаходимо всі натуральні дільники числа 12:

```
> with(numtheory): M:=divisors(12);
```

$$M := \{1,\ 2,\ 3,\ 4,\ 6,\ 12\}$$

Отже, $k_1+1 \in \{1,2,3,4,6,12\}$, $k_1+2 \in \{1,2,3,4,6,12\}$. Оскільки числа k_1 і k_2 мають бути натуральними, то серед чисел $M[i]$ цієї множини вибираємо такі, що $M[i] \geqslant 2$ і $M[i] \leqslant 11$:

```
> for i from 1 to tau(12) do
    if M[i]>=2 and M[i]<=11 then
    k1:=M[i]-1; k2:=12/M[i]-1; print(k1,k2);
    end if;
  end do;
```

$$1,\ 5$$
$$2,\ 3$$
$$3,\ 2$$
$$5,\ 1$$

Нехай $k_1 \leqslant k_2$. Тоді: 1) $k_1=1$, $k_2=5$; 2) $k_1=2$, $k_2=3$.

Випадок 1): $k_1=1$, $k_2=5$. Підставимо значення k_1 і k_2 в друге рівняння системи (II.17). Для зручності позначимо частку $\frac{p_1^{k_1+1}-1}{p_1-1}$ через $s1$, а частку $\frac{p_2^{k_2+1}-1}{p_2-1}$ через $s2$.

```
> k1:=1: k2:=5:
  s1:=(p1^(k1+1)-1)/(p1-1):
  s2:=(p2^(k2+1)-1)/(p2-1):
```

Знайдемо значення виразу $s2$ при $p2=2$, позначимо його через $c2$:

```
> c2:=subs({p2=2},s2);
```

$$c2 := 63$$

Знайдемо тепер розв'язки рівняння $s2 \cdot c2 = 504$ в цілих числах:

```
> isolve(s1*c2=504);
```

$$\{p1 = 7\}$$

Отже, числа $p_1=7$ і $p_2=2$ задовольняють друге рівняння системи (II.17). Тоді

```
> n=7^(1)*2^(5);
```

$$n = 224$$

Перевіримо, чи немає інших пар простих чисел p_1 і p_2, що задовольняють

друге рівняння системи (II.17). Підставимо замість p_2 число 3 і подивимось, чи має розв'язки в цілих числах рівняння $s1 \cdot c2 = 504$:

```
> c2:=subs({p2=3},s2);
```

$$c2 := 364$$

```
> isolve(s1*c2=504);
```

Розв'язків немає. Далі підставляємо $p_2 = 5$.

```
> c2:=subs({p2=5},s2);
```

$$c2 := 3906$$

В цьому випадку $c_2 = 3906 > 504$. Зрозуміло, що в цьому випадку і далі при $p_2 > 5$ простих чисел p_1, що задовольняють друге рівняння системи (II.17), не існує.

Випадок 2: $k_1 = 2$, $k_2 = 3$. Повторюючи аналогічні міркування, послідовно надаватимемо числу p_2 значень 2, 3, 5, ... Важливо: бажано ввести команду restart!

```
> restart:
  k1:=2: k2:=3:
  s1:=(p1^(k1+1)-1)/(p1-1):
  s2:=(p2^(k2+1)-1)/(p2-1):
> c2:=subs({p2=2},s2); isolve(s1*c2=504);
```

$$c2 := 15$$

```
> c2:=subs({p2=3},s2); isolve(s1*c2=504);
```

$$c2 := 40$$

```
> c2:=subs({p2=5},s2); isolve(s1*c2=504);
```

$$c2 := 156$$

```
> c2:=subs({p2=7},s2); isolve(s1*c2=504);
```

$$c2 := 400$$

```
> c2:=subs({p2=11},s2); isolve(s1*c2=504);
```

$$c2 := 1464$$

Бачимо, що в жодному із випадків рівняння $s1 \cdot c2 = 504$ не має розв'язків в цілих числах. При $c_2 = 1464$ підстановку можна завершити. Отже, єдиним числом, що задовольняє систему рівнянь (II.17), є число $n = 224$.

Приклад 8.2. Знайти натуральне число n, якщо n – найменше натуральне число, для якого $\tau(n) = 45$.

Розв'язання. Нехай $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$ – канонічний розклад числа n. Тоді $p_i \neq p_j$ при $i \neq j$. За формулою для числа $\tau(n)$ матимемо: $(k_1+1)(k_2+1)...(k_s+1) = 45$. Оскільки $k_i \geqslant 0$ для всіх $i \in \overline{1,s}$, то

$$k_i + 1 \geqslant 1 \text{ для всіх } i \in \overline{1,s}. \tag{II.25}$$

Не порушуючи загальності, можна вважати, що $k_1 \leqslant k_2 \leqslant ... \leqslant k_s$. Тоді

$$k_i + 1 \leqslant k_2 + \leqslant ... \leqslant k_s + 1. \tag{II.26}$$

Розглянемо всі можливі розклади числа 45 в добуток натуральних чисел $k_i + 1$, що задовольняють умови (II.25) і (II.26).

Якщо множників лише $s = 2$, то такими розкладами є: $3 \cdot 15$ і $5 \cdot 9$. Якщо множників $s = 3$, то такий розклад лише один: $3 \cdot 3 \cdot 5$. Крім того, можливий випадок $s = 1$.

Розглянемо кожен із випадків:

а) $k_1 + 1 = 3$, $k_2 + 1 = 15$, тоді $k_1 = 2$, $k_2 = 14$ і $n = p_1^2 p_2^{14}$.

б) $k_1 + 1 = 5$, $k_2 + 1 = 9$, тоді $k_1 = 4$, $k_2 = 8$ і $n = p_1^4 p_2^8$.

в) $k_1 + 1 = 3$, $k_2 + 1 = 3$, $k_3 + 1 = 5$, тоді $k_1 = 2$, $k_2 = 2$, $k_3 = 4$ і $n = p_1^2 p_2^2 p_3^4$.

г) $k_1 + 1 = 45$, тоді $k_1 = 44$ $n = p_1^{44}$.

В кожному із випадків знайдемо найменше натуральне число відповідного виду:

а) найменше натуральне число виду $n = p_1^2 p_2^{14}$ отримаємо при $p_2 = 2$, $p_1 = 3$; отже, $n = 3^2 \cdot 2^{14} = 147456$;

б) найменше число виду $n = p_1^4 p_2^8$ матимемо при $p_2 = 2$, $p_1 = 3$; отже, $n = 3^4 \cdot 2^8 = 20736$;

в) найменше число виду $n = p_1^2 p_2^2 p_3^4$ одержимо при $p_3 = 2$, $p_1 = 3$, $p_2 = 5$; отже, $n = 3^2 \cdot 5^2 \cdot 2^4 = 3600$;

г) найменше число виду $n = p_1^{44}$ – це число $n = 2^{44}$;

Найменше серед чисел у випадках а)-г) – число 3600.

Розв'язання в Maple. За допомогою циклу перевіримо всі числа i від 1 до 100000. Оскільки нас цікавить лише найменше число i, для якого $\tau(i) = 45$, то як тільки таке число знайдене, процес перевірки припиняємо (за допомогою ключового слова break).

```
> for i from 1 to 100000 do
    if tau(i)=45 then print(i); break; end if;
  end do;
```

3600

Число 3600 – найменше серед натуральних чисел, кількість дільників якого дорівнює 45.

Приклад 8.3. Знайти натуральне число n, якщо $n = 2^x \cdot 3^y \cdot 5^z$, причому $\tau(n) = 60$, $\tau(2n) = 75$, $\tau(3n) = 80$.

Розв'язання. Оскільки $2n = 2^{x+1} \cdot 3^y \cdot 5^z$, то $\tau(2n) = (x+2)(y+1)(z+1)$; аналогічно, $5n = 2^x \cdot 3^y \cdot 5^{z+1}$, тому $\tau(5n) = (x+1)(y+1)(z+2)$. За умовою матимемо систему рівнянь:

$$\left\{\begin{array}{rcl}(x+1)(y+1)(z+1) &=& 60,\\ (x+2)(y+1)(z+1) &=& 75,\\ (x+1)(y+1)(z+2) &=& 80.\end{array}\right. \qquad \text{(II.27)}$$

Для її розв'язання домножимо обидві частини 2-го рівняння на $(x+1)$ і обидві частини 3-го рівняння на $(z+1)$:

$$\left\{\begin{array}{rcl}(x+1)(y+1)(z+1) &=& 60,\\ (x+1)(y+1)(z+1)(x+2) &=& 75(x+1),\\ (x+1)(y+1)(z+1)(z+2) &=& 80(z+2);\end{array}\right.$$

тоді, підставивши в 2-ге рівняння замість $(x+1)(y+1)(z+1)$ число 60, отримаємо: $60(x+2) = 75(x+1)$, звідки $x = 3$, і, аналогічно, з 3-го рівняння матимемо: $60(z+2) = 80(z+1)$, звідки $z = 2$. Далі $y+1 = \frac{60}{(x+1)(z+1)} = \frac{60}{4\cdot 3} = 5$. Таким чином, $n = 2^3 \cdot 3^4 \cdot 5^2 = 16200$.

Розв'язання в Maple. Перевіримо, чи задовольняє умову отриманий розв'язок:

```
> with(numtheory):
  tau(16200); tau(2*16200); tau(5*16200);
```

60

75

80

Розв'яжемо систему рівнянь (II.27) в Maple, щоб переконатись, що жодного розв'язку не було втрачено. Для розв'язування систем рівнянь використовується команда solve у форматі **solve({eq1, eq2,...}, {x,y,...})** (див. §7 розд.I).

```
> solve({(x+1)*(y+1)*(z+1)=60,(x+2)*(y+1)*(z+1)=75,(x+1)*(y+1)*(z+2)=8
  {x,y,z});
```

$$\{x = 3,\ y = 4,\ z = 2\}$$

Отже, система має єдиний розв'язок: $x = 3$, $y = 4$, $z = 2$, тоді шукане число $n = 2^3 \cdot 3^4 \cdot 5^2 = 16200$.

Завдання 8. Знайти натуральне число n, якщо:

8.1. n ділиться лише на два різних простих числа, $\tau(n) = 9$, $\sigma(n) = 403$.

8.2. $n \vdots 45$ і $\tau(n) = 18$.

8.3. n – найменше натуральне число, для якого $\tau(n) = 12$.

8.4. $n = 2^x \cdot 3^y \cdot 5^z$, $\tau(n) = 36$, $\tau(2n) = 48$, $\tau(3n) = 45$.

8.5. n має лише два різних простих дільники, $\tau(n) = 10$, $\sigma(n) = 186$.

8.6. $n \vdots 50$ і $\tau(n) = 10$.

8.7. n – найменше натуральне число, для якого $\tau(n) = 20$.

8.8. n має тільки два різних простих дільники, $\tau(n) = 12$, $\sigma(n) = 195$.

8.9. n ділиться лише на два різних простих числа, $\tau(n) = 18$, $\sigma(n) = 2044$.

8.10. n ділиться на 2 і на 9, і має 14 дільників.

8.11. $n \vdots 40$ і $\tau(n) = 15$.

8.12. $n = 3^x \cdot 5^y \cdot 7^z$, $\tau(n) = 24$, $\tau(3n) = 36$, $\tau(5n) = 32$.

8.13. n має лише два різних простих дільники, $\tau(n) = 8$, $\sigma(n) = 320$.

8.14. n ділиться лише на два різних простих числа, $\tau(n) = 6$, $\sigma(n) = 104$.

8.15. $n \vdots 54$ і $\tau(n) = 14$.

8.16. n має тільки два різних простих дільники, $\tau(n) = 10$, $\sigma(n) = 372$.

8.17. n – найменше натуральне число, для якого $\tau(n) = 28$.

8.18. $n = 2^x \cdot 3^y \cdot 7^z$, $\tau(2n) = 24$, $\tau(8n) = 36$, $\tau(9n) = 36$.

8.19. n має лише два різних простих дільники, $\tau(n) = 6$, $\sigma(n) = 28$.

8.20. $n \vdots 63$ і $\tau(n) = 10$.

8.21. n ділиться лише на два різних простих числа, $\tau(n) = 9$, $\sigma(n) = 91$.

8.22. n має тільки три різних простих дільники, $\tau(n) = 8$, $\sigma(n) = 72$.

8.23. $n \vdots 56$ і $\tau(n) = 21$.

8.24. n – найменше натуральне число, для якого $\tau(n) = 18$.

8.25. n має тільки два різних простих дільники, $\tau(n) = 6$, $\sigma(n) = 124$.

Приклад 9.1. Знайти кількість натуральних чисел, які менші від числа $n = 624$ і мають з ним найбільший спільний дільник $d = 13$.

Розв'язання. Нехай $x \in \mathbb{N}$ таке, що $x < 624$ і $(x, 624) = 13$. За властивістю 5° п.2 це можливо тоді і лише тоді, коли $x = 13x_1$, $624 = 13 \cdot 48$, де $(x_1, 48) = 1$, $x_1 < 48$. Значить, чисел x існує стільки ж, скільки чисел x_1. Кількість чисел x_1 дорівнює

$$\varphi(48) = \varphi(2^4 \cdot 3) = \varphi(2^4)\varphi(3) = (2^4 - 2^3) \cdot 2 = (16 - 8) \cdot 2 = 16,$$

де $\varphi(n)$ – значення функції Ойлера для числа n.

Розв'язання в Maple. Нехай m – кількість чисел, які менші від числа

```
> n:=624;
```

$$n := 624$$

і мають з ним найбільший спільний дільник

```
> d:=13;
```

$$d := 13$$

Для кожного із чисел від 1 до $n-1$ перевіримо, чи має воно із числом n найбільший спільний дільник d. До початку перевірки надаємо m значення 0. Як тільки число, що має із n найбільший спільний дільник, що дорівнює d, знайдено, збільшуємо m на 1. В кінці перевірки виводимо значення m на екран:

```
> m:=0:
  for i from 1 to n-1 do
    if igcd(i,n)=d then m:=m+1; end if;
  end do;
  print(m);
```

Отже, $m = 16$.

У випадку виявленої помилки перевірте, чи правильно було виконано обчислення:

```
> phi(48);
```

16

Приклад 9.2. Знайти кількість натуральних чисел, які кратні числу $n = 624$ і містяться між 10^6 і 10^7.

Розв'язання. Припустимо, що серед чисел від 1 до 10^6 включно чисел, кратних 624, є k:

$$624, 2 \cdot 624, \ldots, k \cdot 624,$$

де $k \cdot 624$ – найбільше з них. Тоді має місце нерівність $k \cdot 624 \leqslant 10^6 < (k+1) \cdot 624$ або

$$k \leqslant \frac{10^6}{624} < k + 1.$$

Звідки

$$k = \left[\frac{10^6}{624}\right] = 1602,$$

тобто серед чисел від 1 до 10^6 включно є 1602 числа, кратних 624.

Нехай l – кількість чисел, кратних 624, серед чисел від 1 до 10^7 включно. Аналогічно неважко показати, що

$$l = \left[\frac{10^7}{624}\right] = 16025.$$

Оскільки $10^6 \vdots 624$, то чисел, кратних 624, в межах від 10^6 до 10^7 є $l - k = 16025 - 1602 = 14423$.

Розв'язання в Maple. В цьому випадку цикл for також дозволяє легко знайти потрібну кількість: для кожного із натуральних чисел від 10^6 до 10^7 перевіряємо, чи ділиться воно на n, якщо так, то збільшуємо лічильник m на 1.

```
> n:=624: m:=0:
  for i from 10^6 to 10^7 do
    if i mod n=0 then m:=m+1; end if;
  end do;
  print(m);
```

14423

У випадку виявленої помилки перевірте, чи правильно було виконано обчислення. (Нагадаємо, що для відшукання цілої частини дійсного числа n використовується команда floor(n), див. Приклад 1.)

```
> k:=floor(10^6/624);
```

1602

```
> l:=floor(10^7/624);
```

16025

```
> l-k;
```

14423

Приклад 9.3. Знайти кількість натуральних чисел, які менші від числа $n = 624$ і не діляться на жодне із чисел 5 і 7.

Розв'язання. Чисел, кратних 5, серед чисел від 1 до 623 включно буде $\left[\frac{623}{5}\right] = 124$, кратних 7 – $\left[\frac{623}{7}\right] = 89$. Серед цих 89 чисел є числа, кратні одночасно 5 і 7, тобто кратні 35 (їх $\left[\frac{623}{35}\right] = 17$). Отже, чисел, кратних хоча б одному із чисел 5 або 7 є всього

$$124 + (89 - 17) = 196.$$

А значить, чисел, які не діляться ні на 5, ні на 7, є

$$623 - 196 = 427.$$

Розв'язання в Maple. Аналогічно до попередніх Прикладів 9.1 і 9.2 використаємо цикл for:

```
> n:=624: m:=0:
  for i from 1 to n-1 do
    if (i mod 5<>0) and (i mod 7 <>0) then m:=m+1; end if;
  end do;
  print(m);
```

427

Перевірка проміжних обчислень виглядає наступним чином:

```
> with(numtheory):
> s1:=floor(623/5);
```

124

```
> s2:=floor(623/7);
```

89

```
> s3:=floor(623/35);
```

$$17$$

```
> s1+(s2-s3);
```

$$196$$

```
> (n-1)-%;
```

$$427$$

Завдання 9. Знайти кількість натуральних чисел, які:

а) менші від числа n і мають з ним найбільший спільний дільник d;
б) кратні числу n і містяться між 10^5 і 10^6;
в) менші від числа n і не діляться на жодне із чисел a і b.

9.1. $n = 945, \quad d = 15, \quad a = 3, \quad b = 7.$

9.2. $n = 882, \quad d = 18, \quad a = 5, \quad b = 7.$

9.3. $n = 966, \quad d = 21, \quad a = 11, \quad b = 3.$

9.4. $n = 1026, \quad d = 19, \quad a = 7, \quad b = 5.$

9.5. $n = 918, \quad d = 17, \quad a = 7, \quad b = 3.$

9.6. $n = 816, \quad d = 24, \quad a = 3, \quad b = 11.$

9.7. $n = 903, \quad d = 21, \quad a = 5, \quad b = 7.$

9.8. $n = 1003, \quad d = 17, \quad a = 7, \quad b = 3.$

9.9. $n = 828, \quad d = 18, \quad a = 5, \quad b = 11.$

9.10. $n = 767, \quad d = 13, \quad a = 5, \quad b = 7.$

9.11. $n = 996, \quad d = 12, \quad a = 7, \quad b = 3.$

9.12. $n = 819, \quad d = 21, \quad a = 13, \quad b = 3.$

9.13. $n = 1392, \quad d = 16, \quad a = 3, \quad b = 5.$

9.14. $n = 816, \quad d = 17, \quad a = 11, \quad b = 5.$

9.15. $n = 1080, \quad d = 15, \quad a = 3, \quad b = 7.$

9.16. $n = 874, \quad d = 19, \quad a = 5, \quad b = 11.$

9.17. $n = 876, \quad d = 13, \quad a = 11, \quad b = 3.$

9.18. $n = 1110, \quad d = 15, \quad a = 5, \quad b = 13.$

9.19. $n = 1296, \quad d = 18, \quad a = 11, \quad b = 5.$

9.20. $n = 817, \quad d = 19, \quad a = 3, \quad b = 7.$

9.21. $n = 1008, \quad d = 14, \quad a = 7, \quad b = 5.$

9.22. $n = 871, \quad d = 13, \quad a = 5, \quad b = 3.$

9.23. $n = 1056, \quad d = 22, \quad a = 7, \quad b = 11.$

9.24. $n = 833, \quad d = 17, \quad a = 3, \quad b = 5.$

9.25. $n = 1104, \quad d = 23, \quad a = 11, \quad b = 5.$

Приклад 10. Знайти:

а) канонічний розклад числа 48!;
б) скількома нулями закінчується число 48!.

Розв'язання. а) До канонічного розкладу числа 48! входять всі прості числа, що не перевищують 48, і лише вони. Для кожного із цих чисел знайдемо показник, з яким воно входить до канонічного розкладу числа 48!

За формулою (II.16) для числа $p_1 = 2$ маємо:

$$k_1 = \left[\frac{48}{2}\right] + \left[\frac{48}{2^2}\right] + \left[\frac{48}{2^3}\right] + \left[\frac{48}{2^4}\right] + \left[\frac{48}{2^5}\right] = 24 + 12 + 6 + 3 + 1 = 46.$$

Далі,

$$\begin{array}{ll} p_2 = 3 & k_2 = \left[\frac{48}{3}\right] + \left[\frac{48}{3^2}\right] + \left[\frac{48}{3^3}\right] = 16 + 5 + 1 = 22; \\ p_3 = 5 & k_3 = \left[\frac{48}{5}\right] + \left[\frac{48}{5^2}\right] = 9 + 1 = 10; \\ p_4 = 7 & k_4 = \left[\frac{48}{7}\right] = 6; \\ p_5 = 11 & k_5 = \left[\frac{48}{11}\right] = 4; \\ p_7 = 13 & k_7 = \left[\frac{48}{13}\right] = 3; \\ p_8 = 17 & k_8 = \left[\frac{48}{17}\right] = 2; \\ p_9 = 19 & k_9 = \left[\frac{48}{19}\right] = 2; \\ p_{10} = 23 & k_{10} = \left[\frac{48}{23}\right] = 2. \end{array}$$

Для числа $p_{11} = 29$ показник дорівнює 1, оскільки серед множників добутку 48! немає таких, що кратні 29, окрім самого числа 29. Аналогічно для

чисел 31, 37, 41, 43, 47. (Зауважимо, що показник, з яким входить число 11 до канонічного розкладу числа 48!, можна знайти і наступним чином: серед множників числа 48! на 11 діляться лише числа 11, 22, 33, 44; при цьому кожне з них не ділиться на 11^2. Отже, показник $k_5 = 4$.)

Таким чином, канонічний розклад числа 48! має вигляд:

$$48! = 2^{46} \cdot 3^{22} \cdot 5^{10} \cdot 7^6 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1 \cdot 47^1.$$

б) Нехай s – кількість нулів, якими закінчується число 48!. Тоді $48! \vdots 10^s$ і s – максимальне із невід'ємних цілих чисел із даною умовою. Але тоді $48! \vdots 2^s$ і $48! \vdots 5^s$, а значить, s – менше із чисел k_1 і k_3:

$$s = \min\{k_1, k_3\} = \min\{22, 10\} = 10.$$

Отже, число 48! закінчується 10-ма нулями.

Розв'язання в Maple. Для одержання канонічного розкладу використовуємо команду **ifactor**:

```
> ifactor(48!);
```

$(2)^{46}$ $(3)^{22}$ $(5)^{10}$ $(7)^6$ $(11)^4$ $(13)^3$ $(17)^2$ $(19)^2$ $(23)^2$ (29) (31) (37) (41) (43) (47)

Знайдемо число 48!

```
> 48!;
```

12413915592536072670862289047373375038521486354677760000000000

Це число закінчується 10-ма нулями.

Завдання 10. Знайти:

а) канонічний розклад числа $n!$;

б) кількість нулів, якими закінчується число $n!$, якщо:

10.1. $n = 28$.
10.2. $n = 34$.
10.3. $n = 44$.
10.4. $n = 41$.
10.5. $n = 52$.
10.6. $n = 61$.
10.7. $n = 37$.
10.8. $n = 63$.
10.9. $n = 54$.
10.10. $n = 32$.
10.11. $n = 51$.
10.12. $n = 29$.
10.13. $n = 50$.
10.14. $n = 56$.
10.15. $n = 33$.
10.16. $n = 53$.
10.17. $n = 46$.
10.18. $n = 62$.
10.19. $n = 30$.
10.20. $n = 55$.
10.21. $n = 47$.
10.22. $n = 31$.
10.23. $n = 52$.
10.24. $n = 42$.
10.25. $n = 49$.

5. Конгруенції. Класи лишків. Повна і зведена системи лишків за даним модулем

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай m – деяке натуральне число. Цілі числі a і b називаються конгруентними за модулем m, якщо $(a-b) \vdots m$. Пишуть

$$a \equiv b \,(\mathrm{mod} m) \text{ або } a \equiv b \,(m)\,. \tag{II.28}$$

Співвідношення (II.28) називають конгруенцією. Якщо числа a і b не є конгруентними за модулем m, то пишуть $a \not\equiv b \,(\mathrm{mod}\, m)$ або $a \not\equiv b \,(m)$.

Теорема. *Наступні твердження еквівалентні:*

1) цілі числа a і b конгруентні за модулем m: $a \equiv b \,(\mathrm{mod}\, m)$;
2) цілі числа a і b пов'язані співвідношенням: $a = b + mt$, де $t \in \mathbb{Z}$, $m \in \mathbb{N}$;
3) двом цілим числам a і b відповідає одна й та сама остача r при діленні їх на натуральне число m: $a = mq + r$, $b = mq_1 + r$, де $0 \leqslant r < m$.

Властивості конгруенцій:

1. Конгруенції за одним і тим же модулем можна почленно додавати, віднімати, перемножувати.
2. Доданок, що стоїть у якій-небудь частині конгруенції, можна переносити в іншу частину, змінивши знак на протилежний.
3. До обох частин конгруенції можна додати (або від обох частин конгруенції можна відняти) одне й те саме ціле число.
4. До будь-якої із частин конгруенції можна додати (або відняти) довільне ціле число, кратне модулю.
5. Обидві частини конгруенції можна помножити на одне й те саме ціле число.
6. Обидві частини конгруенції можна піднести до одного й того самого натурального степеня.
7. Обидві частини конгруенції можна поділити на їхній спільний дільник, взаємно простий з модулем.
8. Обидві частини конгруенції і модуль можна помножити на одне й те саме натуральне число.
9. Обидві частини конгруенції і модуль можна поділити на будь-який їхній спільний натуральний дільник.
10. Якщо конгруенція має місце за кількома модулями, то вона матиме місце і за модулем, що дорівнює їхньому найменшому спільному кратному.
11. Якщо конгруенція має місце за модулем m, то вона матиме місце і за будь-яким натуральним дільником d цього модуля.
12. Якщо $a \equiv b \,(\mathrm{mod}\, m)$, то $(a, m) = (b, m)$.

Відношення конгруентності „a і b конгруентні за модулем m", що задається формулою $a \equiv b \,(\mathrm{mod}\, m)$, є відношенням еквівалентності на множині $\mathbb{Z}$ цілих чисел. Нехай a – деяке ціле число. Множину

$$K_a^{(m)} = \{x \in \mathbb{Z} | x \equiv a \,(\mathrm{mod}\, m)\}$$

– всіх цілих чисел x, конгруентних числу a за модулем m називають класом лишків за модулем m, число a – представником даного класу, будь-який елемент x із $K_a^{(m)}$ – лишком.

Властивості класів лишків:

1°. Якщо $b \in K_a^{(m)}$, то $K_b^{(m)} = K_a^{(m)}$.
2°. $K_a^{(m)} = K_{a+mt}^{(m)}$, де $t \in \mathbb{Z}$.
3°. $K_a^{(m)} = K_r^{(m)}$, де r – остача від ділення a на m.
4°. Для даного $m \in \mathbb{N}$ існує рівно m класів лишків за модулем m: $K_0^{(m)}$, $K_1^{(m)}$,..., $K_{m-1}^{(m)}$.
5°. Два цілих числа a і b тоді і лише тоді належать до одного й того самого класу $K_r^{(m)}$, коли при діленні їх на m отримуємо одну й ту саму остачу r, тобто коли $a \equiv b \,(\mathrm{mod}\, m)$.
6°. Або $K_a^{(m)} = K_b^{(m)}$, або $K_a^{(m)} \cap K_b^{(m)} = \varnothing$ для будь-яких $K_a^{(m)}$ і $K_b^{(m)}$.
7°. Для будь-якого $m \in \mathbb{N}$, $K_0^{(m)} \cup K_1^{(m)} \cup ... \cup K_{m-1}^{(m)} = \mathbb{Z}$.
8°. Якщо $d > 1$, то $K_a^{(m)} = K_a^{(dm)} \cup K_{a+m}^{(dm)} \cup K_{a+2m}^{(dm)} \cup ... \cup K_{a+(d-1)m}^{(dm)}$.

Множина $\mathbb{Z}_m = \left\{K_0^{(m)}, K_1^{(m)}, \ldots, K_{m-1}^{(m)}\right\}$ всіх різних класів лишків за модулем m відносно операцій додавання і множення, заданих наступним чином:

$$K_a^{(m)} + K_b^{(m)} = K_{a+b}^{(m)},$$

$$K_a^{(m)} \cdot K_b^{(m)} = K_{a \cdot b}^{(m)};$$

є комутативним кільцем з одиницею. При цьому:

1) якщо число m – складене, то $\mathbb{Z}_m$ – кільце з дільниками нуля;
2) якщо число m – просте, то $\mathbb{Z}_m$ – поле;
3) якщо $m = 1$, то $\mathbb{Z}_m$ – нульове кільце.

До класу $K_a^{(m)}$ кільця $\mathbb{Z}_m$ існує обернений клас $\left(K_a^{(m)}\right)^{-1}$ тоді і лише тоді, коли $(a, m) = 1$.

Нехай a і b – елементи кільця K такі, що $a \neq 0$, $b \neq 0$, але $a \cdot b = 0$. Тоді a називають лівим дільником нуля, b – правим дільником нуля кільця, K називають кільцем з дільниками нуля. Якщо елемент a одночасно є і лівим, і правим дільником нуля кільця K, то його просто називають дільником нуля кільця K.

Повною системою лишків за модулем m (ПСЛ(m)) називається сукупність лишків $x_0, x_1, \ldots, x_{m-1}$, взятих по одному із кожного класу $K_0^{(m)}$, $K_1^{(m)}$, ..., $K_{m-1}^{(m)}$. Найчастіше використовують:

- повну систему найменших невід'ємних лишків: $0, 1, ..., m-1$.
- повну систему найменших додатних лишків: $1, 2, ..., m$.
- повну систему абсолютно найменших лишків (із кожного класу беруть найменший за абсолютною величиною лишок).

Властивості повної системи лишків:

1. Будь-яка сукупність m цілих чисел: $x_1, x_2, \ldots, x_m$, попарно не конгруентних за модулем m, утворює повну систему лишків за модулем m.

2. Нехай $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, причому $(a, m) = 1$. Тоді якщо числа $x_1, x_2, \ldots, x_m$ утворюють повну систему лишків за модулем m, то і числа $ax_1 + b, ax_2 + b, \ldots, ax_m + b$ утворюють повну систему лишків за модулем m.

Клас лишків $K_a^{(m)}$ називається взаємно простим із модулем m, якщо $(a, m) = 1$.

Зведеною системою лишків за модулем m називається сукупність $\varphi(m)$ лишків, взятих по одному із кожного класу, взаємно простого із модулем m.

Властивості зведеної системи лишків:

1. Будь-яка сукупність $\varphi(m)$ цілих чисел $x_1, x_2, \ldots, x_{\varphi(m)}$, попарно не конгруентних між собою за модулем m і взаємно простих із m, утворює зведену систему лишків за модулем m.

2. Нехай $a \in \mathbb{Z}$, $m \in \mathbb{N}$, причому $(a, m) = 1$. Тоді якщо числа $x_1, x_2, \ldots, x_{\varphi(m)}$ утворюють зведену систему лишків за модулем m, то і числа $ax_1, ax_2, \ldots, ax_{\varphi(m)}$ утворюють зведену систему лишків за модулем m.

Множина $\mathbb{Z}_m^*$ класів лишків за модулем m, взаємно простих із m, утворює мультиплікативну групу. Її називають мультиплікативною групою кільця $\mathbb{Z}_m$ класів лишків за модулем m.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 11.1. Визначити, чи утворюють повну систему лишків за модулем $m = 7$ числа

а) -62, 108, -36, 21, 501, 96, 149;
б) -62, 108, -36, 21, 501, 96;
в) -62, 8, -36, 21, 501, 96, 149?

Розв'язання. Щоб визначити, чи є деяка система чисел $a_1, a_2, \ldots, a_s$ повною системою лишків за модулем m, треба:

1) перевірити, чи чисел є m (тобто чи $s = m$);
2) перевірити, чи всі вони між собою попарно неконгруентні за модулем m: для цього замінимо кожне із чисел сукупності на конгруентний йому найменший невід'ємний лишок із того ж самого класу лишків за модулем m, що й дане число (це неважко зробити, знайшовши остачу від ділення заданого числа на модуль m). Відповідно до властивості 5°, числа заданої системи є попарно неконгруентні за модулем тоді і лише тоді, коли всі отримані остачі різні.

а) В розглядуваному прикладі маємо:

1) чисел у системі є 7;

2) $$\begin{aligned} -62 &\equiv 1 \,(\mathrm{mod}\, 7)\,, & 501 &\equiv 4 \,(\mathrm{mod}\, 7)\,,\\ 108 &\equiv 3 \,(\mathrm{mod}\, 7)\,, & 96 &\equiv 5 \,(\mathrm{mod}\, 7)\,,\\ -36 &\equiv 6 \,(\mathrm{mod}\, 7)\,, & 149 &\equiv 2 \,(\mathrm{mod}\, 7)\,,\\ 21 &\equiv 0 \,(\mathrm{mod}\, 7)\,, \end{aligned}$$

Дістали нову сукупність чисел: $1, 3, 6, 0, 4, 5, 2$. Оскільки всі числа різні, то задана сукупність чисел утворює повну систему лишків за модулем $m = 7$.

б) В заданій сукупності чисел не 7, а 6, а отже, задана сукупність чисел не утворює ПСЛ(7).

в) В даній сукупності чисел є 7, але серед чисел є попарно конгруентні за модулем 7 (дійсно, $-62 \equiv 1 \,(\mathrm{mod}\, 7)$ і $8 \equiv 1 \,(\mathrm{mod}\, 7)$, значить, $-62 \equiv 8 \,(\mathrm{mod}\, 7)$), а отже, задана сукупність чисел не утворює ПСЛ(7).

Розробка процедур. Спеціальної команди для перевірки, чи утворює сукупність чисел повну систему лишків в Maple не передбачено. Створимо процедуру **psl(A,m)**, яка визначатиме, чи утворюють числа множини A ПСЛ(m).

В даній процедурі спочатку перевіряється, чи чисел є m ($\#\mathbf{1}$). Якщо так, то s набуває значення 0; в іншому випадку з'являється повідомлення false. Далі перевіряється конгруентність введених чисел за модулем m ($\#\mathbf{2}$). Якщо якась пара чисел конгруентна за модулем m, то число s збільшується на 1 (Умова $A[i] \equiv A[j] \pmod{m}$ замінена на еквівалентну $A[i]-A[j] \equiv 0 \pmod{m}$). В результаті, якщо s залишається рівним 0, то задані числа утворюють ПСЛ(m) (true), якщо $s \neq 0$, то задані числа ПСЛ(m) не утворюють (false).

```
psl:=proc(A::set,m::integer)
local n,s,i,j;
uses numtheory;
   n:=nops(A);
   if n=m then s:=0; #1
      for i from 1 to n-1 do #2
         for j from i+1 to n do
            if A[i]-A[j] mod m =0 then s:=s+1; end if;
         end do;
      end do;
      if s=0 then return true; else return false end if;
   else return false;
   end if;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

задаємо множину чисел A:

```
> A:={-62,108,-36,21,501,96,149}:
```

і застосовуємо команду **psl**:

```
> psl(A,7);
```

true

```
> A:={-62,108,-36,21,501,96}:
> psl(A,7);
```

false

```
> A:={-62,8,-36,21,501,96,149}:
> psl(A,7);
```

false

Приклад 11.2. Визначити, чи утворюють зведену систему лишків за модулем m числа

а) $-4,\ 2,\ 8,\ 4,$ $m = 5;$
б) $13,\ 919,\ 26,\ 38,\ 167,\ -66,$ $m = 9?$

Розв'язання. Щоб визначити, чи є деяка система чисел зведеною системою лишків за модулем m, треба:

1) перевірити, чи чисел є $\varphi(m)$;
2) перевірити, чи всі вони між собою попарно не конгруентні за модулем m;
3) перевірити, чи всі вони взаємно прості із m.

При цьому доцільно замінити кожне із чисел сукупності конгруентним йому найменшим невід'ємним лишком із того ж самого класу лишків за модулем m, що й дане число.

а) В даному випадку маємо:

1) чисел у системі є $\varphi(5) = 4$.

2) Замінимо кожне із чисел заданої сукупності на конгруентний йому найменший невід'ємний лишок за модулем 5:

$$-4 \equiv 1 \,(\mathrm{mod}\, 9)\,,$$
$$8 \equiv 3 \,(\mathrm{mod}\, 9)\,.$$

Отримали нову сукупність чисел 1, 2, 3, 4. Всі числа даної сукупності попарно не конгруентні за модулем 5 (оскільки всі вони різні).

3) Число взаємно просте із модулем m тоді і лише тоді, коли взаємно простим із m є найменший невід'ємний лишок за модулем m. Оскільки всі числа сукупності 1, 2, 3, 4 взаємно прості із m, то і всі числа заданої сукупності також взаємно прості із m.

Таким чином, сукупність чисел -4, 2, 8, 4 утворює ЗСЛ(5).

б) В розглядуваному прикладі маємо:

1) чисел у системі є $\varphi(9) = \varphi(3^2) = 9(1 - \frac{1}{3}) = 6$.

2)
$$\begin{aligned} 13 &\equiv 4 \,(\mathrm{mod}\, 9)\,, & 38 &\equiv 2 \,(\mathrm{mod}\, 9)\,, \\ 919 &\equiv 1 \,(\mathrm{mod}\, 9)\,, & 167 &\equiv 5 \,(\mathrm{mod}\, 9)\,, \\ 26 &\equiv 8 \,(\mathrm{mod}\, 9)\,, & -66 &\equiv 6 \,(\mathrm{mod}\, 9)\,. \end{aligned}$$

Дістали нову сукупність чисел: $4, 1, 8, 2, 5, 6$. Всі числа цієї сукупності попарно не конгруентні, оскільки всі вони різні. Проте число 6 не взаємно просте із модулем $m = 9$, тому отримана сукупність зведеної системи лишків не утворює. А це означає, що і задана сукупність чисел зведеної системи лишків не утворює.

Розробка процедур. Створюємо процедуру zsl, аналогічну до процедури psl. В ході процедури відбувається перевірка:

#1: Чи є в системі чисел $\varphi(m)$;

#2: чи є числа $A[i]$ із множини A взаємнопрості із модулем m;

#2: чи є числа $A[i]$ і $A[j]$ із множини A попарно не конгруентні за модулем m (для всіх $i \in \overline{1, n-1}$, $j \in \overline{i+1, n}$);

```
zsl:=proc(A::set,m::integer)
local n,i,s,j;
uses numtheory;
   n:=nops(A):
   if n=phi(m) then #1
      for i from 1 to n do
         if igcd(A[i],m)=1 then s:=0; #2
            for i from 1 to n-1 do #3
               for j from i+1 to n do
                  if A[i]-A[j] mod m =0 then s:=s+1; end if;
               end do;
            end do;
         end if;
      end do;
      if s=0 then return true; else return false end if;
   else return false;
   end if;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

задаємо множину чисел A і застосовуємо команду **zsl**:

```
> A:={-4,2,8,4};
  zsl(A,5);
```

$$A := \{-4,\ 2,\ 4,\ 8\}$$

$$true$$

Аналогічно для б):

```
> A:={13,919,-26,38,167,-66};
  zsl(A,9);
```

$$A := \{-66,\ -26,\ 13,\ 38,\ 167,\ 919\}$$

$$false$$

Завдання 11. Визначити, чи утворюють: а) повну; б) зведену систему лишків за модулем m числа:

11.1. а) $597, -197, 250, -319, 151, 56, -59, 202$, якщо $m = 8$;
б) $-32, -13, 38, 29, 37, 49, 11, 61$, якщо $m = 15$.

11.2. а) $930, 101, -18, 28, -109, 40, -22, -2, 15$, якщо $m = 9$;
б) $41, 47, 37, -41$, якщо $m = 12$.

11.3. а) $45, 515, 5, -104, 106, 63, 481, -177$, якщо $m = 7$;
б) $-23, -505, -29, 417$, якщо $m = 12$.

11.4. а) $3, 124, 128, -19, 37, 28, -109, 40, -22, -2, 15$, якщо $m = 11$;
б) $137, -205, 280, 77$, якщо $m = 8$.

11.5. а) $7, 16, 10, -11, -55, -29, 35, 27, 36, 14, 19, 23$, якщо $m = 12$;
б) $27, 77, 119, -2, 16, -109$, якщо $m = 9$.

11.6. а) $930, 111, -27, 37, -100, 40, -22, -2, 15$, якщо $m = 9$;
б) $43, 69, 49, -139$, якщо $m = 12$.

11.7. а) $776, 731, -75, 172, 392, 158, 144, -62$, якщо $m = 8$;
б) $216, -15, -712, 14, 23$, якщо $m = 10$.

11.8. а) $568, -125, 349, 161, 184, 109, 431$, якщо $m = 7$;
б) $155, -131, 39, -71$, якщо $m = 8$.

11.9. а) $19, 40, -94, 2, -414, 119, -24, 116, 60$, якщо $m = 9$;
б) $71, -5, 99, 69$, якщо $m = 10$.

11.10. а) $-55, 82, 390, -104, 15, -765, 416, 651, 428$, якщо $m = 9$;
б) $119, -31, 11, -5$, якщо $m = 12$.

11.11. а) $56, 466, 62, 31, -462, 13, -86, 115, -32, 147, -288$, якщо $m = 11$;
б) $-232, 41, 2, -41, 5$, якщо $m = 12$.

11.12. а) $-181, -259, 17, -16, 533, 282, -3, 42$, якщо $m = 8$;
б) $2311, -51, 237, 523, -411$, якщо $m = 10$.

11.13. а) $379, -95, 238, 289, -448, 40, 25$, якщо $m = 7$;
б) $-122, 58, -504, 522, 17, 3, -5$, якщо $m = 9$.

11.14. а) $126, 21, -191, -274, 205, 460, 206, 69, 364$, якщо $m = 9$;
б) $48, 397, -21, -487$, якщо $m = 8$.

11.15. а) $138, 57, -173, 21, 1, -180, 80, -30$, якщо $m = 8$;
б) $-71, 231, 53, -709$, якщо $m = 12$.

11.16. а) $30, 4, -88, 195, 12, -36, 360, 83, -135$, якщо $m = 9$;
б) $7, -85, 65, -5$, якщо $m = 12$.

11.17. а) $-71, 213, 15, 299, -504, 49, 102$, якщо $m = 7$;
б) $-189, 37, 113, 661$, якщо $m = 8$.

11.18. а) $23, -741, 50, 5, -572, 210, 8$, якщо $m = 7$;
б) $21, -14, 573, -101, -12, 14$, якщо $m = 9$.

11.19. а) $234, -471, 21, -36, 544, -3, 11, 24, 1, 23, -15, -44, 6$, якщо $m = 12$;
б) $369, -31, 45, 127$, якщо $m = 8$.

11.20. а) $596, -431, 338, 1000, -70, 134, -681$, якщо $m = 7$;
б) $11, -65, -151, 3$, якщо $m = 12$.

11.21. а) $345, 21, -127, -46, 105, 13, 307, -20, 103$, якщо $m = 9$;
б) $234, -15, 233, -27, 17$, якщо $m = 10$.

11.22. а) $-6, 109, -334, 85, 29, 234, 311, 78, -86$, якщо $m = 9$;
б) $139, -59, 3, 17, -161$, якщо $m = 12$.

11.23. а) $17, 296, -514, -55, 82, 645, 233, 61$, якщо $m = 8$;

б) $261, -302, 49, -21, 54, -31$, якщо $m = 9$.

11.24. а) $-21, 121, 587, 75, 77, 106, -24, -75, 60, 70, 266$, якщо $m = 11$;

б) $113, 79, -5, -363$, якщо $m = 8$.

11.25. а) $350, -480, 12, 90, 88, 361, 342$, якщо $m = 7$;

б) $-133, -301, 255, -433$, якщо $m = 12$.

Приклад 12. У кільці класів лишків за модулем 20 знайти:

а) усі дільники одиниці;

б) усі дільники нуля;

в) клас, протилежний до класу $K_6^{(20)}$;

г) клас, обернений до класу $K_7^{(20)}$.

Розв'язання. а) Дільником одиниці в кільці класів лишків за модулем $m = 20$ є кожен клас $K_a^{(20)}$ такий, що $(a, 20) = 1$. Тому дільниками одиниці є класи: $K_1^{(20)}$, $K_3^{(20)}$, $K_7^{(20)}$, $K_9^{(20)}$, $K_{11}^{(20)}$, $K_{13}^{(20)}$, $K_{17}^{(20)}$, $K_{19}^{(20)}$.

б) Дільником нуля в кільці класів лишків за модулем $m = 20$ є кожен ненульовий клас $K_a^{(20)}$, для якого знайдеться такий клас $K_x^{(20)} \neq K_0^{(20)}$, що $K_a^{(20)} K_x^{(20)} = K_0^{(20)}$, тобто такий клас $K_x^{(20)}$, що $ax \vdots 20$, де $1 \leqslant a, x \leqslant 19$. Тому, фактично, дільниками нуля є всі такі класи $K_a^{(20)}$, що $(a, 20) \neq 1$. Отже, дільниками нуля є класи: $K_2^{(20)}$, $K_4^{(20)}$, $K_5^{(20)}$, $K_6^{(20)}$, $K_8^{(20)}$, $K_{10}^{(20)}$, $K_{12}^{(20)}$, $K_{14}^{(20)}$, $K_{15}^{(20)}$, $K_{16}^{(20)}$, $K_{18}^{(20)}$.

Зауваження. Узагальнюючи міркування п.б), неважко показати, що для довільного $m \in \mathbb{N}$ дільниками нуля в кільці $\mathbb{Z}_m$ класів лишків за модулем m є всі елементи, відмінні від дільників одиниці і самого нуля.

в) Знайдемо такий клас $K_x^{(20)}$, що $K_6^{(20)} + K_x^{(20)} = K_0^{(20)}$. Оскільки $K_6^{(20)} + K_x^{(20)} = K_{6+x}^{(20)}$, то потрібно знайти таке ціле число x, $0 \leqslant x < 20$, що $(6 + x) \vdots 20$. Легко бачити, що одним із таких чисел є $x = 14$. Отже, $-K_6^{(20)} = K_{14}^{(20)}$.

г) *Спосіб I.* Оскільки $(a, m) = (7, 20) = 1$, то клас лишків, обернений до класу $K_7^{(20)}$, існує. Знайдемо цілі числа u і v такі, що $7u + 20v = 1$. Скористаємось для цього алгоритмом Евкліда.

$$\begin{array}{rr|l} a = & 20 & 7 \\ \cline{3-3} & 14 & 2 \\ \cline{2-3} b = & 7 & 6 = r_1 \\ \cline{2-3} & 6 & 1 \\ \cline{2-3} r_1 = 6 & 1 & = r_2 \\ \cline{2-3} & 6 & 6 \\ \cline{2-3} & 0 & \end{array}$$

Запишемо отримані рівності:

$$a = 2b + r_1,$$
$$b = r_1 + 1.$$

Маємо: $r_1 = a - 2b$,

$1 = b - r_1 = b - (a - 2b) = 3b - a = 3 \cdot 7 - 20 \cdot 1 = 7 \cdot 3 + 20 \cdot (-1)$.

Звідси випливає, що $7 \cdot 3 \equiv 1 \pmod{20}$, тоді $K_{7\cdot 3}^{(20)} = K_1^{(20)}$, значить, $K_7^{(20)} \cdot K_3^{(20)} = K_1^{(20)}$. Отже, оберненим до класу $K_7^{(20)}$ є клас $K_3^{(20)}$, тобто $(K_7^{(20)})^{-1} = K_3^{(20)}$.

Спосіб II. Клас $K_u^{(m)}$, обернений до класу $K_a^{(m)}$, можна іноді легко знайти усно, підбираючи таке ціле число u, щоб добуток au при діленні на m давав остачу 1. Так, для класу $K_7^{(20)}$ класи $K_5^{(20)}$, $K_7^{(20)}$, $K_9^{(20)}$, $K_{11}^{(20)}$, $K_{13}^{(20)}$, $K_{17}^{(20)}$, $K_{19}^{(20)}$ оберненими не можуть бути, оскільки числа $7 \cdot 5 = 35$, $7 \cdot 7 = 49$, $7 \cdot 9 = 63$, $7 \cdot 11 = 66$, $7 \cdot 13 = 91$, $7 \cdot 17 = 119$, $7 \cdot 19 = 133$ при діленні на 20 дають остачу $15, 9, 3, 17, 11$ відповідно (а не 1). Зрозуміло також, що дільники нуля випробовувати теж не потрібно (оскільки вони не можуть бути дільниками одиниці). Натомість остача при діленні на $m = 20$ числа $7 \cdot 3 = 21$ дорівнює 1, тому $(K_7^{(20)})^{-1} = K_3^{(20)}$.

Спосіб III. Нехай $K_y^{(20)} \cdot K_7^{(20)} = K_1^{(20)}$, звідки $K_{7y}^{(20)} = K_1^{(20)}$. Тоді $7y \equiv 1 \pmod{20}$. Помічаємо, що $y = 3$ задовольняє дану конгруенцію. Отже, $(K_7^{(20)})^{-1} = K_3^{(20)}$.

Розробка процедур. Для створення процедур **diln1Z** і **diln0Z**, за допомогою яких здійснюватиметься пошук дільників одиниці і дільників нуля в кільці $\mathbb{Z}_m$ класів лишків за модулем m, використаємо той факт, що дільником одиниці в кільці $\mathbb{Z}_m$ є кожен клас $K_a^{(m)}$ такий, що $(a, m) = 1$, а дільником нуля – кожен такий клас $K_a^{(m)}$, $a \neq 0$, що $(a, m) \neq 1$. В процесі виконання даних процедур для всіх чисел i від 0 до $m - 1$ (від 1 до $m - 1$ відповідно) знаходимо найбільший спільний дільник чисел i та m, перевіряємо, чи виконується умова $(i, m) = 1$ ($(i, m) \neq 1$ відповідно), якщо умова виконується, число виводиться на екран.

Процедура **diln1Z**:

```
diln1Z:=proc(m::integer)
local i;
uses numtheory;
   for i from 0 to m-1 do
      if igcd(i,m)=1 then print(i); end if;
   end do;
end proc:
```

Процедура **diln0Z**:

```
diln0Z:=proc(m::integer)
local i;
uses numtheory;
   for i from 0 to m-1 do
      if igcd(i,m)<>1 then print(i); end if;
   end do;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

а) Дільники одиниці кільця $\mathbb{Z}_{20}$ знаходимо, застосовуючи команду **diln1Z**:

```
> diln1Z(20);
```

$$1$$
$$3$$
$$7$$
$$9$$
$$11$$
$$13$$
$$17$$
$$19$$

Отже, дільниками одиниці в $\mathbb{Z}_{20}$ є класи: $K_1^{(20)}$, $K_3^{(20)}$, $K_7^{(20)}$, $K_9^{(20)}$, $K_{11}^{(20)}$, $K_{13}^{(20)}$, $K_{17}^{(20)}$, $K_{19}^{(20)}$.

б) Дільники нуля кільця $\mathbb{Z}_{20}$ знаходимо за допомогою команди **diln0Z**:

```
> diln0Z(20);
```

$$2$$
$$4$$
$$5$$
$$6$$

8
10
12
14
15
16
18

Отже, дільниками нуля в $\mathbb{Z}_{20}$ є класи: $K_2^{(20)}$, $K_4^{(20)}$, $K_5^{(20)}$, $K_6^{(20)}$, $K_8^{(20)}$, $K_{10}^{(20)}$, $K_{12}^{(20)}$, $K_{14}^{(20)}$, $K_{15}^{(20)}$, $K_{16}^{(20)}$, $K_{18}^{(20)}$.

в) Клас, протилежний до класу $K_a^{(m)}$, легко знайти наступним чином: **-a mod m**. Маємо:

```
> -6 mod 20;
```

14

Отже, протилежним до класу $K_6^{(20)}$ є клас $K_{14}^{(20)}$.

г) Аналогічно, як і в пункті в), клас, обернений до класу $K_a^{(m)}$, можна легко знайти, вводячи: **a^ (-1) mod m**. Маємо:

```
> 7^(-1) mod 20;
```

3

Отже, оберненим до класу $K_7^{(20)}$ є клас $K_3^{(20)}$.

Зауваження 1. У випадку, коли до класу $K_a^{(m)}$ оберненого не існує (тобто коли цей клас не є дільником одиниці в $\mathbb{Z}_m$) з'являється відповідне повідомлення:

```
> 2^(-1) mod 20;

Error, the modular inverse does not exist
```

(Помилка, обернене за модулем число не існує)

Завдання 12. Знайти в кільці класів лишків:

а) за модулем m_1 усі дільники одиниці;

б) за модулем m_2 усі дільники нуля;

в) за модулем m_3 клас, протилежний до класу $K_b^{(m)}$;

г) за модулем m_3 клас, обернений до класу $K_a^{(m)}$.

12.1. $m_1 = 32$; $m_2 = 15$; $m_3 = 180$; $b = 126$; $a = 133$.

12.2. $m_1 = 18$; $m_2 = 22$; $m_3 = 324$; $b = 211$; $a = 127$.

12.3. $m_1 = 28$; $m_2 = 24$; $m_3 = 448$; $b = 301$; $a = 149$.

12.4. $m_1 = 42$; $m_2 = 30$; $m_3 = 256$; $b = 248$; $a = 103$.

12.5. $m_1 = 24$; $m_2 = 21$; $m_3 = 156$; $b = 53$; $a = 29$.

12.6. $m_1 = 27$; $m_2 = 29$; $m_3 = 625$; $b = 202$; $a = 611$.

12.7. $m_1 = 40$; $m_2 = 12$; $m_3 = 96$; $b = 44$; $a = 23$.

12.8. $m_1 = 16$; $m_2 = 15$; $m_3 = 144$; $b = 75$; $a = 81$.

12.9. $m_1 = 12$; $m_2 = 14$; $m_3 = 500$; $b = 61$; $a = 33$.

12.10. $m_1 = 27$; $m_2 = 35$; $m_3 = 150$; $b = 83$; $a = 119$.

12.11. $m_1 = 26$; $m_2 = 21$; $m_3 = 324$; $b = 105$; $a = 55$.

12.12. $m_1 = 24$; $m_2 = 25$; $m_3 = 84$; $b = 62$; $a = 61$.

12.13. $m_1 = 14$; $m_2 = 18$; $m_3 = 168$; $b = 54$; $a = 97$.

12.14. $m_1 = 32$; $m_2 = 10$; $m_3 = 225$; $b = 41$; $a = 77$.

12.15. $m_1 = 16$; $m_2 = 26$; $m_3 = 384$; $b = 111$; $a = 151$.

12.16. $m_1 = 21$; $m_2 = 12$; $m_3 = 420$; $b = 203$; $a = 143$.

12.17. $m_1 = 24$; $m_2 = 15$; $m_3 = 240$; $b = 13$; $a = 91$.

12.18. $m_1 = 28$; $m_2 = 38$; $m_3 = 185$; $b = 97$; $a = 131$.

12.19. $m_1 = 22$; $m_2 = 14$; $m_3 = 112$; $b = 44$; $a = 103$.

12.20. $m_1 = 8$; $m_2 = 49$; $m_3 = 546$; $b = 213$; $a = 263$.

12.21. $m_1 = 16$; $m_2 = 22$; $m_3 = 620$; $b = 124$; $a = 587$.

12.22. $m_1 = 32$; $m_2 = 21$; $m_3 = 460$; $b = 222$; $a = 77$.

12.23. $m_1 = 12$; $m_2 = 25$; $m_3 = 524$; $b = 494$; $a = 311$.

12.24. $m_1 = 22$; $m_2 = 16$; $m_3 = 480$; $b = 317$; $a = 91$.

12.25. $m_1 = 18$; $m_2 = 35$; $m_3 = 256$; $b = 141$; $a = 167$.

6. Теореми Ойлера і Ферма

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай a – довільне ціле число.

Теорема (Ойлера)**.** *Якщо* $m > 1$*, причому* $(a, m) = 1$*, то* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Теорема (Ферма)**.** *Для будь-якого простого* p *такого, що* $(a, p) = 1$*,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Наслідок. *Якщо* p *– просте число, то* $a^p \equiv a \pmod{p}$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 13.1. Знайти остачу від ділення:

а) 232^{2009} на 63; б) 462^{2012} на 360.

Розв'язання. За означенням, ціле число r є остачею від ділення числа a^s на число $m > 0$, якщо виконуються умови: $a^s = mq + r$ і $0 \leqslant r < m$ для деякого $q \in \mathbb{Z}$. В силу теореми п.5, дані умови еквівалентні наступним:

$$a^s \equiv r \,(\mathrm{mod}\, m) \quad \text{і} \quad 0 \leqslant r < m.$$

а) Необхідно знайти число r таке, що $232^{2009} \equiv r \,(\mathrm{mod}\, 63)$, де $0 \leqslant r < 63$. Оскільки $232 \equiv 43 \,(\mathrm{mod}\, 63)$, то, в силу властивості 6 конгруенцій (див. п.5) $232^{2009} \equiv 43^{2009} \,(\mathrm{mod}\, 63)$, звідки $r \equiv 43^{2009} \,(\mathrm{mod}\, 63)$.

Оскільки $(43, 63) = 1$, то, за теоремою Ойлера, $43^{\varphi(63)} \equiv 1 \,(\mathrm{mod}\, 63)$. Враховуючи, що $\varphi(63) = \varphi(3^2 \cdot 7) = \varphi(3^2) \cdot \varphi(7) = (3^2 - 3)(7 - 1) = 36$, маємо: $43^{36} \equiv 1 \,(\mathrm{mod}\, 63)$.

Поділимо число 2009 на число $\varphi(63) = 36$ з остачею: $2009 = 36 \cdot 55 + 29$. Тоді

$$r \equiv 43^{2009} \,(\mathrm{mod}\, 63) \equiv 43^{36 \cdot 55 + 29} \,(\mathrm{mod}\, 63) \equiv (43^{36})^{55} \cdot 43^{29} \,(\mathrm{mod}\, 63) \equiv \\ \equiv 1 \cdot 43^{29} \,(\mathrm{mod}\, 63)\,.$$

Враховуючи, що $43 \equiv -20 \,(\mathrm{mod}\, 63)$, далі матимемо:

$$r \equiv (-20)^{29} \,(\mathrm{mod}\, 63) \equiv -20^{29} \,(\mathrm{mod}\, 63) \equiv -\left(20^3\right)^9 \cdot 20^2 \,(\mathrm{mod}\, 63) \equiv \\ \equiv -(-1) \cdot 20^2 \,(\mathrm{mod}\, 63) \equiv 22 \,(\mathrm{mod} 63)$$

(оскільки $20^3 \equiv -1 \,(\mathrm{mod}\, 63)$).

Отже, остача від ділення числа 232^{2009} на число 63 дорівнює 22.

б) Дана задача еквівалентна наступній: знайти число r таке, що

$$462^{2012} \equiv r \,(\mathrm{mod}\, 360) \quad \text{і} \quad 0 \leqslant r < 360.$$

З огляду на те, що $462 \equiv 102 \,(\mathrm{mod}\, 360)$, за властивістю 6 конгруенцій (п.5), маємо: $462^{2012} \equiv 102^{2012} \,(\mathrm{mod}\, 360)$, значить,

$$r \equiv 102^{2012} \,(\mathrm{mod}\, 360)\,. \tag{II.29}$$

Оскільки $(102, 360) \neq 1$, то застосувати теорему Ойлера не можна. Знайдемо найбільший спільний дільник чисел 102^{2012} і 360. Оскільки

$$102^{2012} = (2 \cdot 3 \cdot 17)^{2012} = 2^{2012} \cdot 3^{2012} \cdot 17^{2012}, \qquad 360 = 2^3 \cdot 3^2 \cdot 5;$$

то $(102^{2012}, 360) = 2^3 \cdot 3^2$. За властивістю 12 конгруенцій (п.5), із конгруенції (II.29) випливає, що $(r, 360) = (102^{2012}, 360) = 2^3 \cdot 3^2 = 72$, а значить, $r = 72 \cdot r_1$, де $r_1 \in \mathbb{Z}$. Відмітимо також: із умови $0 \leqslant r < 360$ випливає, що

$$0 \leqslant r_1 < 5. \tag{II.30}$$

Отримуємо:

$$72r_1 \equiv 102^{2012} \pmod{360}$$

або

$$2^3 \cdot 3^2 \cdot r_1 \equiv 2^{2012} \cdot 3^{2012} \cdot 17^{2012} \left(\mathrm{mod}\, 2^3 \cdot 3^2 \cdot 5\right).$$

Із урахуванням властивості 9 конгруенцій (п.5), поділимо обидві частини і модуль даної конгруенції на число $2^3 \cdot 3^2$. Маємо:

$$r_1 \equiv 2^{2009} \cdot 3^{2010} \cdot 17^{2012} \pmod{5}.$$

Оскільки $3 \equiv -2 \pmod{5}$, $17 \equiv 2 \pmod{5}$, то

$$r_1 \equiv 2^{2009} \cdot (-2)^{2010} \cdot 2^{2012} \pmod{5} \equiv 2^{6031} \pmod{5}.$$

Враховуючи, що $(2, 5) = 1$, за теоремою Ферма, отримуємо: $2^4 \equiv 1 \pmod{5}$. Тоді

$$r_1 \equiv 2^{6031} \pmod{5} \equiv 2^{4 \cdot 1507 + 3} \pmod{5} \equiv \left(2^4\right)^{1507} \cdot 2^3 \pmod{5} \equiv$$
$$\equiv 1 \cdot 2^3 \pmod{5} \equiv 3 \pmod{5}.$$

Число 3 задовольняє умову (II.30), отже, $r_1 = 3$. Тоді $r = 72 \cdot r_1 = 72 \cdot 3 = 216$.

Отже, остача від ділення числа 462^{2012} на число 360 дорівнює 216.

Розв'язання в Maple. Остачу від ділення числа a на число b знаходимо, використовуючи оператор **mod**. Відмітимо, що при обчисленні остач від ділення числа a^s на m, коли s – досить велике число, доцільніше вводити вираз у вигляді **a&^ s mod m**. Якщо вираз ввести у форматі **a^ s mod m**, то спочатку програма обчислює значення степеня, а лише потім знаходить остачу. Для високих степенів це призводить до значних затрат часу.

```
> 232&^2009 mod 63;
```

22

```
> 462&^2012 mod 360;
```

216

Приклад 13.2. Знайти останню цифру числа 1327^{546}.

Розв'язання. Остання цифра натурального числа a дорівнює остачі від ділення a на 10. Тому необхідно знайти таке ціле число r, що

$$1327^{546} \equiv r \,(\mathrm{mod}\, 10) \quad \text{і} \quad 0 \leqslant r < 10.$$

З огляду на те, що $1327 \equiv 7 \,(\mathrm{mod}\, 10)$, маємо: $1327^{546} \equiv 7^{546} \,(\mathrm{mod}\, 10)$, звідки $r \equiv 7^{546} \,(\mathrm{mod}\, 10)$.

Оскільки $(7, 10) = 1$, можемо застосувати теорему Ойлера: $7^{\varphi(10)} \equiv 1 \,(\mathrm{mod}\, 10)$, тобто $7^4 \equiv 1 \,(\mathrm{mod}\, 10)$. Тоді

$$r \equiv 7^{546} \,(\mathrm{mod}\, 10) \equiv 7^{4\cdot 136+2} \,(\mathrm{mod}\, 10) \equiv \left(7^4\right)^{136} \cdot 7^2 \,(\mathrm{mod}\, 10) \equiv$$
$$\equiv 7^2 \,(\mathrm{mod}\, 10) \equiv 49 \,(\mathrm{mod}\, 10) \equiv 9 \,(\mathrm{mod}\, 10)\,.$$

Таким чином, остання цифра 1327^{546} числа дорівнює 9.

Розв'язання в Maple. Знаходимо остачу від ділення заданого числа на 10:

```
> 1327&^546 mod 10;
```

$$9$$

Приклад 13.3. Знайти останні дві цифри числа 1956^{659}.

Розв'язання. Необхідно знайти таке ціле число r, що $1956^{659} = 100 \cdot q + r$ і $0 \leqslant r < 100$, де $q \in \mathbb{Z}$. Це означає, що число r повинно задовольняти умови:

$$1956^{659} \equiv r \,(\mathrm{mod}\, 100) \quad \text{і} \quad 0 \leqslant r < 100.$$

З огляду на те, що $1956 \equiv 56 \,(\mathrm{mod}\, 100)$, за властивістю 6 конгруенцій (п.5), маємо: $1956^{659} \equiv 56^{659} \,(\mathrm{mod}\, 100)$. Тому

$$r \equiv 56^{659} \,(\mathrm{mod}\, 100)\,. \tag{II.31}$$

Знайдемо найбільший спільний дільник чисел 56^{659} і 100. Оскільки

$$56^{659} = (2^3 \cdot 7)^{659} = 2^{1977} \cdot 7^{659}, \qquad 100 = 2^2 \cdot 5^2;$$

то $(56^{659}, 100) = 2^2 = 4$. В силу властивості 12 конгруенцій (п.5), із (II.31) випливає, що $(r, 100) = (56^{659}, 100) = 4$, а значить, $r = 4r_1$, де $r_1 \in \mathbb{Z}$, $0 \leqslant r_1 < 25$. Тоді

$$4r_1 \equiv 56^{659} \,(\mathrm{mod}\, 100)$$

або

$$2^2 \cdot r_1 \equiv 2^{1977} \cdot 7^{659} \left(\mathrm{mod}\, 2^2 \cdot 5^2\right).$$

Поділимо обидві частини і модуль даної конгруенції на 2^2:

$$r_1 \equiv 2^{1975} \cdot 7^{659} \,(\mathrm{mod}\, 25)\,.$$

Оскільки $(2, 25) = 1$, то, за теоремою Ойлера, $2^{\varphi(25)} \equiv 1 \,(\mathrm{mod}\, 25)$, тобто $2^{20} \equiv 1 \,(\mathrm{mod}\, 25)$. Звідси

$$2^{1975} = 2^{20\cdot 98+15} = \left(2^{20}\right)^{98} \cdot 2^{15} \equiv 1 \cdot 2^{15} \,(\mathrm{mod}\, 25) \equiv$$
$$\equiv 2^7 \cdot 2^7 \cdot 2 \,(\mathrm{mod}\, 25) \equiv 3 \cdot 3 \cdot 2 \,(\mathrm{mod}\, 25) \equiv 18 \,(\mathrm{mod}\, 25)\,. \quad \text{(II.32)}$$

Аналогічно можна було б застосувати теорему Ойлера і до степеня 7^{659}, однак простіше в цьому випадку поступити іншим чином. Помічаємо, що $7^2 \equiv -1 \,(\mathrm{mod}\, 25)$, значить,

$$7^{659} = 7^{2\cdot 329+1} = \left(7^2\right)^{329} \cdot 7 \equiv (-1)^{329} \cdot 7 \,(\mathrm{mod}\, 25) \equiv -7 \,(\mathrm{mod}\, 25)\,. \quad \text{(II.33)}$$

Тоді із (II.32) і (II.33)

$$r_1 \equiv 18\cdot(-7) \,(\mathrm{mod}\, 25) \equiv (-7)\cdot(-7) \,(\mathrm{mod}\, 25) \equiv -1 \,(\mathrm{mod}\, 25) \equiv 24 \,(\mathrm{mod}\, 25)\,.$$

Значить, $r_1 = 24$, звідки $r = 4r_1 = 4 \cdot 24 = 96$.

Отже, останніми двома цифрами числа 1956^{659} є 96.

Розв'язання в Maple. Знаходимо остачу від ділення заданого числа на 100:

```
> 1956&^659 mod 100;
```

96

Завдання 13. Знайти:

а) остачу від ділення числа a на число m;

б) останню цифру числа c;

в) останні дві цифри числа d.

13.1. $a = 1142^{400} + 17^{200}$, $m = 12$, $c = 2003^{2003}$, $d = 735^{289}$.

13.2. $a = 19^{1981} + 1234^{251}$, $m = 18$, $c = 1907^{1996}$, $d = 384^{545}$.

13.3. $a = 264^{261} + 23^{349}$, $m = 60$, $c = 5044^{1003}$, $d = 693^{243}$.

13.4. $a = 161^{2031} + 159^{94}$, $m = 21$, $c = 2013^{2009}$, $d = 832^{437}$.

13.5. $a = 356^{273} + 7^{31}$, $m = 16$, $c = 1048^{5761}$, $d = 547^{547}$.

13.6. $a = 2007^{2007} + 13^{150}$, $m = 30$, $c = 1993^{1993}$, $d = 396^{175}$.

13.7. $a = 17^{1060} + 555^{243}$, $m = 15$, $c = 2004^{2004}$, $d = 173^{248}$.

13.8. $a = 1001^{526} + 419^{751}$, $m = 22$, $c = 1997^{1997}$, $d = 439^{236}$.

13.9. $a = 13^{2008} + 543^{2008}$, $m = 45$, $c = 5042^{2405}$, $d = 408^{531}$.

13.10. $a = 832^{344} + 7^{561}$, $m = 24$, $c = 6868^{2213}$, $d = 573^{249}$.

13.11. $a = 2502^{801} + 19^{175}$, $m = 12$, $c = 2007^{2007}$, $d = 622^{311}$.

13.12. $a = 5^{255} + 684^{468}$, $m = 14$, $c = 1993^{1995}$, $d = 518^{245}$.

13.13. $a = 1625^{2002} + 22^{2002}$, $m = 75$, $c = 2014^{2014}$, $d = 791^{623}$.

13.14. $a = 13^{289} + 1308^{532}$, $m = 60$, $c = 3332^{167}$, $d = 588^{148}$.

13.15. $a = 4082^{801} + 25^{801}$, $m = 14$, $c = 2083^{2005}$, $d = 394^{251}$.

13.16. $a = 9306^{198} + 11^{271}$, $m = 39$, $c = 1994^{1994}$, $d = 507^{699}$.

13.17. $a = 142^{182} + 4907^{836}$, $m = 21$, $c = 1607^{542}$, $d = 354^{453}$.

13.18. $a = 1089^{51} + 166^{142}$, $m = 27$, $c = 2008^{2008}$, $d = 159^{219}$.

13.19. $a = 519^{153} + 107^{153}$, $m = 12$, $c = 1998^{1998}$, $d = 577^{183}$.

13.20. $a = 274^{563} + 19^{2001}$, $m = 42$, $c = 2493^{777}$, $d = 824^{525}$.

13.21. $a = 196^{293} + 293^{196}$, $m = 48$, $c = 2032^{2006}$, $d = 943^{439}$.

13.22. $a = 605^{205} + 1231^{205}$, $m = 15$, $c = 1987^{1986}$, $d = 378^{233}$.

13.23. $a = 961^{2006} + 378^{32}$, $m = 12$, $c = 5014^{1670}$, $d = 5019^{602}$.

13.24. $a = 203^{547} + 1996^{51}$, $m = 24$, $c = 2038^{533}$, $d = 213^{444}$.

13.25. $a = 344^{1521} + 17^{1521}$, $m = 18$, $c = 4993^{1996}$, $d = 508^{193}$.

7. Конгруенції 1-го степеня з одним невідомим

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $m \in \mathbb{N}$. Конгруенція виду

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \equiv 0 \,(\mathrm{mod}\, m)\,, \qquad \text{(II.34)}$$

де $n \in \mathbb{N}$, $a_i \in \mathbb{Z}$, $0 \leqslant i \leqslant n$, називається **конгруенцією з одним невідомим.** Числа a_i називаються **коефіцієнтами** даної конгруенції, a_n – старшим коефіцієнтом. Якщо $a_n \not\equiv 0 \,(\mathrm{mod}\, m)$, то говорять, що конгруенція (II.34) має степінь n.

Розв'язком конгруенції (II.34) називається клас лишків за модулем m, кожне число якого задовольняє дану конгруенцію. Якщо число x_0 задовольняє конгруенцію (II.34), причому $0 \leqslant x_0 < m$, то розв'язок записують у вигляді: $x \equiv x_0 \,(\mathrm{mod}\, m)$ або $K_{x_0}^{(m)}$. Розв'язати конгруенцію (II.34) означає знайти всі її розв'язки або показати, що їх немає.

Конгруенції з одним невідомим називають **рівносильними** або **еквівалентними**, якщо множини їхніх розв'язків співпадають. Операції, що не порушують множину розв'язків конгруенцій з одним невідомим (їх називають **елементарними перетвореннями**):

1) додавання до обох частин конгруенції довільного многочлена $q(x)$ з цілими коефіцієнтами;
2) додавання до однієї з частин конгруенції многочлена з коефіцієнтами, кратними модулю m;
3) множення і ділення обох частин конгруенції на число, взаємно просте з модулем;
4) множення і ділення обох частин конгруенції і модуля на одне й те саме додатне ціле число.

Конгруенція виду

$$ax \equiv b \,(\mathrm{mod}\, m)\,, \tag{II.35}$$

де $a \not\equiv 0 \,(\mathrm{mod}\, m)$, називається конгруенцією першого степеня з одним невідомим.

Теорема (про існування та число розв'язків конгруенції першого степеня)**.** *Нехай дано конгруенцію 1-го степеня (1). Тоді:*

1) якщо $(a, m) = 1$, то конгруенція (1) має єдиний розв'язок;
2) якщо $(a, m) = d > 1$ і число b не ділиться на d, то конгруенція (1) не має розв'язків;
3) якщо $(a, m) = d > 1$ і число b ділиться на d, то конгруенція (1) має d розв'язків.

Найбільш поширеними способами розв'язування лінійних конгруенцій є:

I. Спосіб спроб. Використовується при невеликих модулях. В конгруенцію підставляються числа повної системи лишків за модулем m (доцільно брати повну систему найменших за абсолютною величиною лишків).

II. Спосіб рівносильних перетворень (штучний спосіб). За допомогою елементарних перетворень задана конгруенція зводиться до рівносильної їй конгруенції з коефіцієнтом при x, рівним 1.

III. Спосіб Ойлера. Розв'язок конгруенції (II.35), де $(a, m) = 1$, знаходять за формулою:

$$x \equiv b a^{\varphi(m)-1} \,(\mathrm{mod}\, m)\,. \tag{II.36}$$

IV. Застосування класів лишків. Розв'язок конгруенції (II.35), де $(a, m) = 1$, знаходять за формулою:

$$K_x^{(m)} = \left(K_a^{(m)}\right)^{-1} \cdot K_b^{(m)}, \tag{II.37}$$

де $\left(K_a^{(m)}\right)^{-1}$ – клас лишків, обернений до класу $K_a^{(m)}$.

За допомогою конгруенцій 1-го степеня з одним невідомим можна розв'язувати невизначені рівняння 1-го степеня з двома невідомими, тобто рівняння виду

$$ax + by = c, \text{ де } a, b, c \in \mathbb{Z}, \text{ де } a \text{ і } b \text{ одночасно не рівні } 0. \qquad \text{(II.38)}$$

(їх ще називають діофантовими). Розв'язком діофантового рівняння (II.38) називають кожну пару (x_0, y_0) цілих чисел x_0 і y_0 таких, що $ax_0 + by_0 = c$. Діофантове рівняння (II.38) має розв'язок тоді і лише тоді, коли $c \vdots d$, де $d = (a, b)$. Множину всіх розв'язків цього рівняння знаходять за формулами:

$$\begin{aligned} x' &= x_0 + bt, \\ y' &= y_0 - at, \qquad \text{де } t - \text{довільне ціле число.} \end{aligned}$$

ПРИКЛАДИ І ЗАДАЧІ

Спосіб спроб

Приклад 14.1 Розв'язати способом спроб конгруенцію:
а) $5x \equiv 2 \,(\mathrm{mod}\, 7)$;
б) $5x \equiv 13 \,(\mathrm{mod}\, 10)$;
в) $12x \equiv 20 \,(\mathrm{mod}\, 16)$.

Розв'язання. а) Маємо: $a = 5$, $m = 7$, $b = 2$. Знайдемо спочатку $(a, m) = (5, 7) = 1$. Отже, задана конгруенція має, причому лише один, розв'язок. Запишемо повну систему абсолютно найменших лишків за модулем $m = 7$:

$$0, 1, 2, 3, -1, -2, -3. \qquad \text{(II.39)}$$

Послідовно підставляючи лишки системи (II.39) в задану конгруенцію, маємо:

$$\begin{aligned} 5 \cdot 0 = 0 &\not\equiv 2 \,(\mathrm{mod}\, 7)\,, \\ 5 \cdot 1 = 5 &\not\equiv 2 \,(\mathrm{mod}\, 7)\,, \\ 5 \cdot 2 = 10 &\not\equiv 2 \,(\mathrm{mod}\, 7)\,, \\ 5 \cdot 3 = 15 &\not\equiv 2 \,(\mathrm{mod}\, 7)\,, \\ 5 \cdot (-1) = -5 &\equiv 2 \,(\mathrm{mod}\, 7)\,. \end{aligned}$$

Отже, число -1 задовольняє задану конгруенцію. Оскільки $-1 \in K_6^{(7)}$, то розв'язком конгруенції є клас $K_6^{(7)}$. Цей розв'язок можна записати ще таким чином: $x \equiv 6 \,(\mathrm{mod}\, 7)$. Інших розв'язків дана конгруенція не має,

тому немає ніякої потреби підставляти в задану конгруенцію інші лишки системи (II.39).

б) Маємо: $a = 5$, $m = 10$, $b = 13$. Оскільки $(a, m) = (5, 10) = 5 > 1$, але $b \nvdots 5$, то задана конгруенція розв'язків не має.

в) В цьому випадку маємо: $a = 12$, $m = 16$, $b = 20$, $(a, m) = (12, 16) = 4 > 1$ і $b \nvdots 4$. Отже, задана конгруенція має 4 розв'язки. Знайдемо їх. Поділимо на число 4 обидві частини і модуль заданої конгруенції. Отримаємо рівносильну їй конгруенцію:

$$3x \equiv 5 \,(\mathrm{mod}\, 4) \tag{II.40}$$

Оскільки $a_1 = 3, m_1 = 4, b_1 = 5$, $(a_1, m_1) = (3, 4) = 1$, то конгруенція (II.40) має лише один розв'язок. Випишемо повну систему абсолютно найменших лишків за модулем $m_1 = 4$:

$$0, 1, 2, -1. \tag{II.41}$$

Послідовно підставляючи лишки системи (II.41) в задану конгруенцію, маємо:

$$\begin{aligned} 3 \cdot 0 = 0 &\not\equiv 5 \,(\mathrm{mod}\, 4)\,, \\ 3 \cdot 1 = 3 &\not\equiv 5 \,(\mathrm{mod}\, 4)\,, \\ 3 \cdot 2 = 6 &\not\equiv 5 \,(\mathrm{mod}\, 4)\,, \\ 3 \cdot (-1) = -3 &\equiv 5 \,(\mathrm{mod}\, 4)\,. \end{aligned}$$

Отже, число -1 задовольняє конгруенцію (II.40). Оскільки $-1 \in K_3^{(4)}$, а клас $K_3^{(4)}$ за модулем 16 розпадається на 4 класи лишків:

$$K_3^{(4)} = K_3^{(16)} \cup K_7^{(16)} \cup K_{11}^{(16)} \cup K_{15}^{(16)},$$

то розв'язками заданої конгруенції є класи $K_3^{(16)}, K_7^{(16)}, K_{11}^{(16)}, K_{15}^{(16)}$. (Ці розв'язки можна записати ще таким чином: $x \equiv 3 \,(\mathrm{mod}\, 16)$, $x \equiv 7 \,(\mathrm{mod}\, 16)$, $x \equiv 11 \,(\mathrm{mod}\, 16)$, $x \equiv 15 \,(\mathrm{mod}\, 16)$.)

Розробка процедур. Створимо процедуру **congr** для розв'язування конгруенцій *способом спроб*. В процесі виконання даної процедури необхідно:

1) для кожного із класів $K_0^{(m)}, K_1^{(m)}, ..., K_{m-1}^{(m)}$ перевірити, чи його представник задовольняє задану конгруенцію, тобто чи виконується умова $ai - b \equiv 0 \pmod{m}$ (в якості представника беремо найменший невід'ємний лишок i із класу $K_i^{(m)}$);

2) щоб отримати кількість розв'язків конгруенції, задати лічильник – число s, значення якого на початку перевірки дорівнює 0.

В результаті на екран виведемо розв'язки та їхню кількість.

```
congr:=proc(a::integer,b::integer,m::integer)
local s,i;
uses numtheory;
   s:=0;
   for i from 0 to m-1 do
      if a*i-b mod m =0 then s:=s+1; print(i) end if;
   end do;
   print(rozvyazkiv, s)
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і розв'язуємо задані конгруенції:

```
> congr(5,2,7);
```

$$6$$
$$1, \mathit{rozvyazkiv}$$

Конгруенція має один розв'язок: $K_6^{(7)}$.

```
> congr(5,13,10);
```

$$0, \mathit{rozvyazkiv}$$

Конгруенція не має розв'язків.

```
> congr(12,20,16);
```

$$3$$
$$7$$
$$11$$
$$15$$
$$4, \mathit{rozvyazkiv}$$

Конгруенція має чотири розв'язки: $K_3^{(16)}$, $K_7^{(16)}$, $K_{11}^{(16)}$, $K_{15}^{(16)}$.

Спосіб рівносильних перетворень

Приклад 14.2 Розв'язати конгруенцію:

$$31x \equiv 25 \,(\mathrm{mod}\, 41) \tag{II.42}$$

способом рівносильних перетворень (штучним способом).

Розв'язання. а) Маємо: $a = 31$, $m = 41$, $b = 25$, $(a, m) = (31, 41) = 1$. Отже, задана конгруенція має один розв'язок. Додамо до лівої частини конгруенції (II.42) вираз $-41x$, кратний модулю. Дістанемо $-10x \equiv 25 \,(\mathrm{mod}\, 41)$. Поділимо обидві частини одержаної конгруенції на число -5: $2x \equiv -5 \,(\mathrm{mod}\, 41)$. Додамо до правої частини число, рівне модулю:

$2x \equiv 36 \pmod{41}$, і поділимо обидві частини останньої конгруенції на 2: $x \equiv 18 \pmod{41}$. Таким чином, клас $K_{18}^{(41)}$ – розв'язок конгруенції (II.42).

б) Маємо: $a = 62$, $m = 82$, $b = 50$, $(a, m) = (62, 82) = 2$ і $b \vdots 2$. Отже, задана конгруенція має два розв'язки. Розділимо обидві частини і модуль даної конгруенції на число 2. Отримаємо рівносильну конгруенцію: $31x \equiv 25 \pmod{41}$, розв'язком якої є клас $K_{18}^{(41)}$. Цей клас розпадається на два класи лишків за модулем 82: $K_{18}^{(41)} = K_{18}^{(82)} \cup K_{59}^{(82)}$. Класи $K_{18}^{(82)}, K_{59}^{(82)}$ є розв'язками заданої конгруенції.

Розробка процедур. Процедура **congrub** для розв'язування конгруенції $ax \equiv b \pmod{m}$ способом рівносильних перетворень повинна мати наступний алгоритм:

1) перевірка, чи має задана конгруенція розв'язки; якщо так, то скільки їх;

2) зведення заданої конгруенції до конгруенції виду $a_1 x \equiv b_1 \pmod{m_1}$, де $(a_1, m_1) = 1$ (шляхом ділення обох частин конгруенції і модуля на число $d = (a, m)$);

3) пошук числа t такого, що $b_1 + m_1 t \vdots a_1$.

Зауваження. Відмітимо, що для цього достатньо перебрати всі цілі числа із проміжку $[0; |a_1|)$. Дійсно, нехай t_1 – деяке ціле число таке, що $b_1 + m_1 t_1 \vdots a_1$, тобто $b_1 + m_1 t = a_1 y$ (де $y \in \mathbb{Z}$). Розділимо число t_1 на a_1 з остачею: $t_1 = a_1 q + r$, де $0 \leqslant r < |a_1|$; тоді $b_1 + m_1(a_1 q_1 + r_1) = a_1 y$, звідки $b_1 + m_1 r = a_1(y - m_1 q_1)$, значить, $b_1 + m_1 r \vdots a_1$. Число $t = r$ – шукане.

4) розв'язком конгруенції $a_1 x \equiv b_1 + m_1 t \pmod{m_1}$ є $x \equiv \frac{b_1 + m_1 t}{a_1} \pmod{m_1}$;

5) пошук розв'язків заданої конгруенції, враховуючи властивість 8 класів лишків (див. §5).

Відповідна процедура має вигляд:

```
congrub:=proc(a::integer,b::integer,m::integer)
local d,a1,b1,m1,x,i,k;
uses numtheory:
   d:=igcd(a,m); #1
   if b mod d<>0 then print(nemae_rozvyazkiv); end if;
   if b mod d=0 then print(d,rozvyazkiv);
      a1:=a/d; b1:=b/d; m1:=m/d; #2
      for k from 0 to abs(a1) do #3
         if (b1+m1*k) mod a1=0 then
            x:=(b1+m1*k)/a1 mod m1; break; #4
         end if;
      end do;
      for i from 0 to d-1 do print(x+i*m1); end do; #5
   end if;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо команду **congrub**:

```
> congrub(31,25,41);
```

1, *rozvyazkiv*

18

```
> congrub(62,50,82);
```

2, *rozvyazkiv*

18

59

Спосіб Ойлера

Приклад 14.3 Розв'язати конгруенцію:

а) $3x \equiv 4 \pmod 5$;

б) $27x \equiv 30 \pmod{48}$;

в) $15x \equiv 20 \pmod 9$;

способом Ойлера.

Розв'язання. а) Маємо: $a = 3$, $m = 5$, $(a, m) = (3, 5) = 1$. Отже, задана конгруенція має один розв'язок. Цей розв'язок знаходимо за формулою Ойлера (II.36). Обчислюємо: $\varphi(5) = 4$. Тоді:

$$x \equiv 4 \cdot 3^{\varphi(5)-1} \equiv 4 \cdot 3^3 \pmod 5 \equiv 4 \cdot 2 \pmod 5 \equiv 3 \pmod 5 .$$

Отже, розв'язком заданої конгруенції є клас $K_3^{(5)}$.

б) Маємо: $a = 27$, $m = 48$, $b = 30$, $(a, m) = (27, 48) = 3 > 1$ і $b \vdots 3$. Отже, задана конгруенція має 3 розв'язки. Поділимо на число 3 обидві частини і модуль заданої конгруенції. Отримаємо рівносильну їй конгруенцію:

$$9x \equiv 10 \pmod{16} \qquad \text{(II.43)}$$

Оскільки $a_1 = 9$, $m_1 = 16$, $(a_1, m_1) = (9, 16) = 1$, то конгруенція (II.43) має лише один розв'язок, який можна знайти за формулою (II.36). Маємо:

$$x \equiv 10 \cdot 9^{\varphi(16)-1} \pmod{16} .$$

Знайдемо спочатку $\varphi(16)$: $\varphi(16) = \varphi(2^4) = 2^4(1 - \frac{1}{2}) = 8$. Тоді

$$x \equiv 10 \cdot 9^7 \pmod{16} \equiv 10 \cdot (9^2)^3 \cdot 9 \pmod{16} \equiv$$
$$\equiv 10 \cdot 1^3 \cdot 9 \pmod{16} \equiv 90 \pmod{16} \equiv 10 \pmod{16} .$$

Отже, клас $K_{10}^{(16)}$ є розв'язком конгруенції (II.43).

Цей клас розпадається на 3 класи лишків за модулем 48:

$$K_{10}^{(16)} = K_{10}^{(48)} \cup K_{26}^{(48)} \cup K_{42}^{(48)},$$

які є розв'язками заданої конгруенції. Запишемо їх в іншому вигляді: $x \equiv 10 \,(\mathrm{mod}\, 48)$, $x \equiv 26 \,(\mathrm{mod}\, 48)$, $x \equiv 42 \,(\mathrm{mod}\, 48)$.

в) Маємо: $a = 15$, $m = 9$, $b = 20$, $(a, m) = (15, 9) = 3 > 1$ і $b \vdots 3$. Отже, задана конгруенція не має розв'язків.

Зауваження. Недоліком способу Ойлера є те, що при великому значенні $\varphi(m)$ знаходження найменшого невід'ємного лишку того класу чисел за модулем m, до якого належить число $ba^{\varphi(m)-1}$, стає громіздким.

Розробка процедур. Для того, щоб при розв'язуванні конгруенції можна було скористатись способом Ойлера, необхідно, щоб виконувалась умова $(a, m) = 1$. Тому першим рядком в тілі відповідної процедури **congruv** має бути рядок, що визначає кількість розв'язків заданої конгруенції: спочатку знаходимо $d = (a, m)$ і перевіряємо, чи $b \vdots d$. Якщо конгруенція має d розв'язків, то ділимо кожне із чисел a, b, m на d.

```
congruv:=proc(a::integer,b::integer,m::integer)
local d,a1,b1,m1,x,i;
uses numtheory;
   d:=igcd(a,m);
   if b mod d<>0 then print(nemae_rozvyazkiv); end if;
   if b mod d=0 then print(d,rozvyazkiv);
      a1:=a/d; b1:=b/d; m1:=m/d;
      x:=b1*a1^(phi(m1)-1) mod m1;
      for i from 0 to d-1 do print(x+i*m1); end do;
   end if;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо процедуру **congruv**: для розв'язання заданих конгруенцій:

```
> congruv(3,4,5);
```

$$1,\ \mathit{rozvyazkiv}$$

$$3$$

Конгруенція має один розв'язок: $K_3^{(5)}$.

```
> congruv(15,20,25);
```

$$5,\ \mathit{rozvyazkiv}$$

3
8
13
18
23

Конгруенція має п'ять розв'язків: $K_3^{(25)}$, $K_8^{(25)}$, $K_{13}^{(25)}$, $K_{18}^{(25)}$, $K_{23}^{(25)}$.

```
> congruv(15,20,9);
```

nemae_rozvyazkiv

Конгруенція не має розв'язків.

Застосування класів лишків

Приклад 14.4 Розв'язати конгруенцію із використанням класів лишків:

а) $37x \equiv 10 \pmod{62}$;

б) $15x \equiv 20 \pmod{25}$;

в) $15x \equiv 20 \pmod{9}$

Розв'язання. а) Маємо: $a = 37$, $m = 62$, $b = 10$, $(a, m) = (37, 62) = 1$. Отже, задана конгруенція має один розв'язок. Використовуючи формулу (II.37), дістаємо:

$$K_x^{(62)} = \left(K_{37}^{(62)}\right)^{-1} \cdot K_{10}^{(62)}. \qquad \text{(II.44)}$$

Обчислимо $\left(K_{37}^{(62)}\right)^{-1}$ – клас лишків, обернений до класу $K_{37}^{(62)}$.

Для цього, використовуючи алгоритм Евкліда, знаходимо лінійне представлення найбільшого спільного дільника чисел $a = 37$ і $m = 62$. Маємо:

$$\begin{array}{rr|l|l}
m = & 62 & 37 & = a \\
\hline
 & 37 & 1 & \\
\hline
a = & 37 & 25 & = r_1 \\
\hline
 & 25 & 1 & \\
\hline
r_1 = & 25 & 12 & = r_2 \\
\hline
 & 24 & 2 & \\
\hline
r_2 = & 12 & 1 & = r_3 \neq 0 \\
\hline
 & 12 & 12 & \\
\hline
 & 0 & &
\end{array}$$

Запишемо отримані рівності:

$$\begin{array}{lll} m = a + r_1, & & r_1 = m - a, \\ a = r_1 + r_2, & \text{звідки} & r_2 = a - r_1, \\ r_1 = 2r_2 + 1, & & 1 = r_1 - 2r_2. \end{array}$$

Із останньої рівності отримуємо:

$$1 = r_1 - 2r_2 = r_1 - 2(a - r_1) = -2a + 3r_1 = -2a + 3(m - a) = \\ = 3m - 5a = 3m + (-5)a = 3 \cdot 62 + (-5) \cdot 37.$$

Тоді

$$K_1^{(62)} = K_{3\cdot 62+(-5)\cdot 37}^{(62)} = K_{3\cdot 62}^{(62)} + K_{(-5)\cdot 37}^{(62)} = K_0^{(62)} + K_{(-5)\cdot 37}^{(62)} = \\ = K_{(-5)\cdot 37}^{(62)} = K_{-5}^{(62)} \cdot K_{37}^{(62)} = K_{57}^{(62)} \cdot K_{37}^{(62)}.$$

Таким чином, $K_1^{(62)} = K_{57}^{(62)} \cdot K_{37}^{(62)}$, значить,

$$(K_{37}^{(62)})^{-1} = K_{57}^{(62)}. \qquad \text{(II.45)}$$

Із умов (II.44) і (II.45) отримуємо:

$$K_x^{(62)} = K_{57}^{(62)} \cdot K_{10}^{(62)} = K_{-5}^{(62)} \cdot K_{10}^{(62)} = K_{-50}^{(62)} = K_{12}^{(62)}.$$

Отже, розв'язком заданої конгруенції є клас $K_{12}^{(62)}$.

б) Маємо: $a = 15$, $m = 25$, $b = 20$, $(a, m) = (15, 25) = 5$ і $b \vdots 5$. Отже, задана конгруенція має п'ять розв'язків. Розділимо обидві частини і модуль даної конгруенції на 5: $3x \equiv 4 \pmod 5$. Щоб знайти розв'язки триманої конгруенції, застосуємо формулу (II.37): $K_x^{(5)} = \left(K_3^{(5)}\right)^{-1} \cdot K_4^{(5)}$. Клас, обернений до класу $K_3^{(5)}$, легко знайти: цим класом є $K_2^{(5)}$. Отже, $K_x^{(5)} = K_2^{(5)} \cdot K_4^{(5)} = K_8^{(5)} = K_3^{(5)}$. Цей клас розпадається на 5 класів лишків за модулем 25:

$$K_3^{(5)} = K_3^{(25)} \cup K_8^{(25)} \cup K_{13}^{(25)} \cup K_{18}^{(25)} \cup K_{23}^{(25)}.$$

Розв'язками заданої конгруенції є: $K_3^{(25)}, K_8^{(25)}, K_{13}^{(25)}, K_{18}^{(25)}, K_{23}^{(25)}$.

в) Маємо: $a = 15$, $m = 9$, $b = 20$, $(a, m) = (15, 9) = 3$ і $b \vdots 5$. Отже, задана конгруенція не має розв'язків.

Розробка процедур. Для існування класу лишків, оберненого до класу $K_a^{(m)}$, необхідно, щоб виконувалась умова $(a, m) = 1$. Тому процедура **congrug**

має початок, ідентичний початку процедури **congruv** із Прикладів 14.2 і 14.3. Різниця – у формулі для відшукання розв'язку.

```
congrug:=proc(a::integer,b::integer,m::integer)
local d,a1,b1,m1,x,i;
uses numtheory;
   d:=igcd(a,m);
   if b mod d<>0 then print(nemae_rozvyazkiv); end if;
   if b mod d=0 then print(d,rozvyazkiv);
      a1:=a/d; b1:=b/d; m1:=m/d;
      x:=(a1^(-1) mod m1)*b1 mod m1;
      for i from 0 to d-1 do print(x+i*m1);
      end do;
   end if;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо команду **congrug**:

```
> congrug(37,10,62);
```

$$1,\ rozvyazkiv$$
$$12$$

Конгруенція має один розв'язок: $K_{12}^{(62)}$.

```
> congrug(15,20,25);
```

$$5,\ rozvyazkiv$$
$$3$$
$$8$$
$$13$$
$$18$$
$$23$$

Конгруенція має п'ять розв'язків: $K_3^{(25)}$, $K_8^{(25)}$, $K_{13}^{(25)}$, $K_{18}^{(25)}$, $K_{23}^{(25)}$.

```
> congrug(15,20,9);
```

$$nemae\_rozvyazkiv$$

Конгруенція не має розв'язків.

Використання команди ***msolve***

В Maple є і власна вбудована команда **msolve**, яка дозволяє розв'язувати конгруенції довільного степеня та системи конгруенцій. Команда має наступний формат **msolve(eqns,vars,m)** або **msolve(eqns,m)**, де eqns – рівняння (набір рівнянь), vars – (необов'язковий параметр) – набір змінних. Якщо розв'язок невизначений, то, в разі, якщо це можливо, він подається

через змінні, імена яких зазначено в vars (або глобальні імена _Z1, _Z2, _Z3, якщо vars упущено). Команда msolve повертає NULL, якщо в цілих числах за mod m конгруенція розв'язків немає. В окремих випадках повертається частинний розв'язок. Якщо msolve не може розв'язати конгруенцію (або систему конгруенцій), але і не може довести, що розв'язків немає, то з'являється запис FAIL.

Конгруенцію $5x \equiv 2 \pmod 7$ записуємо у вигляді рівняння $5x = 2$ за модулем 7:

```
> msolve(5*x=2,7);
```

$$\{x = 6\}$$

Дана конгруенція має єдиний розв'язок $K_6^{(7)}$.

```
> msolve(5*x=13,10);
```

В рядку виведення не з'явилось жодного запису. Це означає, що конгруенція не має розв'язків.

```
> msolve(12*x=20,16);
```

$$\{x = 3\},\ \{x = 7\},\ \{x = 11\},\ \{x = 15\}$$

Конгруенція має 4 розв'язки: $K_3^{(16)}$, $K_7^{(16)}$, $K_{11}^{(16)}$, $K_{15}^{(16)}$.

Створення власної процедури, навіть у випадку коли вбудована команда існує, дає певні переваги: зокрема, це можливість перевірки правильності проміжних обчислень. Виклик на екран результатів проміжних обчислень здійснюється за допомогою команди **trace**. Для цього після введення процедури, застосовуємо команду trace і викликаємо процедуру. Так, наприклад, для виведення на екран проміжних обчислень при розв'язуванні конгруенції $27x \equiv 30 \pmod{48}$ способом Ойлера потрібно зробити наступне.

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Записуємо команду **trace** із параметром congruv (назва потрібної процедури):

```
> trace(congruv);
```

В результаті застосування процедури **congruv** до заданих чисел отримаємо:

```
> congruv(27,30,48);
```

congruv

```
{--> enter congruv, args = 27, 30, 48
```

$$d := 3$$

3, *rozvyaz*

$$a1 := 9$$
$$b1 := 10$$
$$m1 := 16$$
$$x := 10$$
$$10$$
$$26$$
$$42$$

```
<-- exit congruv (now at top level) = }
```

Отже, в ході процедури було знайдено:
1) $d = (a, m) = 3$;
2) кількість розв'язків – 3;
3) рівносильну заданій конгруенцію $9x \equiv 10 \pmod{16}$;
4) розв'язок $K_{10}^{(16)}$ конгруенції із п.3);
5) розв'язки заданої конгруенції $K_{10}^{(48)}$, $K_{26}^{(48)}$, $K_{42}^{(48)}$.

Завдання 14. Розв'язати конгруенцію:
а) способом спроб;
б) способом рівносильних перетворень (штучним способом);
в) способом Ойлера;
г) із використанням класів лишків.

14.1. а) $6x \equiv 12 \pmod{8}$; в) $22x \equiv -64 \pmod{13}$;
б) $192x \equiv 9 \pmod{327}$; г) $21x \equiv 24 \pmod{99}$.

14.2. а) $3x \equiv 2 \pmod{8}$; в) $21x \equiv 3 \pmod{12}$;
б) $20x \equiv 14 \pmod{52}$; г) $32x \equiv 94 \pmod{51}$.

14.3. а) $6x \equiv 9 \pmod{15}$; в) $3x \equiv 8 \pmod{23}$;
б) $32x \equiv 100 \pmod{46}$; г) $4x \equiv 15 \pmod{21}$.

14.4. а) $5x \equiv 7 \pmod{6}$; в) $28x \equiv 43 \pmod{19}$;
б) $32x \equiv 44 \pmod{12}$; г) $22x \equiv -64 \pmod{54}$.

14.5. а) $4x \equiv 6 \pmod{10}$; в) $22x \equiv 62 \pmod{12}$;
б) $239x \equiv 302 \pmod{471}$; г) $21x \equiv 33 \pmod{57}$.

14.6. а) $4x \equiv 9 \pmod{5}$; в) $5x \equiv 6 \pmod{11}$;
б) $50x \equiv 62 \pmod{42}$; г) $26x \equiv 58 \pmod{60}$.

14.7. а) $10x \equiv 12 \pmod 8$; в) $26x \equiv 3 \pmod{15}$;
б) $111x \equiv 75 \pmod{32}$; г) $21x \equiv 24 \pmod{69}$.

14.8. а) $5x \equiv 11 \pmod{13}$; в) $15x \equiv 20 \pmod{22}$;
б) $48x \equiv 60 \pmod{52}$; г) $28x \equiv 43 \pmod{51}$.

14.9. а) $12x \equiv 4 \pmod 8$; в) $12x \equiv 90 \pmod{39}$;
б) $90x \equiv 24 \pmod{48}$; г) $15x \equiv 23 \pmod{81}$.

14.10. а) $6x \equiv 2 \pmod 7$; в) $17x \equiv 23 \pmod{12}$;
б) $312x \equiv 2180 \pmod{148}$; г) $13x \equiv -1 \pmod{99}$.

14.11. а) $9x \equiv 6 \pmod{12}$; в) $11x \equiv -32 \pmod{13}$;
б) $27x \equiv 48 \pmod{31}$; г) $14x \equiv 16 \pmod{79}$.

14.12. а) $5x \equiv 11 \pmod 9$; в) $15x \equiv 2 \pmod{34}$;
б) $42x \equiv 70 \pmod{63}$; г) $28x \equiv 43 \pmod{91}$.

14.13. а) $10x \equiv 6 \pmod 8$; в) $12x \equiv 4 \pmod{20}$;
б) $57x \equiv 21 \pmod{39}$; г) $27x \equiv 31 \pmod{95}$.

14.14. а) $4x \equiv 3 \pmod{10}$; в) $21x \equiv 36 \pmod{15}$;
б) $16997x \equiv 53 \pmod{169}$; г) $12x \equiv 22 \pmod{106}$.

14.15. а) $15x \equiv 10 \pmod{20}$; в) $20x \equiv 60 \pmod{48}$;
б) $32x \equiv 43 \pmod{51}$; г) $19x \equiv 23 \pmod{83}$.

14.16. а) $4x \equiv 7 \pmod 5$; в) $25x \equiv 61 \pmod{18}$;
б) $152x \equiv 14 \pmod{70}$; г) $54x \equiv 27 \pmod{123}$.

14.17. а) $18x \equiv 9 \pmod{15}$; в) $32x \equiv 5 \pmod{13}$;
б) $23x \equiv 41 \pmod{57}$; г) $15x \equiv 43 \pmod{73}$.

14.18. а) $8x \equiv 3 \pmod{15}$; в) $28x \equiv 2 \pmod{40}$;
б) $378x \equiv 342 \pmod{51}$; г) $10x \equiv 12 \pmod{92}$.

14.19. а) $5x \equiv 6 \pmod{10}$; в) $17x \equiv 21 \pmod{15}$;
б) $27x \equiv 24 \pmod{102}$; г) $11x \equiv 13 \pmod{87}$.

14.20. а) $9x \equiv 2 \pmod{10}$; в) $11x \equiv 6 \pmod{18}$;
б) $32x \equiv 44 \pmod{46}$; г) $55x \equiv 2 \pmod{147}$.

14.21. а) $22x \equiv 4 \pmod{6}$; в) $4x \equiv 9 \pmod{11}$;
б) $1215x \equiv 560 \pmod{275}$; г) $42x \equiv 130 \pmod{172}$.

14.22. а) $4x \equiv 9 \pmod{7}$; в) $28x \equiv 6 \pmod{34}$;
б) $36x \equiv 30 \pmod{42}$; г) $23x \equiv 3 \pmod{74}$.

14.23. а) $14x \equiv 18 \pmod{20}$; в) $7x \equiv 13 \pmod{12}$;
б) $42x \equiv 51 \pmod{39}$; г) $52x \equiv 10 \pmod{132}$.

14.24. а) $8x \equiv 3 \pmod{7}$; в) $27x \equiv 3 \pmod{20}$;
б) $440x \equiv 56 \pmod{696}$; г) $52x \equiv 13 \pmod{69}$.

14.25. а) $8x \equiv 12 \pmod{10}$; в) $12x \equiv 51 \pmod{39}$;
б) $12x \equiv 30 \pmod{50}$; г) $43x \equiv 27 \pmod{85}$.

Приклад 15. Розв'язати в цілих числах $7x - 12y = 15$ (за допомогою конгруенцій).

Розв'язання. Оскільки $(7, -12) = 1$, $15 \vdots 1$, то рівняння має розв'язки. Нехай (x_0, y_0) – один із розв'язків заданого рівняння. Тоді $7x_0 - 12y_0 = 15$. Перейдемо до конгруенції за модулем 12 (наприклад): для чисел x_0, y_0 справедливо, що $7x_0 - 12y_0 \equiv 15 \pmod{12}$, а значить, $7x_0 \equiv 3 \pmod{12}$. Це означає, що клас $K_{x_0}^{(12)}$ є розв'язком конгруенції $7x \equiv 3 \pmod{12}$. Розв'яжемо її. Використаємо штучний спосіб: $7x - 12x \equiv 3 + 12 \pmod{12}$, тобто $-5x \equiv 15 \pmod{12}$, звідки $x \equiv -3 \pmod{12}$. Дана конгруенція має розв'язком клас $K_9^{(12)}$, а отже, $x_0 \in K_9^{(12)}$.

Нехай $x_0 = 9$, тоді $63 - 12y_0 = 15$, звідки $y_0 = 4$. Отже, одним із розв'язків заданого рівняння є $(9, 4)$. Всі розв'язки знаходимо за формулами (II.38):

$$\begin{aligned} x' &= 9 - 12t, \\ y' &= 4 - 7t, \qquad \text{де } t \in \mathbb{Z}. \end{aligned}$$

Отже, розв'язком заданого рівняння є кожна пара $(9-12t, 4-7t)$, де $t \in \mathbb{Z}$.

Розв'язання в Maple. Для розв'язування рівнянь в цілих числах використовується команда **isolve**, формат якої аналогічний до формату команди **solve** (див. §6 розд.I). У випадку одного рівняння маємо:

```
> isolve(7*x-12*y=15);
```

$$\{x = 9 + 12\,\_Z1,\ y = 4 + 7\,\_Z1\}$$

При $z\_1 = -t$ маємо розв'язок, отриманий аналітично.

Завдання 15. Розв'язати в цілих числах:

15.1. а) $2x - 3y = 7$; б) $-8x + 6y = 12$.

15.2. а) $-3x + 5y = 6$; б) $14x - 4y = 12$.

15.3. а) $2x - 3y = 7$; б) $-8x + 6y = 12$.

15.4. а) $2x - 5y = 8$; б) $6x + 20y = 22$.

15.5. а) $x + 8y = -11$; б) $-24x + 30y = 42$.

15.6. а) $-8x + 9y = 5$; б) $15x + 12y = 18$.

15.7. а) $7x - 2y = 13$; б) $5x - 25y = 14$.

15.8. а) $4x + 3y = 9$; б) $-18x + 20y = -26$.

15.9. а) $-5x + 7y = 12$; б) $15x + 9y = 20$.

15.10. а) $2x + 5y = 11$; б) $10x - 25y = 33$.

15.11. а) $3x - 10y = -5$; б) $15x + 18y = -21$.

15.12. а) $6x - 7y = 9$; б) $-4x + 10y = 24$.

15.13. а) $-x + 8y = 10$; б) $20x - 15y = 16$.

15.14. а) $5x - y = 7$; б) $8x - 6y = 28$.

15.15. а) $-4x + 3y = 2$; б) $3x + 24y = 21$.

15.16. а) $2x + 7y = -9$; б) $6x + 12y = 15$.

15.17. а) $3x + 8y = 10$; б) $-15x + 12y = 24$.

15.18. а) $-12x + 5y = 4$; б) $12x + 15y = 18$.

15.19. а) $-x + y = 7$; б) $9x + 15y = -48$.

15.20. а) $5x - 8y = 10$; б) $-6x + 15y = 41$.

15.21. а) $6x - y = 3$; б) $14x - 6y = -20$.

15.22. а) $-4x + 7y = 13$; б) $-6x + 16y = 22$.

15.23. а) $10x + 3y = 7$; б) $14x - 12y = 16$.

15.24. а) $-3x + 5y = 12$; б) $20x - 16y = 25$.

15.25. а) $5x - 4y = 13$; б) $4x + 14y = -30$.

8. Системи конгруенцій 1-го степеня з одним невідомим

ТЕОРЕТИЧНІ ВІДОМОСТІ

Розв'язування системи конгруенцій 1-го степеня з одним невідомим

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1}, \\ a_2x \equiv b_2 \pmod{m_2}, \\ \dots \quad \dots \quad \dots, \\ a_sx \equiv b_s \pmod{m_s}, \end{cases}$$

починають із зведення її (якщо це можливо) до виду

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots \quad \dots \quad \dots, \\ x \equiv c_s \pmod{m_s}, \end{cases} \tag{II.46}$$

(тобто знаходять розв'язки кожної із конгруенцій окремо). Якщо якась із конгруенцій не має розв'язків, то і вся задана система також не має розв'язків.

Можливі наступні випадки.

а) У випадку попарно взаємно простих модулів системи (II.48) розв'язання грунтується на китайській теоремі про остачі.

Теорема (китайська теорема про остачі)**.** *Якщо* $(m_i, m_j) = 1$ *для всіх* $i, j \in \overline{1,s}$, $i \neq j$, *то розв'яок системи* (II.48) *існує і ним є клас лишків* $K_{x_0}^{(M)}$ *такий, що:*

$$\begin{aligned} M &= m_1m_2...m_s; \\ x_0 &\equiv c_1y_1M_1 + c_2y_2M_2 + ... + c_sy_sM_s \pmod{M}, \end{aligned} \tag{II.47}$$

де $M_i = \frac{M}{m_i}$ *для всіх* $i = 1, 2, ..., s$,
а y_i *визначаються із умов* $y_iM_1 \equiv 1 \pmod{m_i}$.

В загальному випадку (коли числа m_i не обов'язково попарно взаємно прості) систему конгруенцій (II.48) розв'язують в наступний спосіб. Нехай $K_{x_0}^{(m_1)}$ – розв'язок системи (II.48). Тоді

$$\begin{cases} x_0 \equiv c_1 \pmod{m_1}, \\ x_0 \equiv c_2 \pmod{m_2}, \\ .. \quad ... \quad\quad ...., \\ x_0 \equiv c_s \pmod{m_s}. \end{cases} \tag{II.48}$$

З 1-ої конгруенції отримуємо:

$$x_0 = c_1 + m_1 t_1 \tag{II.49}$$

для деякого $t_1 \in \mathbb{Z}$. Це значення підставляємо в 2-гу конгруенцію і шукаємо t_1: $c_1 + m_1 t_1 \equiv c_2 \pmod{m_2}$. Знайдений вираз для t_1 підставляємо в рівність (II.49), а отриманий вираз для x_0, в свою чергу, в 3-тю конгруенцію системи і т.д. Зрозуміло, що на деякому кроці можна отримати конгруенцію, що не має розв'язків, тоді і задана система конгруенцій не має розв'язків.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 16.1 Розв'язати систему конгруенцій:

$$\begin{cases} 2x \equiv 9 \pmod{17}, \\ 15x \equiv 25 \pmod{19}, \\ 21x \equiv 18 \pmod{30}. \end{cases}$$

Розв'язання. Розв'язуючи кожну конгруенцію окремо, заміняємо задану систему конгруенцій на еквівалентну їй:

$$\begin{cases} x \equiv 13 \pmod{17}, \\ x \equiv 8 \pmod{19}, \\ x \equiv 8 \pmod{10}. \end{cases} \tag{II.50}$$

Оскільки модулі конгруенцій попарно взаємно прості, то можна використати китайську теорему про остачі. Маємо: $M = m_1 m_2 m_3 = 17 \cdot 19 \cdot 10 = 3230$, $M_1 = \frac{M}{m_1} = \frac{3230}{17} = 190$, $M_2 = \frac{M}{m_2} = \frac{3230}{19} = 170$, $M_3 = \frac{M}{m_3} = \frac{3230}{10} = 323$. Знаходимо y_i із умов: $M_i y_i \equiv 1 \pmod{m_i}$. Маємо: $190y_1 \equiv 1 \pmod{17}$, тоді $3y_1 \equiv 18 \pmod{17}$, звідки $y_1 \equiv 6 \pmod{17}$. Далі $170y_2 \equiv 1 \pmod{19}$, тому $-y_2 \equiv 1 \pmod{19}$, звідки $y_2 \equiv -1 \pmod{19}$. І $323y_3 \equiv 1 \pmod{10}$, тоді $3y_3 \equiv 21 \pmod{10}$, а значить, $y_3 \equiv 7 \pmod{10}$.

За формулою (II.47), $x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 \pmod{M} \equiv 190 \cdot 6 \cdot 13 + 170 \cdot (-1) \cdot 8 + 323 \cdot 7 \cdot 10 \pmod{3230} \equiv 2478 \pmod{3230}$. Отже, розв'язком системи конгруенцій є клас $K_{2478}^{(3230)}$.

Розв'язання в Maple. На основі китайської теореми про остачі в Maple розроблено команду **chrem(c,m)** для розв'язування системи конгруенцій

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots \quad \dots \quad \dots, \\ x \equiv c_3 \pmod{m_s}; \end{cases}$$

із попарно взаємно простими модулями. Параметрами даної команди є списки c=[c1,c2,...,cs], m=[m1,m2,...,ms].

Застосуємо дану команду до системи (II.50). Маємо:

```
> chrem([13,8,8],[17,19,10]);
```

2478

Отже, розв'язком системи конгруенцій є клас $K_{2478}^{(3230)}$.

Приклад 16.2 Розв'язати систему конгруенцій:

$$\begin{cases} 2x \equiv 31 \pmod{35}, \\ 4x \equiv 7 \pmod{25}, \\ 5x \equiv 18 \pmod{21}. \end{cases}$$

Розв'язання. Розв'язавши спочатку кожну із конгруенцій окремо, отримуємо рівносильну заданій систему конгруенцій:

$$\begin{cases} x \equiv 33 \pmod{35}, \\ x \equiv 8 \pmod{25}, \\ x \equiv 12 \pmod{21}. \end{cases} \tag{II.51}$$

Оскільки модулі даної конгруенції не є попарно взаємно простими, то китайську теорему про остачі застосувати не можна.

Нехай $K_{x_0}^{(M)}$ – розв'язок даної системи, тоді $M = [35, 25, 21] = 525$ і

$$\begin{cases} x_0 \equiv 33 \pmod{35}, \\ x_0 \equiv 8 \pmod{25}, \\ x_0 \equiv 12 \pmod{21}. \end{cases}$$

З 1-ої конгруенції маємо: $x_0 = -2 + 35t$ для деякого $t \in \mathbb{Z}$. Підставляючи x_0 в другу конгруенцію, отримуємо: $-2 + 35t \equiv 8 \pmod{25}$, тобто $10t \equiv 10 \pmod{25}$. Розділити обидві частини конгруенції на 10 не можна, оскільки $(10, 25) \neq 1$. Тому розділимо обидві частини і модуль на 5: $2t \equiv 2 \pmod{5}$.

Оскільки $(2, 5) = 1$, то можна розділити обидві частини конгруенції на 2: $t \equiv 1 \pmod{5}$, звідси $t = 1 + 5s$ для деякого $s \in \mathbb{Z}$. Тоді $x_0 = -2 + 35(1 + 5s) = 33 + 175t$.

Тепер підставимо x_0 в третю конгруенцію: $33 + 175t \equiv -21 \pmod{21}$, тобто $7s \equiv 0 \pmod{s}$. Тоді $s = 3k$ для деякого $k \in \mathbb{Z}$, звідки $x_0 = 33 + 175 \cdot 3k = 33 + 525k$. Отже, $x_0 \in K_{33}^{(525)}$, а значить, $K_{33}^{(525)}$ – розв'язок заданої системи конгруенцій.

Розробка процедур. Щоб створити процедуру **syscongr** для розв'язування системи конгруенцій

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1}, \\ a_1 x \equiv b_2 \pmod{m_2}, \\ \dots \\ a_s x \equiv b_s \pmod{m_s}. \end{cases} \tag{II.52}$$

із довільними модулями розглянемо алгоритм розв'язування такої системи:
1) перехід до системи конгруенцій виду

$$\begin{cases} x \equiv c_1 \pmod{m_1'}, \\ x \equiv c_2 \pmod{m_2'}, \\ x \equiv c_3 \pmod{m_3'}, \\ \dots \\ x \equiv c_s \pmod{m_s'}. \end{cases}$$

Для цього кожну конгруенцію розв'язують окремо. При цьому можливо, що якась із конгруенцій системи не має розв'язків ($b_i \vdots d_i$, $d_i = (a_i, b_i)$) – тоді і задана система не матиме розв'язків.

2) Далі, виразивши з 1-ої конгруенції x: $x = c_1 + m_1' t_1$, $t_1 \in \mathbb{Z}$, і підставивши вираз до 2-ої конгруенції, матимемо:

$$\begin{cases} c_1 + m_1' t_1 \equiv c_2 \pmod{m_2'}, \\ x \equiv c_3 \pmod{m_3'}, \\ \dots \\ x \equiv c_s \pmod{m_s'}. \end{cases}$$

Тоді, розв'язуючи 1-шу конгруенцію, наприклад, способом 4 (із використанням класів лишків), отримуємо (якщо вона має розв'язки, тобто якщо $(c_2 - c_1) \vdots d_1'$, де $d_1' = (m_1', m_2')$): $t_1 \equiv \left(\frac{m_1'}{d_1'}\right)^{-1} \cdot \frac{c_2 - c_1}{d_1'} \pmod{\frac{m_2'}{d_1'}}$, звідки $t_1 = \left[\left(\left(\frac{m_1'}{d_1'}\right)^{-1} \cdot \frac{c_2 - c_1}{d_1'} \right) \mathrm{mod} \frac{m_1'}{d_1'} \right] + \frac{m_2'}{d_1'} t_2$, де $t_2 \in \mathbb{Z}$. Тепер повертаємось до невідомого x:

$$x = c_1 + m_1' t_1 = c_1 + m_1' \left(\left[\left(\left(\frac{m_1'}{d_1'}\right)^{-1} \cdot \frac{c_2 - c_1}{d_1'} \right) \mathrm{mod} \frac{m_1'}{d_1'} \right] + \frac{m_2'}{d_1'} t_2 \right) =$$

$$= c_1 + m_1' \left[\left(\left(\frac{m_1'}{d_1'}\right)^{-1} \cdot \frac{c_2 - c_1}{d_1'} \right) \mathrm{mod} \frac{m_1'}{d_1'} \right] + \frac{m_1' m_2'}{d_1'} t_2.$$

Нехай $c_1 = h_1$, $h_1 + m'_1 \left[(\left(\frac{m'_1}{d'_1}\right)^{-1} \cdot \frac{c_2 - h_1}{d'_1}) \mathrm{mod} \frac{m'_2}{d'_1} \right] = h_2$. Тоді $x = h_2 + \frac{m'_1 m'_2}{d'_1} t_2$.

3) Тепер підставляємо вираз для x в 3-тю конгруенцію системи (II.52), отримуємо: $h_2 + \frac{m'_1 m'_2}{d'_1} t_2 \equiv c_3 \pmod{m'_3}$. Розв'язком даної конгруенції (якщо вона має розв'язки) є: $t_2 \equiv \left(\frac{m'_1 m'_2}{d'_1 d'_2}\right)^{-1} \cdot \frac{c_3 - h_2}{d'_2} \pmod{\frac{m'_3}{d'_2}}$, звідки $t_1 = \left[(\left(\frac{m'_1 m'_2}{d'_1 d'_2}\right)^{-1} \cdot \frac{c_3 - h_2}{d'_2}) \mathrm{mod} \frac{m'_3}{d'_2} \right] + \frac{m'_3}{d'_2} t_3$. Тепер повертаємось до невідомого x:

$$x = h_2 + \frac{m'_1 m'_2}{d'_1} t_2 = h_2 + \frac{m'_1 m'_2}{d'_1} \left[(\left(\frac{m'_1 m'_2}{d'_1 d'_2}\right)^{-1} \cdot \frac{c_3 - h_2}{d'_2}) \mathrm{mod} \frac{m'_3}{d'_2} \right] + \frac{m'_1 m'_2 m'_3}{d'_1 d'_2} t_3.$$

Нехай $h_2 + \frac{m'_1 m'_2}{d'_1} \left[(\left(\frac{m'_1 m'_2}{d'_1 d'_2}\right)^{-1} \cdot \frac{c_3 - h_2}{d'_2}) \mathrm{mod} \frac{m'_3}{d'_2} \right] = h_3$. Тоді $x = h_3 + \frac{m'_1 m'_2 m'_3}{d'_1 d'_2} t_3$.

І т.д. до останньої конгруенції системи (II.52). Відповідно до даного алгоритму маємо процедуру:

```
syscongr := proc (A, B, M)
local k, i, d, h, m, q, C;
uses numtheory;
   k := nops(M);
   C := array(1 .. k);
   q := 1;
   for i to k do
      d := igcd(A[i], M[i]);
      if B[i] mod d = 0 then
         C[i] := ((A[i]/d)^(-1)*(B[i]/d)) mod M[i]/d
      else q := 0; break:
      end if;
   end do;
   if q = 1 then
      h := C[1]; m := M[1];
      for i from 2 to k do
         d := igcd(m, M[i]);
         if (C[i]-h) mod d = 0 then
            h := h+m*(((m/d)^(-1)*(C[i]-h)/d) mod M[i]/d);
            m := m*M[i]/d
         else q := 0; break
         end if
      end do;
      return(h mod m);
   else return NULL;
   end if;
end proc:
```

В результаті застосування даної процедури до системи (II.52) отримуємо представник класу лишків $K_h^{(m)}$, де m – найменше спільне кратне чисел $m_1, m_2, ..., m_s$. У випадку, коли система не має розв'язків, процедура нічого не виводить.

Розв'язання в Maple. Спосіб I. Розв'язуємо за допомогою розробленої процедури **syscongr**. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Задаємо списки коефіцієнтів $A = [2, 4, 5]$, $B = [31, 7, 18]$ і список модулів $M = [35, 25, 21]$.

```
> A := [2, 4, 5]: B := [31, 7, 18]: M := [35, 25, 21]:
```

і викликаємо процедуру **syscongr**:

```
> syscongr(A, B, M);
```

$$33$$

Отримали представник класу лишків за модулем m, що є найменшим спільним кратним чисел m_1, m_2, m_3:

```
> ilcm(35, 25, 21);
```

$$525$$

Отже, розв'язком заданої системи конгруенцій є клас лишків $K_{33}^{(525)}$.

Спосіб II. Спочатку розв'яжемо кожну із конгруенцій окремо за допомогою команди **msolve**:

```
> msolve(2*x=31,35);
```

$$\{x = 33\}$$

```
> msolve(4*x=7,25);
```

$$\{x = 8\}$$

```
> msolve(5*x=18,21);
```

$$\{x = 12\}$$

Отже, задана система рівносильна системі (II.51). Замінимо кожну із конгруенцій отриманої системи на рівносильну її за модулем $M = [35, 25, 21] = 525$ і знову застосуємо команду **msolve** у форматі **msolve(eqns,M)**, eqns – множина рівнянь (конгруенцій) системи:

```
> msolve({15*x=495,21*x=168,25*x=300},525);
```

$$\{x = 33\}$$

Таким чином, розв'язком заданої системи конгруенцій є клас $K_{33}^{(525)}$.

Завдання 16. Розв'язати систему конгруенцій:

16.1. а) $\begin{cases} x \equiv 1 \pmod 4, \\ 2x \equiv 11 \pmod 9, \\ 5x \equiv 2 \pmod 7; \end{cases}$ б) $\begin{cases} 4x \equiv 2 \pmod 6, \\ 3x \equiv 4 \pmod{10}, \\ 5x \equiv -1 \pmod{18}. \end{cases}$

16.2. а) $\begin{cases} 3x \equiv 5 \pmod 8, \\ 7x \equiv 2 \pmod 9, \\ 6x \equiv 1 \pmod 7; \end{cases}$ б) $\begin{cases} 2x \equiv 3 \pmod 9, \\ -5x \equiv 2 \pmod{18}, \\ 8x \equiv 3 \pmod{10}. \end{cases}$

16.3. а) $\begin{cases} 3x \equiv 2 \pmod{13}, \\ 7x \equiv 2 \pmod 9, \\ 6x \equiv 1 \pmod 7; \end{cases}$ б) $\begin{cases} 6x \equiv -1 \pmod{12}, \\ 2x \equiv 7 \pmod{10}, \\ 5x \equiv -1 \pmod 6. \end{cases}$

16.4. а) $\begin{cases} 2x \equiv 1 \pmod 9, \\ 5x \equiv 7 \pmod{17}, \\ 8x \equiv 1 \pmod{13}; \end{cases}$ б) $\begin{cases} 5x \equiv 2 \pmod 6, \\ 6x \equiv 7 \pmod{14}, \\ 3x \equiv 4 \pmod{11}. \end{cases}$

16.5. а) $\begin{cases} 7x \equiv 9 \pmod{11}, \\ 2x \equiv 11 \pmod{13}, \\ 5x \equiv 9 \pmod 9; \end{cases}$ б) $\begin{cases} 5x \equiv 7 \pmod 8, \\ 3x \equiv -5 \pmod{10}, \\ 7x \equiv 2 \pmod{12}. \end{cases}$

16.6. а) $\begin{cases} x \equiv 2 \pmod 3, \\ 5x \equiv 3 \pmod 7, \\ 6x \equiv -1 \pmod{11}; \end{cases}$ б) $\begin{cases} 3x \equiv 6 \pmod 9, \\ 21x \equiv 5 \pmod{12}, \\ 12x \equiv 9 \pmod{15}. \end{cases}$

16.7. а) $\begin{cases} 3x \equiv 5 \pmod{13}, \\ 2x \equiv 17 \pmod{21}, \\ 5x \equiv 31 \pmod{32}; \end{cases}$ б) $\begin{cases} 5x \equiv 4 \pmod{14}, \\ 6x \equiv 8 \pmod{16}, \\ 7x \equiv -3 \pmod{18}. \end{cases}$

16.8. а) $\begin{cases} 3x \equiv 5 \pmod{14}, \\ 5x \equiv 1 \pmod 9, \\ 7x \equiv 2 \pmod{25}; \end{cases}$ б) $\begin{cases} 3x \equiv 6 \pmod 8, \\ 7x \equiv 4 \pmod{12}, \\ -2x \equiv 14 \pmod{16}. \end{cases}$

16.9. а) $\begin{cases} 4x \equiv 1 \pmod{13}, \\ -3x \equiv 5 \pmod 9, \\ 2x \equiv 3 \pmod 7; \end{cases}$ б) $\begin{cases} 5x \equiv 7 \pmod 6, \\ 2x \equiv -3 \pmod 8, \\ -6x \equiv 12 \pmod{10}. \end{cases}$

16.10. а) $\begin{cases} 3x \equiv -5 \pmod{10}, \\ 6x \equiv 4 \pmod 7, \\ 10x \equiv 3 \pmod{11}; \end{cases}$ б) $\begin{cases} 5x \equiv 7 \pmod 8, \\ 2x \equiv 10 \pmod{12}, \\ -3x \equiv 5 \pmod{16}. \end{cases}$

16.11. а) $\begin{cases} 7x \equiv 4 \pmod{15}, \\ 3x \equiv -5 \pmod{28}, \\ 5x \equiv -3 \pmod{11}; \end{cases}$ б) $\begin{cases} 2x \equiv 3 \pmod{7}, \\ -5x \equiv 4 \pmod{10}, \\ 16x \equiv 4 \pmod{12}. \end{cases}$

16.12. а) $\begin{cases} 3x \equiv 8 \pmod{12}, \\ 4x \equiv 1 \pmod{17}, \\ 5x \equiv 2 \pmod{11}; \end{cases}$ б) $\begin{cases} 31x \equiv 5 \pmod{18}, \\ 5x \equiv 3 \pmod{21}, \\ 20x \equiv -6 \pmod{24}. \end{cases}$

16.13. а) $\begin{cases} 8x \equiv 1 \pmod{11}, \\ 7x \equiv -2 \pmod{13}, \\ 2x \equiv 11 \pmod{5}; \end{cases}$ б) $\begin{cases} 3x \equiv 5 \pmod{35}, \\ 4x \equiv 6 \pmod{18}, \\ 5x \equiv 7 \pmod{21}. \end{cases}$

16.14. а) $\begin{cases} 4x \equiv 5 \pmod{27}, \\ 3x \equiv 11 \pmod{13}, \\ 6x \equiv 9 \pmod{12}; \end{cases}$ б) $\begin{cases} 3x \equiv 7 \pmod{10}, \\ 5x \equiv -1 \pmod{14}, \\ 6x \equiv 14 \pmod{16}. \end{cases}$

16.15. а) $\begin{cases} 7x \equiv 2 \pmod{9}, \\ -6x \equiv 5 \pmod{17}, \\ 3x \equiv 19 \pmod{20}; \end{cases}$ б) $\begin{cases} 2x \equiv 3 \pmod{9}, \\ 5x \equiv -2 \pmod{14}, \\ 14x \equiv 10 \pmod{12}. \end{cases}$

16.16. а) $\begin{cases} 2x \equiv 3 \pmod{20}, \\ -4x \equiv 1 \pmod{9}, \\ 5x \equiv 2 \pmod{11}; \end{cases}$ б) $\begin{cases} 3x \equiv 7 \pmod{14}, \\ 5x \equiv 7 \pmod{28}, \\ 9x \equiv 6 \pmod{42}. \end{cases}$

16.17. а) $\begin{cases} 6x \equiv 10 \pmod{16}, \\ 4x \equiv 11 \pmod{7}, \\ -2x \equiv 3 \pmod{11}; \end{cases}$ б) $\begin{cases} 6x \equiv 1 \pmod{13}, \\ 9x \equiv 4 \pmod{14}, \\ 5x \equiv 3 \pmod{12}. \end{cases}$

16.18. а) $\begin{cases} 3x \equiv 2 \pmod{17}, \\ 3x \equiv 7 \pmod{25}, \\ 7x \equiv 5 \pmod{12}; \end{cases}$ б) $\begin{cases} 4x \equiv 6 \pmod{10}, \\ -7x \equiv 5 \pmod{9}, \\ 3x \equiv 4 \pmod{8}. \end{cases}$

16.19. а) $\begin{cases} 5x \equiv 32 \pmod{19}, \\ 7x \equiv -1 \pmod{10}, \\ 4x \equiv 13 \pmod{7}; \end{cases}$ б) $\begin{cases} 2x \equiv 7 \pmod{12}, \\ 3x \equiv 4 \pmod{15}, \\ 4x \equiv 10 \pmod{18}. \end{cases}$

16.20. а) $\begin{cases} 3x \equiv 1 \pmod{25}, \\ 6x \equiv 5 \pmod{33}, \\ 4x \equiv 3 \pmod{8}; \end{cases}$ б) $\begin{cases} 15x \equiv 18 \pmod{21}, \\ 7x \equiv 5 \pmod{24}, \\ 2x \equiv 1 \pmod{27}. \end{cases}$

16.21. а) $\begin{cases} 2x \equiv 7 \pmod{13}, \\ 5x \equiv 9 \pmod{14}, \\ -3x \equiv 8 \pmod{15}; \end{cases}$ б) $\begin{cases} 4x \equiv -3 \pmod{10}, \\ 27x \equiv 6 \pmod{12}, \\ 5x \equiv 2 \pmod{14}. \end{cases}$

16.22. а) $\begin{cases} 3x \equiv 12 \pmod{21}, \\ 5x \equiv 7 \pmod{31}, \\ -4x \equiv 13 \pmod{29}; \end{cases}$ б) $\begin{cases} 6x \equiv 13 \pmod{10}, \\ 7x \equiv 2 \pmod{15}, \\ -3x \equiv 16 \pmod{20}. \end{cases}$

16.23. а) $\begin{cases} 3x \equiv -7 \pmod{13}, \\ 4x \equiv 10 \pmod{12}, \\ 7x \equiv 2 \pmod{11}; \end{cases}$ б) $\begin{cases} 2x \equiv -1 \pmod{15}, \\ 4x \equiv 12 \pmod{20}, \\ 3x \equiv 7 \pmod{25}. \end{cases}$

16.24. а) $\begin{cases} 2x \equiv 3 \pmod{12}, \\ 6x \equiv 5 \pmod{7}, \\ -x \equiv 2 \pmod{5}; \end{cases}$ б) $\begin{cases} 5x \equiv 2 \pmod{6}, \\ 3x \equiv 1 \pmod{10}, \\ 2x \equiv 5 \pmod{9}. \end{cases}$

16.25. а) $\begin{cases} 5x \equiv 4 \pmod{7}, \\ 4x \equiv 5 \pmod{33}, \\ 6x \equiv 8 \pmod{17}; \end{cases}$ б) $\begin{cases} 5x \equiv 7 \pmod{12}, \\ 2x \equiv 11 \pmod{15}, \\ 4x \equiv 10 \pmod{18}. \end{cases}$

8. Конгруенції n-го степеня

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай задано конгруенцію виду

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \,(\mathrm{mod}\, p)\,, \qquad \text{(II.53)}$$

де p – просте, $n \in \mathbb{Z}$, $n \geqslant 2$, $a_i \in \mathbb{Z}$, $0 \leqslant i \leqslant n$, $a_n \not\equiv 0 \,(\mathrm{mod}\, p)$.

Рівносильними перетвореннями конгруенції (II.53), що спрощують її розв'язання, є:

1. Заміна коефіцієнтів $a_0, a_1, ..., a_n$ на конгруентні їм абсолютно найменші (або найменші невід'ємні) лишки за модулем p.

2. Пониження степеня конгруенції. При цьому:

а) якщо $a_0 \not\equiv 0 \,(\mathrm{mod}\, p)$, то замінюємо в конгруенції (II.53) доданки $a_k x^k$ на конгруентні їм $a_k x^r$, де r – остача від ділення числа k на $p-1$.

б) якщо $a_j \equiv 0 \,(\mathrm{mod}\, p)$ для всіх $j = 0, 1, ..., t$, де $0 \leqslant t < n$, $a_{t+1} \not\equiv 0 \,(\mathrm{mod}\, p)$, то конгруенція (II.53) еквівалентна сукупності конгруенцій

$$x \equiv 0 \,(\mathrm{mod}\, p) \quad \text{і}$$

$$\varphi(x) = a_n x^{n-t-1} + a_{n-1}x^{n-t-2} + \ldots + a_{t+2}x + a_{t+1} \equiv 0 \,(\mathrm{mod}\, p)\,,$$

де $a_{t+1} \not\equiv 0 \,(\mathrm{mod}\, p)$.

3. Перехід до еквівалентної конгруенції, старший коефіцієнт якої рівний 1. Для цього:
1) знаходимо ціле число y_0 таке, що $a_n y_0 \equiv 1 \pmod{p}$;
2) множимо обидві частини конгруенції (II.53) на y_0.

Теорема. *Конгруенція n-го степеня за простим модулем може мати не більше ніж n коренів.*

Конгруенція (II.53) називається тотожною, якщо всі її коефіцієнти конгруентні нулю за модулем m.

Наслідок. *Якщо конгруенція* (II.53) *має більш як n розв'язків, то вона є тотожною.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 17. Спростити конгруенцію (зменшити коефіцієнти за абсолютною величиною, понизити степінь, зробити старший коефіцієнт рівним 1) і розв'язати способом підбору:

а) $75x^{13} - 62x^{12} - 53x^{11} - 22x^6 + 13x - 27 \equiv 0 \pmod{7}$;

б) $13x^{17} + 2x^1 1 + 12x^7 - 32x^6 + 3x^5 - x + 4 \equiv 0 \pmod{7}$;

в) $24x^{23} - 138x^{14} + 64x^{11} - 94x^8 - x^6 - 76x^5 + 3x^2 \equiv 0 \pmod{7}$.

Розв'язання. а) Замінимо спочатку коефіцієнти заданої конгруенції на конгруентні їм абсолютно найменші лишки за модулем 7:

$$75 \equiv -2 \pmod{7}, \qquad -53 \equiv 3 \pmod{7}, \qquad 13 \equiv -1 \pmod{7},$$
$$-62 \equiv 1 \pmod{7}, \qquad -22 \equiv -1 \pmod{7}, \qquad -27 \equiv 1 \pmod{7}.$$

Тоді задана конгруенція рівносильна конгруенції

$$-2x^{13} + x^{12} + 3x^{11} - x^6 - x + 1 \equiv 0 \pmod{7}. \tag{II.54}$$

Тепер понизимо степінь одержаної конгруенції. Оскільки $x \equiv 0 \pmod{7}$ не є розв'язком конгруенції (II.54), то невідома x може приймати лише значення, взаємно прості із $m = 7$. Тому можемо записати, що $(x, 7) = 1$. Тоді за теоремою Ферма $x^6 \equiv 1 \pmod{7}$. В силу цього

$x^{13} = x^{6\cdot 2+1} = (x^6)^2 \cdot x \equiv x \pmod{7}$,
$x^{12} = x^{6\cdot 2} = (x^6)^2 \equiv 1 \pmod{7}$,
$x^{11} = x^{6\cdot 1+5} = x^6 \cdot x^5 \equiv x^5 \pmod{7}$.

Конгруенція (II.54), а значить, і задана конгруенція, рівносильна наступній конгруенції:

$$-2x + 1 + 3x^5 - 1 - x + 1 \equiv 0 \,(\mathrm{mod}\, 7)\,,$$

яку після зведення подібних доданків запишемо у вигляді:

$$3x^5 - 3x + 1 \equiv 0 \,(\mathrm{mod}\, 7)\,. \tag{II.55}$$

Замінимо тепер конгруенцію (II.55) на еквівалентну їй конгруенцію із старшим коефіцієнтом рівним 1. Для цього розв'яжемо допоміжну конгруенцію $3y \equiv 1 \,(\mathrm{mod}\, 7)$.

Легко бачити, що $y_0 = -2$ задовольняє цю конгруенцію. Домножимо обидві частини конгруенції (II.55) на -2: $-6x^5 + 6x - 2 \equiv 0 \,(\mathrm{mod}\, 7)$ або

$$g(x) = x^5 - x - 2 \equiv 0 \,(\mathrm{mod}\, 7)\,. \tag{II.56}$$

Розв'яжемо отриману конгруенцію способом підбору.

Для цього запишемо повну систему абсолютно найменших лишків за модулем 7: $0, 1, 2, 3, -3, -2, -1$. Оскільки $x \equiv 0 \,(\mathrm{mod}\, 7)$ не є розв'язком конгруенції (II.54), то перевіряємо тільки лишки $1, 2, 3, -3, -2, -1$. Маємо:

$$\begin{aligned}
g(1) &= 1^5 - 1 - 2 = -2 \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(2) &= 2^5 - 2 - 2 = 28 \equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(3) &= 3^5 - 3 - 2 = (3^2)^2 \cdot 3 - 3 - 2 \equiv 2^2 \cdot 3 - 3 - 2 \,(\mathrm{mod}\, 7) \equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(-3) &= (-3)^5 + 3 - 2 = ((-3)^2)^2 \cdot (-3) + 1 \equiv 2^2 \cdot (-3) + 1 \,(\mathrm{mod}\, 7) \equiv\\
&\quad \equiv 3 \,(\mathrm{mod}\, 7) \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(-2) &= (-2)^5 + 2 - 2 = -32 \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(-1) &= (-1)^5 + 1 - 2 = 0 \,(\mathrm{mod}\, 7) \not\equiv 0 \,(\mathrm{mod}\, 7)\,.
\end{aligned}$$

Таким чином, лишки 2 і 3 задовольняють конгруенцію (II.56), а значить, і задану конгруенцію. Отже, класи $K_2^{(7)}$ і $K_3^{(7)}$ є розв'язками заданої конгруенції.

б) Замінимо спочатку коефіцієнти заданої конгруенції на конгруентні їм абсолютно найменші лишки за модулем 7:

$$\begin{aligned}
13 &\equiv -1 \,(\mathrm{mod}\, 7)\,, \qquad & 12 &\equiv -2 \,(\mathrm{mod}\, 7)\,,\\
-32 &\equiv 3 \,(\mathrm{mod}\, 7)\,, & 4 &\equiv -3 \,(\mathrm{mod}\, 7)\,.
\end{aligned}$$

Тоді задана конгруенція рівносильна конгруенції

$$-x^{17} + 2x^{11} - 2x^7 + 3x^6 + 3x^5 - x - 3 \equiv 0 \,(\mathrm{mod}\, 7)\,. \tag{II.57}$$

Тепер понизимо степінь одержаної конгруенції. Оскільки $x \equiv 0 \pmod 7$ не є розв'язком конгруенції (II.57), то невідома x може приймати лише значення, взаємно прості із $m = 7$. Тому можемо записати, що $(x, 7) = 1$. Тоді за теоремою Ферма $x^6 \equiv 1 \pmod 7$. В силу цього

$x^{17} = x^{6\cdot 2+5} = (x^6)^2 \cdot x^5 \equiv x^5 \pmod 7$,
$x^{11} = x^{6\cdot 1+5} = x^6 \cdot x^5 \equiv x^5 \pmod 7$,
$x^7 = x^6 x \equiv x \pmod 7$.

Конгруенція (II.57), а значить, і задана конгруенція, рівносильна наступній конгруенції:

$$-x^5 + 2x^5 - 2x + 3 + 3x^5 - x - 3 \equiv 0 \pmod 7,$$

яку після зведення подібних доданків запишемо у вигляді:

$$4x^5 - 3x \equiv 0 \pmod 7. \tag{II.58}$$

Замінимо тепер конгруенцію (II.58) на еквівалентну їй конгруенцію із старшим коефіцієнтом рівним 1. Для цього розв'яжемо допоміжну конгруенцію $4y \equiv 1 \pmod 7$.

Легко бачити, що $y_0 = 2$ задовольняє цю конгруенцію. Домножимо обидві частини конгруенції (II.58) на 2:

$$x^5 + x \equiv 0 \pmod 7$$

або

$$g(x) = x^5 + x \equiv 0 \pmod 7. \tag{II.59}$$

Розв'яжемо отриману конгруенцію способом підбору.

Для цього запишемо повну систему абсолютно найменших лишків за модулем 7: $0, 1, 2, 3, -3, -2, -1$. Оскільки $x \equiv 0 \pmod 7$ не є розв'язком конгруенції (II.57), то перевіряємо тільки лишки $1, 2, 3, -3, -2, -1$. Маємо:

$$\begin{aligned}
g(1) &= 1^5 + 1 = 2 \not\equiv 0 \pmod 7,\\
g(2) &= 2^5 + 2 = 34 \not\equiv 0 \pmod 7,\\
g(3) &= 3^5 + 3 = 3^3 \cdot 3^2 + 3 \equiv (-1) \cdot 2 + 3 \pmod 7 \equiv 1 \pmod 7 \not\equiv 0 \pmod 7,\\
g(-3) &= (-3)^5 - 3 = (-3)^3 \cdot (-3)^2 - 3 \equiv 1 \cdot (-2) - 3 \pmod 7 \equiv\\
&\equiv -5 \pmod 7 \not\equiv 0 \pmod 7,\\
g(-2) &= (-2)^5 - 2 = -32 \not\equiv 0 \pmod 7,\\
g(-1) &= (-1)^5 - 1 = -2 \pmod 7 \not\equiv 0 \pmod 7.
\end{aligned}$$

Таким чином, жоден із лишків не задовольняє конгруенцію (II.59), а значить, і задану конгруенцію. Отже, задана конгруенція розв'язків не має.

в) Заміняємо коефіцієнти заданої конгруенції на конгруентні їм абсолютно найменші лишки за модулем 7:

$$24 \equiv 3 \,(\mathrm{mod}\, 7)\,, \qquad -138 \equiv 2 \,(\mathrm{mod}\, 7)\,, \qquad 64 \equiv 1 \,(\mathrm{mod}\, 7)\,,$$
$$-94 \equiv -3 \,(\mathrm{mod}\, 7)\,, \qquad -76 \equiv 1 \,(\mathrm{mod}\, 7)\,, \qquad -4 \equiv 3 \,(\mathrm{mod}\, 7)\,.$$

Тоді задана конгруенція рівносильна конгруенції

$$3x^{23} + 2x^{14} + x^{11} - 3x^8 - x^6 + x^5 + 3x^2 \equiv 0 \,(\mathrm{mod}\, 7)\,. \tag{II.60}$$

Оскільки $x \equiv 0 \,(\mathrm{mod}\, 7)$ є розв'язком конгруенції (II.60), то використати теорему Ферма для пониження степеня одержаної конгруенції на даному етапі не можна (не для всіх розв'язків $K_{x_0}^{(7)}$ справедливо, що $(x_0, 7) = 1$). Від розгляду даної конгруенції перейдемо до розгляду рівносильної їй сукупності конгруенцій $x \equiv 0 \,(\mathrm{mod}\, 7)$ і

$$3x^{21} + 2x^{12} + x^9 - 3x^6 - x^4 + x^3 + 3 \equiv 0 \,(\mathrm{mod}\, 7)\,. \tag{II.61}$$

Клас $K_0^{(7)}$ є розв'язком першої із конгруенцій і не є розв'язком другої, тому конгруенцію (II.61) можна спростити, понизивши степінь за допомогою теореми Ферма: $x^6 \equiv 1 \,(\mathrm{mod}\, 7)$. В силу цього
$x^{21} = x^{6\cdot 3+3} = (x^6)^3 \cdot x^3 \equiv x^3 \,(\mathrm{mod}\, 7)$,
$x^{12} = x^{6\cdot 2} = (x^6)^2 \equiv 1 \,(\mathrm{mod}\, 7)$,
$x^9 = x^6 x^3 \equiv x^3 \,(\mathrm{mod}\, 7)$.
Конгруенція (II.61) рівносильна наступній конгруенції:

$$3x^3 + 2 + x^3 - 3 - x^4 + x^3 + 3 \equiv 0 \,(\mathrm{mod}\, 7)\,,$$

яку після зведення подібних доданків запишемо у вигляді:

$$-x^4 + 5x^3 + 2 \equiv 0 \,(\mathrm{mod}\, 7)\,. \tag{II.62}$$

Замінимо тепер конгруенцію (II.62) на еквівалентну їй конгруенцію із старшим коефіцієнтом рівним 1:

$$x^4 - 5x^3 - 2 \equiv 0 \,(\mathrm{mod}\, 7) \tag{II.63}$$

Розв'яжемо її способом підбору.

Для цього запишемо повну систему абсолютно найменших лишків за модулем 7: $0, 1, 2, 3, -3, -2, -1$. Оскільки $x \equiv 0 \,(\mathrm{mod}\, 7)$ не є розв'язком

конгруенції (II.61), то перевіряємо тільки лишки $1, 2, 3, -3, -2, -1$. Маємо:

$$\begin{aligned}
g(1) &= 1^4 - 5 - 2 = -6 \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(2) &= 2^4 - 5 \cdot 2^3 - 2 \equiv 6 \,(\mathrm{mod}\, 7) \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(3) &= 3^4 - 5 \cdot 3^3 - 2 \equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(-3) &= (-3)^4 - 5 \cdot (-3)^3 - 2 \equiv 6 \,(\mathrm{mod}\, 7) \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(-2) &= (-2)^4 - 5 \cdot (-2)^3 - 2 \equiv 1 \,(\mathrm{mod}\, 7) \not\equiv 0 \,(\mathrm{mod}\, 7)\,,\\
g(-1) &= (-1)^4 - 5 \cdot (-1)^3 - 2 \equiv 3 \,(\mathrm{mod}\, 7) \not\equiv 0 \,(\mathrm{mod}\, 7)\,.
\end{aligned}$$

Таким чином, лишок 3 задовольняє конгруенцію (II.63), а значить, і конгруенцію (II.61). Отже, розв'язками заданої конгруенції є класи $K_0^{(7)}$ і $K_3^{(7)}$.

Розробка процедур. Перевірку лише остаточного результату можна здійснити за допомогою команди msolve (див. §7).

Для перевірки проміжних результатів створимо процедуру **congVS**, яка буде поетапно виконувати такі рівносильні перетворення конгруенції як:

1) заміна коефіцієнтів $a_0, a_1, ..., a_n$ на конгруентні їм абсолютно найменші лишки за модулем p;

```
> f1:=mods(f,p);
```

2) пониження степеня конгруенції шляхом ділення отриманого в п.1) многочлена f1 на $x^{p-1} - 1$

```
> f2:=rem(f1,x^(p-1)-1,x));
```

3) перехід до еквівалентної конгруенції $g(x) \equiv 0 \pmod{p}$, старший коефіцієнт якої рівний 1

```
> y0:=a^(-1) mod p; g:=mods(f2*y0,p);
```

Зауважимо, що перед тим, як понижувати степінь конгруенції, необхідно перевірити, чи є розв'язком клас $K_0^{(p)}$. Якщо так, число 0 виводимо на екран, а потім многочлен f1 ділимо на x доти, доки це можливо:

```
> if subs({x=0},f1) mod p =0 then print(0);
  while subs({x=0},f1) mod p=0 do f1:=quo(f1,x,x); end do:
```

Подальше розв'язування способом підбору здійснюємо наступним чином: для всіх $i \in \overline{0, p-1}$ перевіряємо, чи є клас $K_i^{(p)}$ розв'язком:

```
> for i from 0 to p-1 do
     if subs({x=i},g) mod p=0 then print(i); end if;
  end do;
```

Процедура congVS виглядатиме наступним чином:

```
congVS:=proc(f,p::integer)
local f1,f2,g,i,n,a,y0:
   f1:=mods(f,p);
   print(f1);
   if subs({x=0},f1) mod p =0 then print(0);
      while subs({x=0},f1) mod p=0 do f1:=quo(f1,x,x);
      end do:
   end if;
   f2:=rem(f1,x^(p-1)-1,x); print(f2);
   n:=degree(f2,x);
   a:=coeff(f2,x,n);
   y0:=a^(-1) mod p;
   g:=mods(f2*y0,p); print(g);
   for i from 0 to p-1 do
      if subs({x=i},g) mod p=0 then print(i); end if;
   end do;
end proc:
```

Для опису процедури було використано команди:
mods(f,m) – заміна коефіцієнтів многочлена $f(x)$ на абсолютно найменші за модулем m лишки;
quo(f,g,x) і **rem(f,g,x)** – пошук неповної частки (відповідно остачі) від ділення многочлена $f(x)$ на многочлен $g(x)$ з остачею;
degree(f,x) – степінь многочлена $f(x)$;
coeff(f,x,n) – коефіцієнт многочлена $f(x)$ при x^n
(детальніше про ці команди див. в розд.IV).

В результаті на екран буде виведено проміжні перетворення:

$$\mathbf{f}1$$
$$\mathbf{f}2$$
$$\mathbf{g}$$

В наступних рядках виводяться розв'язки конгруенції. Якщо конгруенція розв'язків не має, то ці рядки залишаються порожніми.

Розв'язання в Maple. Остаточний результат перевіряємо за допомогою команди **msolve(f,p)**, де $f(x) \equiv 0 \pmod p$ – задана конгруенція. Матимемо:

```
> msolve(75*x^13-62*x^12-53*x^11-22*x^6+13*x-27,7);
```

$$\{x = 2\},\ \{x = 3\}$$

Розв'язками заданої конгруенції є класи: $K_2^{(7)}$ і $K_3^{(7)}$.

Для перевірки проміжних перетворень використаємо процедуру **congVS** із бібліотеки atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Задаємо многочлен f:

```
> f:=75*x^13-62*x^12-53*x^11-22*x^6+13*x-27:
```

і застосовуємо процедуру **congVS**:

```
> congVS(f,7);
```

$$-2\,x^{13}+x^{12}+3\,x^{11}-x^6-x+1$$
$$1-3\,x+3\,x^5$$
$$-2-x+x^5$$
$$2$$
$$3$$

Отже, після заміни коефіцієнтів на конгруентні їм абсолютно найменші за модулем отримуємо конгруенцію $-2x^{13}+x^{12}+3x^{11}-x^6-x+1\equiv 0 \pmod 7$. Пониження степеня дасть конгруенцію $3x^5-3x+1\equiv 0 \pmod 7$. Конгруенцією, в якої старший коефіцієнт дорівнює 1, є конгруенція $x^5-x-2\equiv 0 \pmod 7$. Розв'язками конгруенції є класи $K_2^{(7)}$ і $K_3^{(7)}$.

```
> f:=13*x^17+2*x^11+12*x^7-32*x^6+3*x^5-x+4:
  congVS(f,7);
```

$$-x^{17}+2\,x^{11}-2\,x^7+3\,x^6+3\,x^5-x-3$$
$$4\,x^5-3\,x$$
$$x^5+x$$

Конгруенція розв'язків не має.

```
> f:=24*x^23-138*x^14+64*x^11-94*x^8-x^6-76*x^5+3*x^2:
  congVS(f,7);
```

$$3\,x^{23}+2\,x^{14}+x^{11}-3\,x^8-x^6+x^5+3\,x^2$$
$$0$$
$$2-x^4+5\,x^3$$
$$-2+x^4+2\,x^3$$
$$3$$

Розв'язками конгруенції є класи $K_0^{(7)}$ і $K_3^{(7)}$.

Завдання 17. Спростити конгруенцію (зменшити коефіцієнти за абсолютною величиною, понизити степінь, зробити старший коефіцієнт рівним 1) і розв'язати способом підбору.

17.1. $13x^{17}+2x^{11}+12x^7-32x^6+3x^5-x+4\equiv 0 \pmod 7$.

17.2. $47x^{54}-20x^{34}-21x^{32}+32x^{24}-13x^{12}+10x^{10}+40x^2+2\equiv 0 \pmod{11}$.

17.3. $245x^{201} + 51x^{64} + 3x^{47} + 28x^{19} + 7x^8 - 10x^6 - 33x^4 + 2 \equiv 0 \pmod 5$.

17.4. $10x^{29} + 5x^{14} + 8x^{11} + x^8 + x^6 - 8x^5 - 3x^2 + 10 \equiv 0 \pmod 7$.

17.5. $79x^{62} + 107x^{49} - 93x^{37} - x^{25} + 131x^{24} - 18x^{13} + 15x^{12} - 30 \equiv 0 \pmod{13}$.

17.6. $35x^{93} + 121x^{85} + 42x^{53} - 25x^{43} + 24x^{13} + 90x^{11} + x^{10} - 100x + 42 \equiv 0 \pmod{11}$.

17.7. $15x^{27} + 43x^{25} - 6x^{21} - 24x^{14} + 69x^9 + 71x^7 - 4x^6 + 8x^2 + 5 \equiv 0 \pmod 7$.

17.8. $29x^{86} + 38x^{62} + 14x^{38} + 7x^{37} + 81x^{25} - 18x^{24} - 8x^{13} + 23 \equiv 0 \pmod{13}$.

17.9. $68x^{19} + 121x^{17} + 85x^{11} - 75x^7 + 4x^6 - 126x^5 - 4x - 3 \equiv 0 \pmod 7$.

17.10. $156x^{91} - 6x^{74} - 157x^{49} - 29x^{45} + x^{32} + 114x^{21} + 23x^{15} + 42x^{12} + 31 \equiv 0 \pmod 7$.

17.11. $43x^{410} + 25x^{28} + 39x^{20} + 3x^{11} - 17x^8 + 11x^7 - 22 \equiv 0 \pmod 5$.

17.12. $24x^{23} - 138x^{14} + 64x^{11} - 94x^8 - x^6 - 76x^5 + 3x^2 - 4 \equiv 0 \pmod 7$.

17.13. $36x^{54} - 4x^{42} + 120x^{34} - 54x^{32} + 119x^{10} + 49x^4 - 5x^2 + 82 \equiv 0 \pmod{11}$.

17.14. $41x^{98} + 81x^{50} - 137x^{37} + 120x^{36} + 62x^{25} + 14x^{12} + 24 \equiv 0 \pmod{13}$.

17.15. $71x^{33} - 68x^{15} + x^{13} + 58x^9 + 37x^8 - 115x^6 + 24x^2 - 7 \equiv 0 \pmod 7$.

17.16. $53x^{63} + 76x^{51} + 29x^{40} - 3x^{31} - 72x^{23} + 78x^{10} + 6 \equiv 0 \pmod{11}$.

17.17. $33x^{133} + 32x^{85} + 8x^{72} + 40x^{62} + 27x^{38} - 55x^{13} + 14x^{12} - 19 \equiv 0 \pmod{13}$.

17.18. $86x^{13} + 97x^{11} - 84x^7 - 12x^6 - x^5 + 87x + 2 \equiv 0 \pmod 7$.

17.19. $10x^{2002} + 36x^{74} + 29x^{44} - 27x^{32} + 51x^{20} - 114x^{12} + 35 \equiv 0 \pmod{11}$.

17.20. $78x^{93} + 111x^{62} - 134x^{49} - 15x^{36} + 126x^{14} - 101x^{13} + x^{12} + 5 \equiv 0 \pmod{13}$.

17.21. $213x^{29} + 64x^{24} - 64x^{11} + x^8 + 85x^6 - 96x^5 + 143x^2 + 1 \equiv 0 \pmod 7$.

17.22. $100x^{173} - 80x^{91} - 29x^{23} - 101x^{21} + 48x^{10} + 45 \equiv 0 \pmod{11}$.

17.23. $59x^{48} + 22x^{43} - 2x^{12} + 23x^{11} - 27x^8 + 53x^7 - 101x^4 - 3 \equiv 0 \pmod 5$.

17.24. $113x^{157} + 29x^{134} + 2x^{97} + 21x^{86} - 3x^{50} + 31x^{25} - 31x^{24} + 16x^{12} - 4 \equiv 0 \pmod{13}$.

17.25. $21x^{145} + 15x^{39} + 23x^9 + 5x^8 + 36x^7 + x^6 - 11x^3 + 26x^2 - 18x - 6 \equiv 0 \pmod 7$.

9. Квадратні конгруенції

ТЕОРЕТИЧНІ ВІДОМОСТІ

Конгруенцію 2-го степеня $c_2x^2 + c_1x + c_0 \equiv 0 \pmod p$ за простим модулем $p > 2$, де $c_2 \not\equiv 0 \pmod p$, завжди можна звести до двочленної конгруенції виду

$$y^2 \equiv a \pmod p. \tag{II.64}$$

Для цього слід:

1) домножити обидві частини конгруенції на число b таке, що $bc_2 \equiv 1 \pmod p$;

2) якщо коефіцієнт при x отриманої конгруенції – число непарне, то додати до лівої частини конгруенції многочлен px;

3) виділити повний квадрат.

Якщо конгруенція (II.64) має хоча б один розв'язок, то a називається квадратичним лишком за модулем p, в іншому випадку a називають квадратичним нелишком за модулем p.

Нехай $(a, p) = 1$. Якщо a – квадратичний лишок за модулем p, то конгруенція (II.64) має 2 розв'язки.

При простому непарному p число a є квадратичним лишком за модулем p тоді і лише тоді, коли $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, і квадратичним нелишком за модулем p тоді і лише тоді, коли $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ (критерій Ойлера).

Для ефективного використання критерію Ойлера вводиться так званий символ Лежандра $\left(\frac{a}{p}\right)$ (читається: „символ Лежандра a відносно p"). Символ Лежандра визначається для всіх цілих чисел a таких, що $(a, p) = 1$, рівністю

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо } a \text{ є квадратичним лишком за модулем } p; \\ -1, & \text{якщо } a \text{ є квадратичним нелишком за модулем } p. \end{cases}$$

Критерій Ойлера тоді коротко записується так: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

Основні властивості символу Лежандра:

1°. Якщо $a_1 \equiv a \pmod p$, то $\left(\frac{a_1}{p}\right) = \left(\frac{a}{p}\right)$;

2°. $\left(\frac{a^2}{p}\right) = 1$;

3°. $\left(\frac{1}{p}\right) = 1$;

4°. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

5°. $\left(\frac{a_1a_2\ldots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\ldots\left(\frac{a_n}{p}\right)$;

6°. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

7°. $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$;

8°. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

9°. Якщо p і q – різні непарні прості числа, то $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ (закон взаємності квадратичних лишків).

ПРИКЛАДИ І ЗАДАЧІ

Приклад 18. Визначити, чи має розв'язки конгруенція $x^2 \equiv 47 \pmod{73}$.

Розв'язання. Спосіб I. Використаємо критерій Ойлера. За умовою, $a = 47$, $p = 73$. Маємо:

$$47^{\frac{73-1}{2}} = 47^{36} \equiv 2209^{18} \pmod{73} \equiv 19^{18} \pmod{73} \equiv$$
$$\equiv 361^{9} \pmod{73} \equiv (-4)^{9} \pmod{73} \equiv -1 \pmod{73}.$$

В силу критерію Ойлера, задана конгруенція розв'язків не має.

Спосіб II. Використаємо символ Лежандра. За законом взаємності квадратичних лишків, маємо:

$$\left(\frac{47}{73}\right) = \left(\frac{73}{47}\right) \cdot (-1)^{\frac{47-1}{2}\cdot\frac{73-1}{2}} = \left(\frac{73}{47}\right) \cdot (-1)^{23\cdot 36} = \left(\frac{73}{47}\right).$$

Далі $73 \equiv 26 \pmod{47}$, тому, за властивістю 1°, $\left(\frac{73}{47}\right) = \left(\frac{26}{47}\right)$. Тепер, за властивістю 5°, $\left(\frac{26}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{13}{47}\right)$. Обчислимо окремо кожний із даних символів.

В силу властивості 8°, $\left(\frac{2}{47}\right) = (-1)^{\frac{47^2-1}{8}} = 1$; за законом взаємності квадратичних лишків, $\left(\frac{13}{47}\right) = \left(\frac{47}{13}\right) \cdot (-1)^{\frac{47-1}{2}\cdot\frac{13-1}{2}} = \left(\frac{47}{13}\right) \cdot (-1)^{23\cdot 6} = \left(\frac{47}{13}\right)$. Тепер за властивістю 1° $\left(\frac{47}{13}\right) = \left(\frac{8}{13}\right)$. Залишається застосувати властивість 6° і властивість 8°: $\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = -1$. Таким чином, $\left(\frac{47}{73}\right) = \left(\frac{2}{47}\right)\left(\frac{13}{47}\right) = 1 \cdot (-1) = -1$.

Отже, число 47 є квадратичним нелишком за модулем 73, а значить, задана конгруенція розв'язків не має.

Розв'язання в Maple. Для обчислення символу Лежандра $\left(\frac{a}{p}\right)$ використовується команда **legendre(a,p)** із пакету numtheory:

```
> with(numtheory):
  legendre(47,73);
```

$$-1$$

Отже, $\left(\frac{47}{73}\right) = -1$ і задана конгруенція розв'язків не має.

Завдання 18. Визначити, чи має розв'язки конгруенція:

18.1. $x^2 \equiv 33 \pmod{43}$.

18.2. $x^2 \equiv 14 \pmod{59}$.

18.3. $x^2 \equiv 12 \pmod{37}$.

18.4. $x^2 \equiv 6 \pmod{47}$.

18.5. $x^2 \equiv 13 \pmod{83}$.

18.6. $x^2 \equiv 5 \pmod{71}$.

18.7. $x^2 \equiv 20 \pmod{43}$.

18.8. $x^2 \equiv 53 \pmod{73}$.

18.9. $x^2 \equiv 28 \pmod{67}$.

18.10. $x^2 \equiv 40 \pmod{101}$.

18.11. $x^2 \equiv 17 \pmod{23}$.

18.12. $x^2 \equiv 26 \pmod{31}$.

18.13. $x^2 \equiv 35 \pmod{43}$.

18.14. $x^2 \equiv 18 \pmod{47}$.

18.15. $x^2 \equiv 23 \pmod{59}$.

18.16. $x^2 \equiv 6 \pmod{89}$.

18.17. $x^2 \equiv 24 \pmod{41}$.

18.18. $x^2 \equiv 12 \pmod{37}$.

18.19. $x^2 \equiv 32 \pmod{53}$.

18.20. $x^2 \equiv 42 \pmod{71}$.

18.21. $x^2 \equiv 10 \pmod{97}$.

18.22. $x^2 \equiv 28 \pmod{37}$.

18.23. $x^2 \equiv 15 \pmod{67}$.

18.24. $x^2 \equiv 8 \pmod{31}$.

18.25. $x^2 \equiv 27 \pmod{47}$.

10. Порядок числа за модулем. Індекси

ТЕОРЕТИЧНІ ВІДОМОСТІ

Порядком числа a за модулем m називається найменше натуральне число k, для якого виконується умова $a^k \equiv 1 \pmod{m}$ (позначається символом $P_m(a)$).

Властивості:

1°. якщо $a \equiv b \pmod{m}$, то $P_m(a) = P_m(b)$;
2°. якщо $a \in K_b^{(m)}$, то $P_m(a) = P_m(b)$;
3°. якщо $P_m(a) = k$, то числа $1, a, a^2, ..., a^{k-1}$ попарно не конгруентні за модулем m;
4°. якщо $P_m(a) = k$, то умова $a^\alpha \equiv a^\beta \pmod{m}$ справедлива тоді і лише тоді, коли $\alpha \equiv \beta \pmod{k}$;
5°. якщо $P_m(a) = k$ і $a^n \equiv 1 \pmod{m}$, то $n \vdots k$;
6°. якщо $P_m(a) = k$, то $\varphi(m) \vdots k$.

Число a називають первісним коренем за модулем m, якщо $P_m(a) = \varphi(m)$. Якщо a – первісний корінь за модулем m, то числа $1, a, a^2, ..., a^{k-1}$ утворюють ЗСЛ(m). Якщо існує хоча б одне число a таке, що $P_p(a) = k$, де p – просте, то всього таких чисел є $\varphi(k)$.

Якщо число a має порядок k за модулем p, то число a^i ($i \in \overline{0, k-1}$) має порядок k тоді і лише тоді, коли $(i, k) = 1$. Існує точно $\varphi(k)$ класів чисел, що мають порядок k за простим модулем p. Зокрема, існує точно $\varphi(p-1)$ первісних коренів за цим модулем (теорема Гауса)

Первісні корені існують тільки за модулями $m = 2, 4, p^\alpha$ і $2p^\alpha$, де p – непарне просте число, $\alpha \in \mathbb{N}$.

Нехай $(a, m) = 1$, $(b, m) = 1$. Число s називається індексом числа b за основою a і модулем m, якщо $a^s \equiv b \pmod{m}$ (позначають $\operatorname{ind}_a b$). Якщо g – первісний корінь за модулем m, то індекси за основою g існують для всіх чисел, взаємно простих із m.

Нехай g – первісний корінь за модулем m, $(a,m)=(b,m)=1$.

Властивості індексів:

1♯. якщо γ і γ' – індекси числа a за основою g і модулем m, то $\gamma \equiv \gamma' \big(\mathrm{mod}\,\varphi(m)\big)$;
2♯. конгруенція $a \equiv b \,(\mathrm{mod}\, m)$ має місце тоді і лише тоді, коли $\mathrm{ind}_g a \equiv \mathrm{ind}_g b \big(\mathrm{mod}\,\varphi(m)\big)$;
3♯. $\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;
4♯. $\mathrm{ind}_g g \equiv 1 \pmod{\varphi(m)}$;
5♯. $\mathrm{ind}_g(ab) \equiv \mathrm{ind}_g a + \mathrm{ind}_g b \big(\mathrm{mod}\,\varphi(m)\big)$
6♯. $\mathrm{ind}_g a^n \equiv n\,\mathrm{ind}_g a \big(\mathrm{mod}\,\varphi(m)\big)$.
7♯. якщо $a \vdots b$, то $\mathrm{ind}_g \frac{a}{b} \equiv \mathrm{ind}_g a - \mathrm{ind}_g b \big(\mathrm{mod}\,\varphi(m)\big)$.

Перехід від конгруенції між числами до конгруенції їхніх індексів називається індексацією, а навпаки – потенціюванням.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 19.1. Розв'язати конгруенцію $11 \cdot 5^{3x} + 27 \equiv 0 \pmod{29}$.

Розв'язання. Розв'язком показникової конгруенції $a^x \equiv b \pmod{m}$ називають множину всіх цілих значень x, що задовольняють дану конгруенцію. Нехай x_0 – один із розв'язків заданої конгруенції. Тоді $11 \cdot 5^{3x_0} + 27 \equiv 0 \pmod{29}$. За властивостями числових конгруенцій матимемо: $11 \cdot 5^{3x_0} \equiv 176 \pmod{29}$, звідки $5^{3x_0} \equiv 16 \pmod{29}$. Беремо індекси від обох частин конгруенції: $3x_0 \cdot \mathrm{ind}\,5 \equiv \mathrm{ind}\,16 \pmod{28}$. За таблицею індексів для числа $p = 29$ маємо: $\mathrm{ind}\,5 = 22$, $\mathrm{ind}\,16 = 4$, тоді $3x_0 \cdot 22 \equiv 4 \pmod{28}$, звідки $10x_0 \equiv 4 \pmod{28}$. Розділимо обидві частини конгруенції і модуль на 2: $5x_0 \equiv 2 \pmod{14}$. тоді $5x_0 \equiv 30 \pmod{14}$, звідки $x_0 \equiv 6 \pmod{14}$. Отже, розв'язком заданої конгруенції є кожне ціле число x_0 таке, що $x_0 = 6 + 14t$, де $t \in \mathbb{Z}$.

Розв'язання в Maple. Використовуємо команду **msolve** (див. §14). Маємо:

```
> msolve(11*5^(3*x)+27=0,29);
```

$$\{x = 6 + 14\,\_Z2\}$$

Приклад 19.2. Розв'язати конгруенцію $40x^{10} \equiv 3 \pmod{17}$.

Розв'язання. Дана конгруенція рівносильна конгруенції $6x^{10} \equiv 3 \pmod{17}$. Візьмемо індекси від обох частин конгруенції: $\mathrm{ind}\,6x^{10} \equiv \mathrm{ind}\,3 \pmod{16}$. За властивостями $5^\sharp$ і $6^{\cdot\sharp}$, $\mathrm{ind}\,6 + 10\,\mathrm{ind}\,x \equiv \mathrm{ind}\,3 \pmod{16}$. За таблицею індексів для числа 17 знаходимо $\mathrm{ind}\,6 = 15$, $\mathrm{ind}\,3 = 1$, тоді отримуємо: $15 + 10\,\mathrm{ind}\,x \equiv 1 \pmod{16}$, звідки $10\,\mathrm{ind}\,x \equiv -14 \pmod{16}$.

Отримали конгруенцію 1-го степеня відносно x. Розв'яжемо її. Оскільки $(10, 16) = 1$ і $-14 \vdots 2$, то конгруенція має 2 розв'язки. Розділимо обидві частини і модуль на 2: $5 \operatorname{ind} x \equiv -7 \pmod 8$, тоді $5 \operatorname{ind} x \equiv -15 \pmod 8$, звідки $\operatorname{ind} x \equiv -3 \pmod 8$, тобто $\operatorname{ind} x \equiv 5 \pmod 8$. Одержана конгруенція рівносильна сукупності конгруенцій за модулем 16: $\operatorname{ind} x \equiv 5 \pmod{16}$ і $\operatorname{ind} x \equiv 13 \pmod{16}$.

Тепер за таблицею антиіндексів знаходимо x: $x \equiv 5 \pmod{17}$, $x \equiv 12 \pmod{17}$. Отже, розв'язками заданої конгруенції є: $K_5^{(17)}$ і $K_{12}^{(17)}$.

Розв'язання в Maple. Застосовуємо команду **msolve**:

```
> msolve(40*x^(10)=3,17);
```

$$\{x = 5\},\ \{x = 12\}$$

Завдання 19. Розв'язати конгруенції:

19.1. а) $8^x \equiv 5 \pmod{11}$, б) $25x^7 \equiv -7 \pmod{31}$.

19.2. а) $5^x \equiv -1 \pmod{23}$, б) $x^{12} + 8 \equiv 0 \pmod{73}$.

19.3. а) $2 \cdot 3^x + 12 \equiv 0 \pmod{37}$, б) $5x^{11} + 19 \equiv 0 \pmod{29}$.

19.4. а) $3 \cdot 27^x + 4 \equiv 12 \pmod{31}$, б) $x^2 \equiv 15 \pmod{17}$.

19.5. а) $4^x + 3 \equiv -15 \pmod{19}$, б) $3x^8 \equiv 5 \pmod{13}$.

19.6. а) $23^x \equiv 37 \pmod{31}$, б) $x^2 \equiv 47 \pmod{53}$.

19.7. а) $2^{5x} + 1 \equiv 5 \pmod{23}$, б) $x^7 + 27 \equiv 0 \pmod{53}$.

19.8. а) $2 \cdot 4^{3x} - 1 \equiv 0 \pmod{29}$, б) $8x^9 \equiv -17 \pmod{41}$.

19.9. а) $7 \cdot 5^x \equiv -1 \pmod{73}$, б) $x^{15} \equiv 38 \pmod{59}$.

19.10. а) $25^x \equiv -7 \pmod{41}$, б) $x^2 \equiv 40 \pmod{83}$.

19.11. а) $2 \cdot 3^{2x+3} \equiv 1 \pmod{17}$, б) $x^{17} \equiv 13 \pmod{67}$.

19.12. а) $16^x \equiv 11 \pmod{13}$, б) $x^{11} + 36 \equiv 0 \pmod{71}$.

19.13. а) $10^{3x} \equiv 2 \pmod{19}$, б) $15x^9 + 29 \equiv 0 \pmod{47}$.

19.14. а) $27^x + 4 \equiv 0 \pmod{13}$, б) $x^5 + 13 \equiv 0 \pmod{61}$.

19.15. а) $32^x \equiv 15 \pmod{37}$, б) $7x^{13} + 23 \equiv 0 \pmod{47}$.

19.16. а) $17 \cdot 13^{3x} + 27 \equiv 0 \pmod{29}$, б) $2x^7 \equiv -2 \pmod{19}$.

19.17. а) $4 \cdot 5^{5x} + 2 \equiv 0 \pmod{17}$, б) $x^2 \equiv 54 \pmod{71}$.

19.18. а) $19^{7x} \equiv 15 \pmod{59}$, б) $17x^3 + 3 \equiv 0 \pmod{37}$.

19.19. а) $3 \cdot 11^{2x} \equiv -7 \pmod{23}$, б) $6x^7 + 19 \equiv 0 \pmod{23}$.

19.20. а) $-2 \cdot 3^{2x} + 13 \equiv 5 \pmod{19}$, б) $x^2 \equiv 37 \pmod{41}$.

19.21. а) $4 \cdot 3^{-x} + 1 \equiv 0 \pmod{13}$, б) $9x^{11} + 1 \equiv 0 \pmod{43}$.

19.22. а) $25^{5x} \equiv 47 \pmod{61}$, б) $13x^8 + 36 \equiv 0 \pmod{61}$.

19.23. а) $2^{4x} \equiv 5 \pmod{47}$, б) $x^2 \equiv 58 \pmod{61}$.

19.24. а) $12^{7x} \equiv 15 \pmod{31}$, б) $2x^9 + 5 \equiv 0 \pmod{13}$.

19.25. а) $13^x \equiv 25 \pmod{43}$, б) $19x^5 + 13 \equiv 0 \pmod{53}$.

9. Арифметичні застосування конгруенцій

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай над числами $a, b, c, \ldots$ виконано деякі дії (додавання, віднімання, множення, піднесення до степеня). Щоб перевірити правильність отримання результату, використовують наступні способи.

I. Перевірка правильності виконання арифметичних дій за допомогою числа 9. Щоб перевірити результат виконання арифметичних дій за допомогою числа 9, треба:

1) знайти суму цифр кожного з чисел, над якими виконуються обчислення;
2) обчислити остачу від ділення на 9 кожної із знайдених сум цифр;
3) виконати над остачами ті ж дії, які виконуються над числами.

Якщо результат виконання дій над остачами відрізняється від знайденого результату на число, не кратне 9, то обчислення виконано неправильно.

Правило перевірки за допомогою числа 9 може не виявити помилку, якщо різниця між знайденою і істинною величинами кратна 9 (наприклад, не було взято до уваги нуль, або цифри результату записано не в тому порядку).

II. Перевірка правильності виконання арифметичних дій за допомогою числа 11. Щоб перевірити результат виконання арифметичних дій за допомогою числа 11, треба:

1) для кожного з чисел, над якими виконуються обчислення, знайти суму його цифр, взятих справа наліво почергово зі знаком „плюс” і „мінус”;

2) обчислити остачу від ділення на 11 кожної із знайдених сум цифр;
3) виконати над остачами ті ж дії, які виконуються над числами.

Якщо результат виконання дій над остачами відрізняється від знайденого результату на число, не кратне 11, то обчислення виконано неправильно.

При складних обчисленнях доцільно робити дві перевірки: одну числом 9, а іншу – числом 11. Можна також – числом 2.

Для перевірки дії $a \div b = c$ перевіряємо правильність виконання дії $b \cdot c = a$. Для перевірки дії $\sqrt{a} = b$ перевіряємо правильність виконання дії $b \cdot b = a$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 20. Перевірити правильність виконання арифметичних дій над цілими числами, використовуючи числа 9 і 11.

а) $7328 \cdot 8359 + 20431 - 54218 = 6120065$;
б) $574 \cdot 2976 = 1708224$.

Розв'язання. Замінимо рівності а) і б) на конгруентні їм за модулем 9:

а) $7328{\cdot}8359{+}20431{-}54218 \equiv (7{+}3{+}2{+}8){\cdot}(8{+}3{+}5{+}9){+}(2{+}0{+}4{+}3{+}1){-}(5+4+2+1+8) \pmod 9 \equiv 2 \cdot 7 + 1 - 2 \pmod 9 \equiv 4 \pmod 9$;

$61220065 \equiv (6+1+2+2+0+0+6+5) \pmod 9 \equiv 4 \pmod 9$.

б) $574{\cdot}2976 \equiv (5{+}7{+}4){\cdot}(2{+}9{+}7{+}6) \pmod 9 \equiv 7{\cdot}6 \pmod 9 \equiv 6 \pmod 9$;

$1708224 \equiv (1+7+0+8+2+2+4) \pmod 9 \equiv 6 \pmod 9$.

Отже, перевірка числом 9 в жодному з обчислень не виявила помилки. Перевіримо правильність виконання дій, використовуючи число 11.

а) $7328{\cdot}8359{+}20431{-}54218 \equiv (8{-}2{+}3{-}7){\cdot}(9{-}5{+}3{-}8){+}(1{-}3{+}4{-}0{+}2){-}{-}(8-1+2-4+5) \pmod{11} \equiv 2 \cdot (-1) + 4 - 10 \pmod{11} \equiv -8 \pmod{11} \equiv 3 \pmod{11}$;

$61220065 \equiv (5-6+0-0+2-2+1-6) \pmod{11} \equiv 5 \pmod{11}$.

Таким чином, $7328 \cdot 8359 + 20431 - 54218 \not\equiv 61220065 \pmod{11}$.

б) $574 \cdot 2976 \equiv (4-7+5) \cdot (6-7+9-2) \pmod{11} \equiv 2 \cdot 6 \pmod{11} \equiv \equiv 1 \pmod{11}$;

$1708224 \equiv (4-2+2-8+0-7+1) \pmod{11} \equiv 1 \pmod{11}$.

Отже, у прикладі а) дії виконано неправильно, тоді як у виконанні арифметичних дій над цілими числами у прикладі б) помилки не виявлено.

Розв'язання в Maple. Визначимо, чи конгруентні за модулем m ($m = 9$ або $m = 11$) ліва і права частина кожної із заданих рівностей. Перевіримо спочатку правильність обчислень в п.а) і б) числом 9.

```
> evalb((7+3+2+8)*(8+3+5+9)+(2+0+4+3+1)-(5+4+2+1+8) mod 9
=6+1+2+2+0+0+6+5 mod 9);
```

true

```
> evalb((5+7+4)*(2+9+7+6) mod 9=1+7+0+8+2+2+4 mod 9);
```

true

В обох випадках рівності правильні (true). Перевірка числом 9 помилок в обчисленнях не виявила.

Перевіримо тепер, чи правильно виконані обчислення за допомогою числа 11.

```
> evalb((8-2+3-7)*(9-5+3-8)+(1-3+4-0+2)-(8-1+2-4+5) mod 11
=5-6+0-0+2-2+1-6 mod 11);
```

false

```
> evalb((4-7+5)*(6-7+9-2) mod 11=4-2+2-8+0-7+1 mod 11);
```

true

В а) допущено помилку (false), в б) помилки не виявлено (але це ще не означає, що її немає).

Завдання 20. Перевірити правильність виконання арифметичних дій над цілими числами, використовуючи числа 9 і 11.

20.1. а) $79645 + 679 \cdot 137 - 17642 = 120016$;

б) $9631 \cdot 9413 = 90656603$.

20.2. а) $17659 + 569 \cdot 329 - 24637 = 180223$;

б) $879 \cdot 468 = 410202$.

20.3. а) $179 \cdot 8764 - 9761 + 746813 = 2302208$;

б) $27996 \cdot 387 = 10834452$.

20.4. а) $5687 \cdot 249 - 259 + 14856 = 1487789$;

б) $2984 \cdot 632 = 1435888$.

20.5. а) $5779 \cdot 887 + 37996 - 466731 = 467238$;

б) $844 \cdot 4973 = 4197212$.

20.6. а) $849 \cdot 625 + 2379 - 24967 = 508037$;

б) $896 \cdot 4788 = 4200048$.

20.7. а) $(8446 + 74349) \cdot 297 = 2450115$;

б) $941 \cdot 734 = 690694$.

20.8. а) $24973 + 238 \cdot 954 - 41957 = 210068$;
б) $679 \cdot 4187 = 2122973$.

20.9. а) $6997 \cdot 467 + 337994 - 19476 = 355117$;
б) $9446 \cdot 8876 = 83842696$.

20.10. а) $(69974 - 467) \cdot 467 = 3245769$;
б) $1759 \cdot 1998 = 3514482$.

20.11. а) $2486 \cdot 597 - 23794 + 14628 = 1474976$;
б) $867 \cdot 5948 = 5156016$.

20.12. а) $289 \cdot 4976 - 496137 + 19443 = 961370$;
б) $6873 \cdot 1946 = 13272258$.

20.13. а) $(667 \cdot 4419 + 7943) \cdot 8 = 23013328$;
б) $8493 \cdot 741 = 6293313$.

20.14. а) $76499 + 12964 \cdot 46 - 144487 = 528356$;
б) $946 \cdot 76744 = 72590824$.

20.15. а) $21794 - 244335 + 5749 \cdot 241 = 116268$;
б) $9471 \cdot 3871 = 36662241$.

20.16. а) $71297 \cdot 4557 - 841196 + 7778884 = 12848117$;
б) $967 \cdot 14763 = 14203821$.

20.17. а) $(88419 \cdot 23 - 95487) \cdot 41 = 7464150$;
б) $943 \cdot 918 = 865674$.

20.18. а) $8712 - 64647 + 8179 \cdot 987 = 8016738$;
б) $1794 \cdot 648 = 1130112$.

20.19. а) $(2479556 + 849 \cdot 248 - 1248732) \cdot 8 = 11531908$;
б) $9947 \cdot 918 = 9131346$.

20.20. а) $(541 + 57186) \cdot 53 - 24795 = 3032036$;
б) $4628 \cdot 297 = 1374516$.

20.21. а) $635 \cdot 448 + 23794 - 14958 = 293316$;
б) $2974 \cdot 4967 = 14721458$.

20.22. а) $21311 + 847 \cdot 2418 - 1874 = 2035083$;

б) $9643 \cdot 2499 = 24097857$.

20.23. а) $236 \cdot 589 - 54976 + 817322 = 901350$;

б) $1479 \cdot 9965 = 14504235$.

20.24. а) $(847628 + 851 \cdot 23) \cdot 34 = 2484834$;

б) $964 \cdot 2276 = 2194064$.

20.25. а) $255947 + 5974 \cdot 98 - 54645 = 786754$;

б) $29463 \cdot 98 = 2824374$.

Розділ III

Теорія кілець

1. Кільце. Поле

ТЕОРЕТИЧНІ ВІДОМОСТІ

Означення (кільця)**.** Впорядкована трійка $\langle K; *, \circ\rangle$, де K – непорожня множина, називається кільцем, якщо виконуються умови:

1) $*$ – бінарна алгебраїчна операція, задана на K;
2) операція $*$ асоціативна на K, тобто для будь-яких елементів $a, b, c \in K$ справедливо: $(a * b) * c = a * (b * c)$;
3) в K існує нейтральний відносно операції $*$ елемент θ, тобто такий, що для будь-якого $a \in K$ справедливо: $a * \theta = \theta * a = a$ (елемент θ називають нульовим);
4) для кожного елемента $a \in K$ в K існує симетричний до нього відносно операції $*$ елемент, тобто такий елемент a', що $a * a' = a' * a = \theta$ (елемент a' називають протилежним до елемента a);
5) операція $*$ комутативна на K, тобто для будь-яких $a, b \in K$ справедливо: $a * b = b * a$;
6) $\circ$ – бінарна алгебраїчна операція, задана на K;
7) операція $\circ$ асоціативна на K, тобто для будь-яких елементів a, b і c із K справедливо: $(a \circ b) \circ c = a \circ (b \circ c)$;
8) операція $\circ$ дистрибутивна зліва і справа відносно операції $*$ на K, тобто для будь-яких елементів a, b, c із K справедливо:

$$a \circ (b * c) = (a \circ b) * (a \circ c),$$
$$(b * c) \circ a = (b \circ a) * (c \circ a).$$

Умови 1)-8) називають аксіомами кільця.

Означення′. Впорядкована трійка $\langle K; *, \circ\rangle$, де K – непорожня множина, називається кільцем, якщо $\langle K; *\rangle$ – абелева група, а для операції $\circ$ виконуються умови 6)-8) означення кільця.

Кільце $\langle K; *, \circ\rangle$ називається **комутативним**, якщо комутативною є операція $\circ$, тобто якщо для будь-яких елементів a, b із K справедливо: $a \circ b = b \circ a$. Кільце $\langle K; *, \circ\rangle$ називають **кільцем з одиницею**, якщо в K існує одиничний елемент e, відмінний від нульового.

Найпростіші властивості довільного кільця:

1) нульовий елемент єдиний;

2) протилежний до кожного елемента кільця єдиний;
3) якщо одиничний елемент в кільці існує, то він єдиний;
4) якщо обернений елемент до даного існує, то він єдиний.

Означення (підкільця)**.** Непорожня підмножина K_1 кільця $\langle K; *, \circ\rangle$ називається підкільцем цього кільця, якщо $\langle K_1; *, \circ\rangle$ – кільце.

Всяке підкільце K_1 кільця K, відмінне від самого кільця K і від нульового підкільця, називається власним підкільцем цього кільця.

Теорема (критерій підкільця)**.** *Нехай $\langle K; *, \circ\rangle$ – кільце. Для того, щоб непорожня підмножина K_1 кільця K була підкільцем цього кільця, необхідно і достатньо, щоб виконувались умови:*

1) операція $*$ замкнена на K_1;
2) для довільного елемента $a \in K_1$ протилежний ло нього в K міститься в K_1;
3) операція $\circ$ замкнена на K_1.

Означення (поля)**.** Впорядкована трійка $\langle P; *, \circ\rangle$, де P – множина, що містить не менше двох елементів, називається полем, якщо виконуються наступні умови:

1) операція $*$ – бінарна алгебраїчна на множині P;
2) операція $*$ асоціативна на P;
3) в P існує нульовий елемент;
4) для кожного елемента a із P в P існує протилежний до нього елемент a';
5) операція $*$ комутативна на P;
6) операція $\circ$ – бінарна алгебраїчна на P;
7) операція $\circ$ асоціативна на P;
8) операція $\circ$ є дистрибутивною відносно операції $*$ на P;
9) операція $\circ$ є комутативною на P;
10) в P існує елемент ξ, нейтральний відносно операції $\circ$ (його називають одиничним);
11) для кожного ненульового елемента a із P існує в P симетричний до нього елемент відносно операції $\circ$ (його називають оберненим до a).

Умови 1)-11) означення поля називаються аксіомами поля.

Нехай P – поле. Мультиплікативну абелеву групу $P^* = P\backslash\{0\}$ називають **мультиплікативною групою поля** P.

Поле називається **скінченним**, якщо множина його елементів скінченна, і нескінченним, якщо множина його елементів нескінченна.

Найпростіші властивості поля:

1) нульовий елемент єдиний;
2) протилежний до кожного елемента єдиний;
3) одиничний елемент єдиний;
4) обернений до кожного ненульового елемента єдиний.

Означення (підполя)**.** Підмножина P_1 поля $\langle P; *, \circ\rangle$ називається підполем цього поля, якщо відносно операцій, заданих в P, вона сама є полем, тобто якщо $\langle P_1; *, \circ\rangle$ – поле.

Всяке підполе поля P, відмінне від самого поля, називається власним підполем цього поля.

Теорема (критерій підполя)**.** *Нехай $\langle P; *, \circ\rangle$ – поле. Для того, щоб підмножина P_1 поля P, яка містить не менше двох елементів, була підполем поля P, необхідно і достатньо, щоб виконувались умови:*

1) операція $*$ замкнена на P_1;
2) для довільного $a \in P_1$ протилежний до a в P міститься в P_1;
3) операція $\circ$ замкнена на P_1;
2) для довільного $a \in P_1$ обернений до a в P міститься в P_1.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 21.1. Визначити, чи утворює кільце (поле) множина M пар (a, b), де $a, b \in \mathbb{Z}_7$, відносно операцій додавання $*$ і множення $\circ$, заданих наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (ac + \overline{4}bd, ad + bc).\end{aligned}$$

Розв'язання. Оскільки кільце $\langle K; *, \circ\rangle$ таке, що $M \subset K$, підібрати важко, то застосувати критерій підкільця не можна. Перевіримо, чи виконуються умови 1)-8) означення кільця.

1) Нехай (a, b), (c, d) – довільні два елементи із M. Тоді $a, b, c, d \in \mathbb{Z}_7$. Маємо: $(a, b) * (c, d) = (a + c, b + d) \in M$, оскільки $a + c \in \mathbb{Z}_7$, $b + d \in \mathbb{Z}_7$. Отже, операція $*$ є замкненою на M. Крім того, операція $+$ виконувана і однозначна на $\mathbb{Z}_7$, тому $*$ є бінарною алгебраїчною на M.

2) Нехай (f, g) – ще один довільний елемент із M. Тоді:

$$\begin{aligned}((a,b) * (c,d)) * (f,g) &= (a+c, b+d) * (f,g) =\\ &= ((a+c)+f, (b+d)+g) = (a+(c+f), b+(d+g)) =\\ &= (a,b) * (c+f, d+g) = (a,b) * ((c,d) * (f,g)).\end{aligned}$$

Отже, операція $*$ є асоціативною на M.

5) Зручно (для спрощення перевірки умов 3) і 4)) показати спочатку, що операція $*$ – комутативна на M. Враховуючи, що операція $+$ комутативна на $\mathbb{Z}_7$, отримуємо:

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

3) В M нейтральним відносно операції $*$ є елемент $(\overline{0}, \overline{0})$, оскільки для довільного елемента $(a, b) \in M$ справедливо:

$$(a, b) * (\overline{0}, \overline{0}) = (a + \overline{0}, b + \overline{0}) = (a, b).$$

4) Легко бачити, що протилежним елементом до елемента $(a, b) \in M$ є елемент $(-a, -b)$, де $-a$ і $-b$ – протилежні до a і b відповідно в $\mathbb{Z}_7$, оскільки

$$(a,b)*(-a,-b)=(a-a,b-b)=(\overline{0},\overline{0}).$$

6) Визначимо, чи є операція $\circ$ бінарною алгебраїчною на M:

$$(a,b)\circ(c,d)=(ac+\overline{4}bd,ad+bc)\in M,$$

оскільки $ac+\overline{4}bd\in\mathbb{Z}_7$, $ad+bc\in\mathbb{Z}_7$. Крім того, операція $\cdot$ виконувана і однозначна на $\mathbb{Z}_7$, тому $\circ$ є бінарною алгебраїчною на M.

7) Покажемо, що операція $\circ$ – асоціативна на M. Маємо:

$$\Big((a,b)\circ(c,d)\Big)\circ(f,g)=(ac+\overline{4}bd,ad+bc)\circ(f,g)=$$
$$=\Big((ac+\overline{4}bd)f+\overline{4}(ad+bc)g,(ac+\overline{4}bd)g+(ad+bc)f\Big)=$$
$$=(acf+\overline{4}bdf+\overline{4}adg+\overline{4}bcg,acg+\overline{4}bdg+adf+bcf);$$
$$(a,b)\circ\Big((c,d)\circ(f,g)\Big)=(a,b)\circ(cf+\overline{4}dg,cg+df)=$$
$$=\Big(a(cf+\overline{4}dg)+\overline{4}b(cg+df),a(cg+df)+b(cf+\overline{4}dg)\Big)=$$
$$=(acf+\overline{4}adg+\overline{4}bcg+\overline{4}bdf,acg+adf+bcf+\overline{4}bdg).$$

звідки $\Big((a,b)\circ(c,d)\Big)\circ(f,g)=(a,b)\circ\Big((c,d)\circ(f,g)\Big)$.

8) Доведемо дистрибутивність операції $\circ$ відносно $*$. Покажемо, що виконується ліва дистрибутивність:

$$(a,b)\circ\Big((c,d)*(f,g)\Big)=(a,b)\circ(c+f,d+g)=$$
$$=\Big(a(c+f)+\overline{4}b(d+g),a(d+g)+b(c+f)\Big)=$$
$$=(ac+af+\overline{4}bd+\overline{4}bg,ad+ag+bc+bf)=$$
$$=\Big((ac+\overline{4}bd)+(af+\overline{4}bg),(ad+bc)+(ag+bf)\Big)=$$
$$=(ac+\overline{4}bd,ad+bc)*(af+\overline{4}bg,ag+bf)=$$
$$=\Big((a,b)\circ(c,d)\Big)*\Big((a,b)\circ(f,g)\Big).$$

Аналогічно легко перевірити праву дистрибутивність.

Умови 1)-8) означення кільця виконуються. Отже, множина M відносно заданих операцій $*$, $\circ$ є кільцем.

Перевіримо, чи буде множина M полем відносно операцій $*$ і $\circ$. Очевидно, M містить не менше двох елементів.

9) Покажемо, що операція $\circ$ комутативна на M:

$$(a,b)\circ(c,d)=(ac+\overline{4}bd,ad+bc)=(ca+\overline{4}db,da+cb)=(c,d)\circ(a,b).$$

10) Одиничним елементом кільця M є елемент $(\overline{1},\overline{0})$, оскільки

$$(a,b)\circ(\overline{1},\overline{0})=(a\cdot\overline{1}+\overline{4}\cdot b\cdot\overline{0},a\cdot\overline{0}+b\cdot\overline{1})=(a,b);$$

$$(\overline{1},\overline{0})\circ(a,b)=(\overline{1}\cdot a+\overline{4}\cdot\overline{0}\cdot b,\overline{1}\cdot b+\overline{0}\cdot a)=(a,b).$$

11) Нехай (a,b) – довільний ненульовий елемент із M, тобто a і b одночасно не рівні $\overline{0}$, і нехай $(x,y)\in M$ – обернений до нього елемент, тобто такий елемент із M, що $(a,b)\circ(x,y)=(\overline{1},\overline{0})$. Тоді $(ax+\overline{4}by,ay+bx)=(\overline{1},\overline{0})$, звідки

$$\begin{cases} ax+\overline{4}by=\overline{1},\\ ay+bx=\overline{0}. \end{cases}$$

Якщо $a=\overline{0}$, то $\overline{4}by=\overline{1}$, звідки $\overline{2}\cdot\overline{4}by=\overline{2}$, тобто $by=\overline{2}$. Оскільки в цьому випадку $b\neq\overline{0}$, то до елемента b в $\mathbb{Z}_7$ існує обернений елемент b^{-1}. Тоді $b^{-1}by=b^{-1}\overline{2}$, тобто $y=b^{-1}\overline{2}$. Із другої рівності знаходимо x: $x=b^{-1}\cdot\overline{0}=\overline{0}$. Отже, оберненим до елемента $(\overline{0},b)$ є елемент $(\overline{0},b^{-1}\overline{2})$.

Нехай $a\neq\overline{0}$, тоді з першого рівняння системи $x=a^{-1}(\overline{1}-\overline{4}by)$, звідси, $ay+ba^{-1}(\overline{1}-\overline{4}by)=\overline{0}$, значить, $(a-\overline{4}b^2a^{-1})y+ba^{-1}=\overline{0}$. Домноживши обидві частини даної рівності на a, матимемо: $(a^2-\overline{4}b^2)y+b=\overline{0}$. Якщо $a^2-\overline{4}b^2=\overline{0}$ і $b\neq\overline{0}$, то дане рівняння розв'язків в $\mathbb{Z}_7$ не має. Але це можливо при $a=\overline{5}$ і $b=\overline{1}$. Таким чином, до елемента $(\overline{5},\overline{1})$ в M оберненого немає. Отже, в кільці не для кожного ненульового елемента існує обернений. Значить, кільце $\langle M;*,\circ\rangle$ не є полем.

Розробка процедур. Вбудованих команд для перевірки, чи є задана множина відносно певних операцій кільцем (полем), в Maple немає. Створимо процедури для перевірки, чи є операція **operation** замкненою (**isClosed**), асоціативною (**isAssociative**), комутативною (**isCommutative**) на множині M, а також процедуру **isDistributive** для перевірки, чи є операція **operation2** дистрибутивною відносно операції **operation1**.

Процедура **isClosed**

В ході процедури для всіх $i,j\in\overline{1,t}$, де t – кількість елементів множини M ($t=nops(M)$), знаходимо результат операції:

```
> a:= operation(M[i],M[j]):
```

Якщо a є елементом множини M:

```
> member(a,M)
```

то збільшуємо лічильник s на 1:

```
> s:=s+1
```

В результаті, якщо $s=t^2$, то операція – замкнена (результат – **true**).

Процедура **isClosed** має наступний опис:

```
isClosed:=proc(M,operation)
local i,j,s,a, t;
   s:=0;
   t:=nops(M);
   for i from 1 to t do
      for j from 1 to t do
         a:= operation(M[i],M[j]):
         if member(a,M) then s:=s+1; end if;
      end do;
   end do;
   evalb(s=t^2)
end proc:
```

Процедура **isClosed** дозволяє також визначити, чи є операція **operation** виконуваною на множині M. У випадку, коли операція нездійсненна для елементів множини M, з'являється повідомлення на зразок наступного:

```
> isClosed(K,operation);
```

```
Error, (in operation) numeric exception: division by zero
```

(Помилка, в operation – ділення на 0).

Однак у випадку, коли операція не є однозначною, Maple може не дати правильної відповіді. Це пов'язано з тим, що для багатозначних операцій (наприклад, добування кореня n-го степеня з комплексного числа x: **root[n](x))** в Maple закладено результат, який задовольняє певні додаткові обмеження (результатом команди **root** є число $e^{\frac{1}{n}\ln x}$:)

```
> root[3](-8.0);
```

$$1.000000000 + 1.732050807\,I$$

Тому необхідна окрема перевірка, чи є задана операція однозначною, чи ні. (Зауважимо, що в наведених варіантах завдань всі операції – однозначні.)

Процедура **isAssociative**

Один із варіантів алгоритму для даної процедури – перевірка для всіх $i, j, k \in \overline{1, t}$, чи однаковими є результати

$$M[i] * (M[j] * M[k]) \qquad i \qquad (M[i] * M[j]) * M[k]. \tag{III.1}$$

Для цього аналогічно до попередньої процедури потрібно ввести лічильник s і використати цикли **for**:

```
s:=0;
t:=nops(M);
for i from 1 to t do
  for j from 1 to t do
    for k from 1 to t do
      if operation(operation(M[i],M[j]),M[k])=
        operation(M[i],operation(M[j],M[k])) then
        s:=s+1
      end if;
    end do;
  end do;
end do;
evalb(s=t^3)
```

Однак такий спосіб для множин M із великою кількість елементів займатиме багато часу. Доцільніше у випадку, коли знайдено трійку елементів, для яких умова (III.1) не виконується, припинити перевірку. Це можна реалізувати наступним чином: спочатку при $j = k = 1$ для всіх $i \in \overline{1,t}$ перевіряємо умову (III.1), потім збільшуємо на 1 число k і знову перевіряємо умову для всіх $i \in \overline{1,t}$, збільшуємо на 1 число k і т.д. Коли $k = t$, збільшуємо на 1 число j і т.д. Якщо в результаті $j = t$ і умова (III.1) виконується, збільшуємо на 1 число i (тобто $i = t + 1$), тоді операція – асоціативна на M. Якщо на якомусь кроці умова (III.1) не виконується, то перевірка припиняється, тоді $i < t + 1$ і операція не є асоціативною на M.

```
isAssociative:=proc(M,operation)
local i,j,k,t;
   t:=nops(M);
   i:=1; j:=1; k:=1;
   while (i<=t) and
      operation(operation(M[i],M[j]),M[k])=
         operation(M[i],operation(M[j],M[k ])) do
      if k=t then
         if j=t then i:=i+1; j:=1; k:=1; else j:=j+1; end if;
      else k:=k+1;
      end if;
   end do;
   evalb(i=t+1);
end proc:
```

Процедура **isCommutative**

Аналогічно до процедури **isAssociative**:

```
isCommutative:=proc(M,operation)
local i,j,t;
   t:=nops(M);
   i:=1; j:=1;
   while (i<=t and operation(M[i],M[j])=operation(M[j],M[i])) do
      if j=t then i:=i+1; j:=1; else j:=j+1; end if;
   end do;
   evalb(i=t+1);
end proc:
```

Процедура **isDistributive**

Аналогічно до процедури **isAssociative**, причому відбувається одночасна перевірка як лівої, так і правої дистрибутивності.

```
isDistributive:=proc(M,operation1,operation2)
local i,j,k,t;
   t:=nops(M);
   i:=1; j:=1;k:=1;
   while (i<=t) and operation2(M[i],operation1(M[j],M[k]))=
      operation1(operation2(M[i],M[j] ),operation2(M[i],M[k])) and
      operation2(operation1(M[i],M[j]),M[k])=
      operation1(operation2(M[i],M[k]),operation2(M[j],M[k])) do
         if k=t then
            if j=t then i:=i+1; j:=1; k:=1; else j:=j+1; end if;
         else k:=k+1;
         end if;
   end do;
   evalb(i=t+1);
end proc:
```

Тепер створимо процедуру **Id(M,operation)** для відшукання в множині **M** елемента, нейтрального відносно операції **operation**: перевіряємо, чи виконуються умови: operation(M[i],M[j])=M[j] та operation(M[j],M[i])=M[j] для всіх $j \in \overline{1,t}$. Якщо для всіх $j \in \overline{1,t}$ умови виконується, то $s = t$ і $M[i]$ – нейтральний відносно операції operation. Якщо ж числа i, для якого були б справедливі дані умови при всіх $j \in \overline{1,t}$ не існує, результатом процедури є false.

```
Id:=proc(M,operation)
local i,j,s,t;
   t:=nops(M);
   i:=1;
   while i<=t do s:=0;
      for j from 1 to t do
         if operation(M[i],M[j])=M[j] and operation(M[j],M[i])=M[j]
            then s:=s+1;
         end if;
      end do;
      if s=t then return(M[i]); break; end if;
      i:=i+1;
   end do;
   return false;
end proc:
```

Зручно створити окрему процедуру **Sym(a,M,operation)** для пошуку в M елемента, симетричного відносно операції **operation** до заданого елемента a. Алгоритм роботи аналогічний до алгоритму процедури **Id**: перевіряємо, чи виконуються умови operation(a,M[j])=Id(M,operation) та operation(M[j],a)=Id(M,operation).

```
Sym:=proc(a,M,operation)
local j,t;
   t:=nops(M);
   j:=1;
   while j<=t do
      if operation(a,M[j])=Id(M,operation) and
               operation(M[j],a)=Id(M,operation) then
         return(M[j]); print(M[j]); break;
      else j:=j+1;
      end if;
   end do;
   if j=t+1 then return false; end if;
end proc:
```

Наступна процедура перевіряє, чи для кожного із елементів $M[i]$ існує симетричний елемент Sym(M[i],M,operation). Якщо для всіх елементів із M Sym(M[i],M,operation)<>false, то лічильник s набуде значення, рівного t.

```
hasSym:=proc(M,operation)
local i,s,t;
   t:=nops(M);
   s:=0;
   for i from 1 to t do
      if Sym(M[i],M,operation)<>false then s:=s+1; end if;
   end do;
   evalb(s=t);
end proc:
```

Розроблені процедури можна використати для створення процедури **isRing**, яка визначатиме, чи є множина **M** кільцем відносно операцій **operation1** і **operation2**. Для того, щоб множина M була кільцем відносно операцій operation1 і operation2, необхідно і достатньо, щоб умови 1)-8) виконувались одночасно (для цього при записі умов в межах умовного оператора **if** вони поєднуються логічним оператором **and** (i)).

```
isRing:=proc(M,operation1,operation2);
   if isClosed(M,operation1) and isAssociative(M,operation1) and
      Id(M,operation1)<>false and hasSym(M,operation1)<>false and
      isCommutative(M,operation1) and isClosed(M,operation2) and
      isAssociative(M,operation2) and
      isDistributive(M,operation1,operation2) then return true
   else return false;
   end if;
end proc:
```

Спробуйте самостійно розробити процедуру **isField**, яка визначатиме, чи є множина **M** полем відносно операцій **operation1** і **operation2**!

Розв'язання в Maple. Задати впорядковану пару можна із використанням об'єктів типу Matrix (матриця), Array (массив), Table (таблиця), List (список). Maple швидше працює із списками, ніж із матрицями, тому задаватимемо множини впорядкованих пар як об'єкти типу List (див. §5 розд.I): пару (a, b) записуємо у вигляді **[a,b]**. Для того, щоб вказати, що a і b можуть набувати значень від $\overline{0}$ до $\overline{m-1}$, використовуємо команду seq:

```
> M:={seq(seq([a,b],a=0..6),b=0..6)};
```

$M := \{[0, 0], [0, 1], [0, 2], [0, 3], [0, 4], [0, 5], [0, 6], [1, 0], [1, 1], [1, 2], [1, 3], [1, 4], [1, 5], [1, 6], [2, 0], [2, 1], [2, 2], [2, 3], [2, 4], [2, 5], [2, 6], [3, 0], [3, 1], [3, 2], [3, 3], [3, 4], [3, 5], [3, 6], [4, 0], [4, 1], [4, 2], [4, 3], [4, 4], [4, 5], [4, 6], [5, 0], [5, 1], [5, 2], [5, 3], [5, 4], [5, 5], [5, 6], [6, 0], [6, 1], [6, 2], [6, 3], [6, 4], [6, 5], [6, 6]\}$

Операцію $*$ задамо за допомогою функціонального оператора (див. §4 розд.I.)): двом елементам $X = [X[1], X[2]]$ і $Y = [Y[1], Y[2]]$ поставимо у відповідність результат операції $X * Y$, тобто пару $[X[1] + X[2] \mod m, [Y[1] + Y[2] \mod m]$:

```
> astra:=(X,Y)->[X[1]+Y[1] mod 7,X[2]+Y[2] mod 7];
```

Результат операції $*$ знаходимо наступним чином:

```
> astra([6,2],[3,4]);
```

[2, 6]

і аналогічно для операції $\circ$:

```
> circ:=(X,Y)->[X[1]*Y[1]+4*X[2]*Y[2] mod 7,
X[1]*Y[2]+X[2]*Y[1] mod 7];
```

Тепер підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);
  with(atchlib):
```

і за допомогою створених процедур послідовно перевіряємо, чи виконуються умови 1)-8) означення кільця.

Умова 1:

```
> isClosed(M,astra);
```

true

Операція $*$ є бінарною алгебраїчною на M.

Умова 2:

```
> isAssociative(M,astra);
```

true

Операція $*$ є асоціативною на M.

Умова 3:

```
> Id(M,astra);
```

[0, 0]

Нульовим (нейтральним відносно операції $*$) є елемент $(\overline{0}, \overline{0})$.

Умова 4:

```
> hasSym(M,astra);
```

true

Для кожного елемента в M протилежний до нього (симетричний відносно операції $*$) елемент існує.

Умова 5:

```
> isCommutative(M,astra);
```

true

Операція $*$ є комутативною на M.

Умова 6:

```
> isClosed(M,circ);
```

true

Операція $\circ$ є бінарною алгебраїчною на M.

Умова 7:

```
> isAssociative(M,circ);
```

true

Операція $\circ$ є асоціативною на M.

Умова 8:

```
> isDistributive(M,astra,circ);
```

true

Операція $\circ$ є дистрибутивною відносно операції $*$ на M.

Таким чином, $\langle K; *, \circ\rangle$ є кільцем.

Тепер визначимо, чи це кільце є комутативним і чи має воно одиничний елемент:

```
> isCommutative(M,circ);
```

true

Операція $\circ$ є комутативною на M.

```
> Id(M,circ);
```

[1, 0]

Одиничним (нейтральним відносно операції $\circ$) є елемент $(\overline{1}, \overline{0})$.

Отже, $\langle K; *, \circ\rangle$ – комутативне кільце з одиницею.

Визначимо, чи є досліджуване кільце полем. Залишається перевірити, чи для кожного елемента, відмінного від нульового, в M існує обернений до нього (симетричний відносно операції $\circ$) елемент. Для цього множину, до якої застосовуємо процедуру **hasSym**, записуємо у вигляді різниці множин M і $\{\mathrm{Id(M, astra)}\}$):

```
> hasSym(M minus {Id(M,astra)},circ);
```

false

Умова не виконується: обернений елемент існує не для всіх елементів, відмінних від нульового. Отже, задана множина M є комутативним кільцем з одиницею, але не є полем.

Процедура **isRing** дає наступний результат:

```
> isRing(M,astra,circ);
```

true

Приклад 21.2. Визначити, чи утворює кільце (поле) множина M пар (a,b), де $a,b \in \mathbb{Z}_8$, відносно операцій додавання $*$ і множення $\circ$, заданих наступним чином:

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

Розв'язання. Оскільки кільце $\langle K;*,\circ\rangle$ таке, що $M \subset K$, підібрати важко, то використати критерій підкільця не маємо змоги. Тому перевіряємо, чи виконуються умови 1)-8) означення кільця.

1) Нехай (a,b), (c,d) – довільні два елементи із M. Тоді $a,b,c,d \in \mathbb{Z}_8$ і $(a,b)*(c,d) = (a+c,bd) \in M$, оскільки $a+c \in \mathbb{Z}_8$, $bd \in \mathbb{Z}_8$. Операція $*$ є замкненою на M. Крім того, операція $+$ виконувана і однозначна на $\mathbb{Z}_8$, тому $*$ є бінарною алгебраїчною на M.

2) Нехай (f,g) – довільний елемент із M. Маємо:

$$\begin{aligned}((a,b)*(c,d))*(f,g) &= (a+c,bd)*(f,g) = ((a+c)+f,(bd)g) =\\ &= (a+(c+f),b(dg)) = (a,b)*(c+f,dg) = (a,b)*((c,d)*(f,g)),\end{aligned}$$

тобто операція $*$ – асоціативна на M.

3) В M нульовим елементом є елемент $(\overline{0},\overline{1})$, оскільки для довільного елемента $(a,b) \in M$ справедливо: $(a,b)*(\overline{0},\overline{1}) = (\overline{0},\overline{1})*(a,b) = (a+\overline{0},b\cdot\overline{1}) = (a,b)$.

4) Припустимо, що (x,y) – протилежний елемент до елемента (a,b). Тоді виконуються умови: $(a,b)*(x,y) = (\overline{0},\overline{1})$, $(x,y)*(a,b) = (\overline{0},\overline{1})$. З першої умови маємо: $(a+x,by) = (\overline{0},\overline{1})$, звідки $a+x = \overline{0}$, $by = \overline{1}$, тобто x – протилежний до a в $\mathbb{Z}_8$, y – обернений до b в $\mathbb{Z}_8$. Оскільки не для кожного елемента в $\mathbb{Z}_8$ обернений існує, то і протилежний до (a,b) в M існуватиме не завжди. Отже, $\langle M;*,\circ\rangle$ не є кільцем.

Розв'язання в Maple. Задаємо множину і операції:

```
> M:={seq(seq([a,b],a=0..7),b=0..7)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 8,X[2]*Y[2] mod 8]:
> circ:=(X,Y)->[X[1]*Y[2] mod 8,X[2]*Y[1] mod 8]:
```

Тепер підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);  with(atchlib):
```

і використовуємо процедури, створені при розв'язанні Прикладу 21.1.

```
> isClosed(M,astra);
```

true

Операція $*$ є бінарною алгебраїчною на M.

```
> isAssociative(M,astra);
```

true

Операція $*$ – асоціативна на M.

```
> Id(M,astra);
```

[0, 1]

Нейтральним відносно операції $*$ є елемент $(\overline{0}, \overline{1})$,

```
> hasSym(M,astra);
```

false

Не для кожного елемента в M існує симетричний до нього відносно операції $*$. Отже, $\langle M; *, \circ\rangle$ не є кільцем.

```
> isRing(M,astra,circ);
```

false

Приклад 21.3. Визначити, чи утворює кільце (поле) множина M пар (a, b), де $a, b \in \mathbb{Z}_7$, відносно операцій додавання $*$ і множення $\circ$, заданих наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (ac, \overline{0}).\end{aligned}$$

Розв'язання. При розв'язанні Прикладу 21.1 було показано, що операція $*$ є бінарною алгебраїчною, асоціативною, комутативною на множині M, має нейтральний елемент і для кожного елемента в M існує симетричний відносно операції $*$. Розглянемо властивості операції $\circ$ на M.

6) Нехай (a, b), (c, d) – довільні два елементи із M, тоді $a, b, c, d \in \mathbb{Z}_7$. Маємо: $(a, b) \circ (c, d) = (ac, \overline{0}) \in M$, оскільки $ac \in \mathbb{Z}_7$. Операція $\circ$ є замкненою на M. Крім того, елемент ac завжди існує в $\mathbb{Z}_7$ і єдиний, отже, $(ac, \overline{0})$ існує і єдиний, тому $\circ$ є бінарною алгебраїчною на M.

7) Покажемо, що операція $\circ$ – асоціативна на M. Нехай $(f, g) \in M$. Маємо:

$$\Big((a,b) \circ (c,d)\Big) \circ (f,g) = (ac, \overline{0}) \circ (f,g) = \Big((ac)f, \overline{0}\Big);$$

$$(a,b) \circ \Big((c,d) \circ (f,g)\Big) = (a,b) \odot (cf, \overline{0}) = \Big(a(cf), \overline{0}\Big).$$

Оскільки операція є асоціативною на $\mathbb{Z}_7$, то $(ac)f = a(cf)$, звідки $\Big((a,b) \circ (c,d)\Big) \circ (f,g) = (a,b) \circ \Big((c,d) \circ (f,g)\Big)$.

8) Доведемо дистрибутивність операції $\circ$ відносно $*$. Покажемо, що виконується ліва дистрибутивність:

$$(a,b)\circ\Big((c,d)*(f,g)\Big)=(a,b)\circ(c+f,d+g)=\ =\Big(a(c+f),\overline{0}\Big);$$

$$\Big((a,b)\circ(c,d)\Big)*\Big((a,b)\circ(f,g)\Big)=(ac,\overline{0})*(af,\overline{0})=(ac+af,\overline{0}).$$

Оскільки на $\mathbb{Z}_7$ справедливо, що $a(c+f)=ac+af$, то $\circ$ – дистрибутивна зліва відносно $*$ на M. Аналогічно легко перевірити праву дистрибутивність.

Умови 1)-8) означення кільця виконуються. Отже, множина M відносно заданих операцій $*$, $\circ$ є кільцем.

Перевіримо, чи буде множина M полем відносно операцій $*$ і $\circ$. Очевидно, M містить не менше двох елементів.

9) Оскільки операція $\cdot$ комутативна на $\mathbb{Z}_7$, то

$$(a,b)\circ(c,d)=(ac,\overline{0})=(ca,\overline{0})=(c,d)\circ(a,b).$$

Отже, операція $\circ$ комутативна на M.

10) Покажемо, що одиничного елемента в M не існує. Дійсно, нехай (x,y) – одиничний елемент. Тоді для довільного $(a,b)\in M$ справедливо, що:

$$(a,b)\circ(x,y)=(a,b)\qquad i\qquad(x,y)\circ(a,b)=(a,b).$$

З першої умови маємо: $(ax,\overline{0})=(a,b)$, тоді $b=\overline{0}$, що суперечить довільності вибору (a,b). Отже, припущення невірне, в M одиничного елемента немає.

Таким чином, $\langle M;*,\circ\rangle$ – комутативне кільце без одиниці.

Розв'язання в Maple. Задаємо множину і операції:

```
> M:={seq(seq([a,b],a=0..6),b=0..6)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 7,X[2]+Y[2] mod 7]:
> circ:=(X,Y)->[X[1]*Y[1] mod 7,0 mod 7]:
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо процедури, створені при розв'язанні Прикладу 21.1.

```
> isClosed(M,astra);
```

true

```
> isAssociative(M,astra);
```

true

```
> Id(M,astra);
```

[0, 0]

```
> hasSym(M,astra);
```

true

```
> isCommutative(M,astra);
```

true

```
> isClosed(M,circ);
```

true

```
> isAssociative(M,circ);
```

true

```
> isDistributive(M,astra,circ);
```

true

```
> isCommutative(M,circ);
```

true

```
> Id(M,circ);
```

false

Таким чином, $\langle M; *, \circ\rangle$ – комутативне кільце без одиниці.

```
> isRing(M,astra,circ);
```

true

Завдання 21. Визначити, чи утворює кільце (поле):

21.1. множина пар (a, b), де $a, b \in \mathbb{Z}_2$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (ac, ab+cd).\end{aligned}$$

21.2. множина пар (a, b), де $a, b \in \mathbb{Z}_7$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a+b, c-d),\\ (a,b) \circ (c,d) &= (ab, cd).\end{aligned}$$

21.3. множина трійок $(a, \overline{0}, b)$, де $a, b, \overline{0} \in \mathbb{Z}_5$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a,\overline{0},b) * (c,\overline{0},d) &= (a+c, \overline{0}, \overline{2}(b+d)),\\ (a,\overline{0},b) \circ (c,\overline{0},d) &= (ac-bd, \overline{0}, abcd).\end{aligned}$$

21.4. множина пар (a, b), де $a, b \in \mathbb{Z}_{10}$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a + , \overline{0}),\\ (a,b) \circ (c,d) &= (ac, bd).\end{aligned}$$

21.5. множина пар (a, b), де $a, b \in \mathbb{Z}_4$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a + c, b + d),\\ (a,b) \circ (c,d) &= (bd - ac, ab + cd).\end{aligned}$$

21.6. множина пар (a, b), де $a, b \in \mathbb{Z}_{13}$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a + d, bc),\\ (a,b) \circ (c,d) &= (a - d, \overline{0}).\end{aligned}$$

21.7. множина пар (a, b), де $a, b \in \mathbb{Z}_5$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a + c, b - d),\\ (a,b) \circ (c,d) &= (ac, b).\end{aligned}$$

21.8. множина пар (a, b), де $a, b \in \mathbb{Z}_6$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a - c, \overline{0}),\\ (a,b) \circ (c,d) &= (ac, \overline{0}).\end{aligned}$$

21.9. множина пар (a, b), де $a, b \in \mathbb{Z}_3$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a, b),\\ (a,b) \circ (c,d) &= (ac, bd).\end{aligned}$$

21.10. множина пар (a, b), де $a, b \in \mathbb{Z}_8$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a + c, b + d),\\ (a,b) \circ (c,d) &= (ac - bd, \overline{0}).\end{aligned}$$

21.11. множина трійок (a, b, c), де $a, b, c \in \mathbb{Z}_5$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a, b, c) * (m, n, l) &= (a + m, b + n, c + l),\\ (a, b, c) \circ (m, n, l) &= (\overline{0}, \overline{0}, \overline{0}).\end{aligned}$$

21.12. множина пар (a, b), де $a, b \in \mathbb{Z}_5$, відносно операцій $*$ і $\circ$, введених наступним чином:

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

21.13. множина трійок $(\overline{0}, a, b)$, де $a, b \in \mathbb{Z}_{10}$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(\overline{0}, a, b) * (\overline{0}, c, d) &= (\overline{0}, a + c, b + d),\\ (\overline{0}, a, b) \circ (\overline{0}, c, d) &= (\overline{0}, ac, ab + cd).\end{aligned}$$

21.14. множина пар (a, b), де $a, b \in \mathbb{Z}_9$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + c, \overline{3}(b + d),\\ (a, b) \circ (c, d) &= (ac, \overline{3}bd).\end{aligned}$$

21.15. множина трійок $(a, \overline{0}, b)$, де $a, b, \overline{0} \in \mathbb{Z}_{11}$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a, \overline{0}, b) * (c, \overline{0}, d) &= (a + c, \overline{0}, \overline{2}(b + d)),\\ (a, \overline{0}, b) \circ (c, \overline{0}, d) &= (ac - bd, \overline{0}, abcd).\end{aligned}$$

21.16. множина пар (a, b), де $a, b \in \mathbb{Z}_4$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (\overline{0}, b + d),\\ (a, b) \circ (c, d) &= (\overline{0}, bd).\end{aligned}$$

21.17. множина пар (a, b), де $a, b \in \mathbb{Z}_6$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + d, bc),\\ (a, b) \circ (c, d) &= (a - d, \overline{0}).\end{aligned}$$

21.18. множина пар (a, b), де $a, b \in \mathbb{Z}_3$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + c, b + d),\\ (a, b) \circ (c, d) &= (bd - ac, ab + cd).\end{aligned}$$

21.19. множина трійок $(\overline{0}, a, b)$, де $a, b \in \mathbb{Z}_5$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(\overline{0}, a, b) * (\overline{0}, c, d) &= (\overline{0}, a + c, b + d),\\ (\overline{0}, a, b) \circ (\overline{0}, c, d) &= (\overline{0}, ac, ab + cd).\end{aligned}$$

21.20. множина пар (a, b), де $a, b \in \mathbb{Z}_{10}$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + b, c - d),\\ (a, b) \circ (c, d) &= (ab, cd).\end{aligned}$$

21.21. множина пар (a, b), де $a, b \in \mathbb{Z}_{11}$, відносно операцій $*$ і $\circ$, введених наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + , \overline{0}),\\ (a, b) \circ (c, d) &= (ac, bd).\end{aligned}$$

21.22. множина пар (a, b), де $a, b \in \mathbb{Z}_8$, відносно операцій $*$ і $\circ$, введених наступним чином:

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

21.23. множина трійок $(a, \overline{0}, b)$, де $a, b\mathbb{Z}_5$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a, \overline{0}, b) * (c, \overline{0}, d) &= (a + c, \overline{0}, b + d),\\ (a, \overline{0}, b) \circ (c, \overline{0}, d) &= (\overline{0}, bd - ac, ab + cd).\end{aligned}$$

21.24. множина пар (a, b), де $a, b \in \mathbb{Z}_3$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + c, b + d),\\ (a, b) \circ (c, d) &= (ac - bd, \overline{0}).\end{aligned}$$

21.25. множина пар (a,b), де $a,b \in \mathbb{Z}_6$, відносно операцій $*$ і $\circ$, заданих наступним чином:

$$\begin{aligned}(a,b)*(c,d) &= (a+c, \overline{4}(b+d)),\\ (a,b)\circ(c,d) &= (ac-bd, abcd).\end{aligned}$$

2. Відношення подільності в комутативних кільцях

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай кільце $\langle K;+,\cdot\rangle$ – комутативне. Говорять, що елемент a кільця K **ділиться** на елемент b цього ж кільця (пишуть $a \vdots b$), якщо існує елемент $c \in K$ такий, що $a = b\cdot c$. В цьому випадку кажуть також, що b є дільником a (пишуть $b \mid a$).

Говорять, що елемент a кільця K не ділиться на елемент b цього ж кільця (пишуть $a \not\vdots b$), якщо в кільці K не існує елемента c такого, що $a = b\cdot c$. В цьому випадку кажуть також, що b не є дільником a (пишуть $b \nmid a$).

Елемент a кільця K, для якого в K існує обернений елемент, називається **дільником одиниці** кільця K.

Нехай θ – нульовий елемент кільця K. Елемент $a \neq \theta$ кільця K, для якого в K існує елемент $b \neq \theta$ такий, що $a\cdot b = \theta$ або $b\cdot a = \theta$, називається **дільником нуля** кільця K. У випадку некомутативного кільця розрізняють поняття лівого дільника нуля і правого дільника нуля. Якщо $a \neq \theta$ і $b \neq \theta$, але $ab = \theta$, то a називається лівим, а b – правим дільником нуля. Дільник нуля кільця K не може бути дільником одиниці цього кільця.

Нехай a, b, c, a_i, b_i, $i \in \overline{1,s}$ – довільні елементи, ε – довільний дільник одиниці комутативного кільця K. Тоді:

1. Якщо $a \vdots b$, $b \vdots c$ в K, то $a \vdots c$ в K.
2. Якщо $a \vdots c$ і $b \vdots c$ в K, то $(a \pm b) \vdots c$ в K.
3. Якщо $a \vdots b$ в K, то $ac \vdots b$ в K.
4. Якщо $a_1 \vdots c, a_2 \vdots c, ..., a_s \vdots c$ в K, то $(a_1b_1 \pm a_2b_2 \pm ... \pm a_sb_s) \vdots c$ в K.
5. $a \vdots \varepsilon$, $a \vdots a\varepsilon$.
6. Якщо $a \vdots b$ в K, то $a \vdots b\varepsilon$ в K.
7. Кожний дільник елемента $a\varepsilon$ є дільником елемента a.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 22.1. В кільці $\langle K;*,\circ\rangle$, де K – множина пар (a,b), $a,b \in \mathbb{Z}_7$, а операції додавання $*$ і множення $\circ$, задані наступним чином:

$$\begin{aligned}(a,b)*(c,d) &= (a+c, b+d),\\ (a,b)\circ(c,d) &= (ac+\overline{4}bd, ad+bc).\end{aligned}$$

знайти всі дільники нуля і, якщо є одиничний елемент, знайти всі дільники одиниці.

Розв'язання. Знайдемо спочатку дільники одиниці кільця K. Одиничним елементом цього кільця є елемент $(\overline{1}, \overline{0})$ (див. Приклад). Нехай (a, b) – довільний дільник одиниці кільця K. Тоді в K існує елемент (x, y), обернений до (a, b), тобто виконується умова: $(a, b) \circ (x, y) = (\overline{1}, \overline{0})$. Звідси, $ax + \overline{4}by = \overline{1}$, $ay + bx = \overline{0}$. Якщо $a = \overline{0}$, то $b \neq \overline{0}$ (оскільки дільник одиниці не може бути нульовим елементом), тоді для b в $\mathbb{Z}_7$ існує обернений елемент b^{-1}. Домножимо обидві частини рівності $\overline{4}by = \overline{1}$ на $\overline{2}$, матимемо: $by = \overline{2}$, звідси, $b^{-1}by = b^{-1} \cdot \overline{2}$, отже, $y = b^{-1} \cdot \overline{2} = \overline{2}b^{-1}$. Далі з рівності $bx = \overline{0}$ отримуємо: $x = b^{-1} \cdot \overline{0} = \overline{0}$. Отже, для елемента $(\overline{0}, b)$ при $b \neq \overline{0}$ оберненим елементом повинен бути елемент $(\overline{0}, \overline{2}b^{-1}$. Такий елемент існує завжди, отже, кожен елемент $(\overline{0}, b)$, $b \neq \overline{0}$, є дільником одиниці в K.

Якщо $b = \overline{0}$, то $ax = \overline{1}$, $ay = \overline{0}$. Оскільки в цьому випадку $a \neq \overline{0}$, то до a в $\mathbb{Z}_7$ існує обернений елемент a^{-1}, тоді $x = a^{-1}$, $y = \overline{0}$. Отже, для елемента $(a, \overline{0})$, де $a \neq \overline{0}$, обернений елемент існує.

Нехай $a \neq \overline{0}$, $b \neq \overline{0}$, тоді в $\mathbb{Z}_7$ існує обернений до a елемент a^{-1}, значить, $x = a^{-1}(\overline{1} - \overline{4}by)$, звідси, $ay + ba^{-1}(\overline{1} - \overline{4}by) = \overline{0}$, значить, $(a - \overline{4}b^2a^{-1})y + ba^{-1} = \overline{0}$. Домноживши обидві частини даної рівності на a, матимемо: $(a^2 - \overline{4}b^2)y + b = \overline{0}$. Знайдемо умови, при яких рівняння $(a^2 - \overline{4}b^2)y + b = \overline{0}$ має розв'язки в $\mathbb{Z}_7$. Якщо $a^2 - \overline{4}b^2 \neq \overline{0}$, то в $\mathbb{Z}_7$ до елемента $a^2 - \overline{4}b^2$ існує обернений елемент, тоді $y = (a^2 - \overline{4}b^2)^{-1}(-b)$. Нехай $a^2 - \overline{4}b^2 = \overline{0}$, тоді $\overline{0}y + b = \overline{0}$. Оскільки $b \neq \overline{0}$, то дане рівняння розв'язків в $\mathbb{Z}_7$ не має.

Таким чином, дільниками одиниці в M є елементи: $(\overline{0}, b)$, де $b \neq \overline{0}$; $(a, \overline{0})$, де $a \neq \overline{0}$; (a, b), де $a^2 - \overline{4}b^2 \neq \overline{0}$.

Тепер знайдемо дільники нуля в K. Нульовим елементом кільця K є елемент $(\overline{0}, \overline{0})$. Нехай (a, b) – довільний дільник нуля в K. Тоді $(a, b) \neq (\overline{0}, \overline{0})$ і в K існує елемент $(x, y) \neq (\overline{0}, \overline{0})$ такий, що $(a, b) \circ (x, y) = (\overline{0}, \overline{0})$, звідки $ax + \overline{4}by = \overline{0}$, $ay + bx = \overline{0}$. (Оскільки задане кільце комутативне, то умову $(x, y) \circ (a, b) = (\overline{0}, \overline{0})$ розглядати не потрібно).

Якщо $a = \overline{0}$, то $b \neq \overline{0}$. Маємо: $\overline{4}by = \overline{0}$, $bx = \overline{0}$. Оскільки в $\mathbb{Z}_7$ дільників нуля немає ($\mathbb{Z}_7$ є полем), то $y = \overline{0}$, $x = \overline{0}$, що неможливо, в силу вибору (x, y). Якщо $b = \overline{0}$, то $a \neq \overline{0}$, і аналогічно приходимо до суперечності.

Нехай $a \neq \overline{0}$, $b \neq \overline{0}$, тоді $x = -a^{-1} \cdot \overline{4}by$, значить, $ay - ba^{-1} \cdot \overline{4}by = \overline{0}$, звідки $(a^2 - \overline{4}b^2)y = \overline{0}$. Якщо $a^2 - \overline{4}b^2 \neq \overline{0}$, то $y = \overline{0}$, звідки $x = \overline{0}$, що суперечить вибору (x, y). Нехай $a^2 - \overline{4}b^2 = \overline{0}$, тоді y – довільний елемент із $\mathbb{Z}_7$. Отже, дільником нуля в M є кожен елемент (a, b), де $a \neq \overline{0}$, $b \neq \overline{0}$, $a^2 - \overline{4}b^2 = \overline{0}$ (наприклад, пара $(\overline{5}, \overline{1})$).

Розробка процедур. Для створення процедури пошуку дільників одиниці в кільці K зручно використати команду **Sym** із параметрами a,K,operation, за допомогою якої знаходимо елемент, симетричний до $a \in K$ відносно операції operation (див. Приклад 21.1). Якщо для елемента $a \in K$ симетричний відносно операції $\circ$ існує, то a – дільник одиниці в K. Множину дільників одиниці позначимо через A. На початку процедури $A = \varnothing$, знайдений в процесі дільник одиниці додається до множини A, для цього використовуємо оператор union.

```
divisorsId:=proc(K,operation2)
local i,A,t;
   t:= nops(K); A:={};
   for i from 1 to t do
      if Sym(K[i],K,operation2)<>false
      then A:=A union {K[i]}; end if;
   end do;
   return(A);
end proc:
```

Дільники нуля знайдемо, перевіривши всі попарні добутки елементів $K[i]$ і $K[j]$ із K: якщо добуток $K[i] \circ K[j]$ дорівнює нульовому елементу кільця K (тобто елемент $Id(K, operation1)$), причому $K[i] \neq Id$, $K[j] \neq Id$, то $K[i]$ є лівим, а $K[j]$ – правим дільником нуля. Оскільки дільником нуля є той елемент кільця, який одночасно є і лівим, і правим дільником нуля, то, знаючи множину A лівих дільників нуля і множину B правих дільників нуля, множину C дільників нуля легко знайти як перетин множин A і B: $C = A \cap B$.

```
divisorsZero:=proc(K,operation1,operation2)
local i,j,A,B,C,t;
   t:=nops(K);
   A:={}; B:={};
   for i from 1 to t do
      for j from 1 to t do
         if (operation2(K[i],K[j])=Id(K,operation1) and
            K[i]<>Id(K,operation1) and K[j]<>Id(K,operation1)) then
            A:=A union {K[i]}; B:=B union {K[i]};
         end if;
      end do;
   end do;
   C:=A intersect B;
   return(C);
end proc:
```

Розв'язання в Maple. Задаємо кільце (множину K і операції $*$, $\circ$):

```
> K:={seq(seq([a,b],a=0..6),b=0..6)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 7,X[2]+Y[2] mod 7]:
> circ:=(X,Y)->[X[1]*Y[1]+4*X[2]*Y[2] mod 7,
  X[1]*Y[2]+X[2]*Y[1] mod 7]:
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);  with(atchlib):
```

Знаходимо дільники одиниці в K:

```
> divisorsId(K,circ);
```

{[0, 1], [0, 2], [0, 3], [0, 4], [0, 5], [0, 6], [1, 0], [1, 1], [1, 2], [1, 5], [1, 6], [2, 0], [2, 2], [2, 3], [2, 4], [2, 5], [3, 0], [3, 1], [3, 3], [3, 4], [3, 6], [4, 0], [4, 1], [4, 3], [4, 4], [4, 6], [5, 0], [5, 2], [5, 3], [5, 4], [5, 5], [6, 0], [6, 1], [6, 2], [6, 5], [6, 6]}

Тепер шукаємо дільники нуля:

```
> divisorsZero(K,astra,circ);
```

{[1, 3], [1, 4], [2, 1], [2, 6], [3, 2], [3, 5], [4, 2], [4, 5], [5, 1], [5, 6], [6, 3], [6, 4]}

Приклад 22.2. В кільці $\langle K; *, \circ\rangle$ впорядкованих пар (a, b), де $a, b \in \mathbb{Z}_7$, в якому операції $*$ і $\circ$ задані наступним чином:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (-ac, bd);\end{aligned}$$

знайти всі дільники нуля і, якщо є одиничний елемент, знайти всі дільники одиниці.

Розв'язання. Нульовий елемент цього кільця (тобто елемент, нейтральний відносно операції $*$) було знайдено при розв'язанні Прикладу 22.1. Знайдемо дільники нуля в K. Нехай (a, b) – довільний дільник нуля в K. Тоді $(a, b) \neq (\overline{0}, \overline{0})$ і в K існує елемент $(m, n) \neq (\overline{0}, \overline{0})$ такий, що

$$(a,b) \circ (m,n) = (\overline{0}, \overline{0}) \text{ або } (m,n) \circ (a,b) = (\overline{0}, \overline{0}). \qquad \text{(III.2)}$$

Неважко показати, що операція $\circ$ – комутативна на K, тому достатньо розглядати лише одну рівність. З першої рівності маємо: $(-am, bn) = (\overline{0}, \overline{0})$, тоді $-am = \overline{0}$, $bn = \overline{0}$. Можливі випадки: а) $a \neq \overline{0}$; б) $a = \overline{0}$.

а) Нехай $a \neq \overline{0}$. Тоді із умови $-am = \overline{0}$ випливає, що $m = \overline{0}$ (оскільки $\mathbb{Z}_7$ – поле і в $\mathbb{Z}_7$ дільників нуля немає), значить, $n \neq \overline{0}$. Але тоді $b = \overline{0}$. Отже, в такому випадку дільником нуля може бути лише елемент $(a, \overline{0})$. Навпаки, для елемента $(a, \overline{0})$, де $a \neq \overline{0}$, елемент $(\overline{0}, n)$, де $n \neq \overline{0}$, який задовольняє

умову (III.2), завжди існує. Отже, елемент $(a, \overline{0})$, де $a \neq \overline{0}$, є дільником нуля в K.

б) Нехай $a = \overline{0}$, тоді $b \neq \overline{0}$. Для елемента $(\overline{0}, b)$ елемент $(m, \overline{0})$, де $m \neq \overline{0}$, який задовольняє умову (III.2), завжди існує. Таким чином, дільником нуля в K є і кожен елемент $(\overline{0}, b)$, де $b \neq \overline{0}$.

Отже, дільниками нуля в K є елементи $(a, \overline{0})$, де $a \neq \overline{0}$, $(\overline{0}, b)$, де $b \neq \overline{0}$. Інших дільників нуля в K немає.

Визначимо, чи має кільце K одиничний елемент. Нехай (x, y) – одиничний елемент кільця K. Тоді для довільного $(a, b) \in K$ справедливо, що $(a, b) \circ (x, y) = (a, b)$. Маємо: $(-ax, by) = (a, b)$, звідси $-ax = a$, $by = b$. В силу довільності a, b в $\mathbb{Z}_7$, $x = -a^{-1}a = -\overline{1} = \overline{6}$, $y = \overline{1}$, отже, $(\overline{6}, \overline{1})$ – одиничний елемент кільця K.

Знайдемо дільники одиниці кільця K. Нехай (a, b) – дільник одиниці в K, тоді в K існує елемент (m, n) такий, що $(a, b) \circ (m, n) = (\overline{6}, \overline{1})$. Тоді $(-am, bn) = (\overline{6}, \overline{1})$, звідси $-am = \overline{6}$, $bn = \overline{1}$. Перше рівняння має в $\mathbb{Z}_7$ розв'язки тоді і лише тоді, коли $a \neq \overline{0}$, друге – тоді і лише тоді, коли $b \neq \overline{0}$, а саме: $m = a^{-1}$, $n = b^{-1}$. Отже, дільником одиниці є кожен елемент (a, b) кільця K, де $a \neq \overline{0}$, $b \neq \overline{0}$.

Зауваження 2. Як відомо, дільник одиниці кільця не може бути дільником нуля. Тому, знайшовши дільники нуля кільця K із Прикладу 22.2, можна при пошуку дільників одиниці виключити елементи $(a, \overline{0})$, де $a \neq \overline{0}$, $(\overline{0}, b)$, де $b \neq \overline{0}$, а також нульовий елемент $(\overline{0}, \overline{0})$ із розгляду (тобто шукати дільники одиниці лише серед елементів (a, b), $a \neq \overline{0}$, $b \neq \overline{0}$. Зауважимо, що в Прикладі 22.2 кожен елемент такого виду є дільником одиниці, але в загальному вмпадку це не так: в кільці можуть існувати елементи, відмінні від дільників нуля, нульового елемента і дільників одиниці (елементарним прикладом такого кільця є кільце $\mathbb{Z}$ цілих чисел).

Розв'язання в Maple. Задаємо множину і операції:

```
> K:={seq(seq([a,b],a=0..6),b=0..6)}:
> astra:=(X,Y)->[(X[1]+Y[1]) mod 7,(X[2]+Y[2]) mod 7]:
> circ:=(X, Y) -> [(-X[1]*Y[1]) mod 7,(X[2]*Y[2]) mod 7]:
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Знаходимо дільники одиниці в K:

```
> divisorsId(K,circ);
```

{[1, 1], [1, 2], [1, 3], [1, 4], [1, 5], [1, 6], [2, 1], [2, 2], [2, 3], [2, 4], [2, 5], [2, 6], [3, 1], [3, 2], [3, 3], [3, 4], [3, 5], [3, 6], [4, 1], [4, 2], [4, 3], [4, 4], [4, 5], [4, 6], [5, 1], [5, 2], [5, 3], [5, 4], [5, 5], [5, 6], [6, 1], [6, 2], [6, 3], [6, 4], [6, 5], [6, 6]}

Тепер знаходимо дільники нуля в K:

```
> divisorsZero(K,astra,circ);
```

$$\{[0,\ 1],\ [0,\ 2],\ [0,\ 3],\ [0,\ 4],\ [0,\ 5],\ [0,\ 6],\ [1,\ 0],\ [2,\ 0],\ [3,\ 0],\ [4,\ 0],\ [5,\ 0],\ [6,\ 0]\}$$

Приклад 22.3. В кільці $\langle K; *, \circ\rangle$ впорядкованих пар (a, b), де $a, b \in \mathbb{Z}_8$, в якому операції $*$ і $\circ$ задані наступним чином:

$$\begin{aligned}(a, b) * (c, d) &= (a + c, b + d),\\ (a, b) \circ (c, d) &= (ac, bd);\end{aligned}$$

знайти всі дільники нуля і, якщо є одиничний елемент, знайти всі дільники одиниці.

Розв'язання. Нульовим елементом цього кільця є елемент $(\overline{0}, \overline{0})$. Дійсно, для довільного $(a, b) \in K$ справедливо, що $(a, b) * (\overline{0}, \overline{0}) = (\overline{0}, \overline{0}) * (a, b) = (a, b)$. Знайдемо дільники нуля кільця K. Нехай (a, b) – довільний дільник нуля в K. Тоді $(a, b) \neq (\overline{0}, \overline{0})$ і в K існує елемент $(m, n) \neq (\overline{0}, \overline{0})$ такий, що

$$(a, b) \circ (m, n) = (\overline{0}, \overline{0}) \text{ або } (m, n) \circ (a, b) = (\overline{0}, \overline{0}). \qquad \text{(III.3)}$$

Неважко показати, що операція $\circ$ – комутативна на K, тому достатньо розглядати лише одну рівність. З першої рівності маємо: $(am, bn) = (\overline{0}, \overline{0})$, тоді $am = \overline{0}$, $bn = \overline{0}$. Можливі випадки: а) $a = \overline{0}$, б) $a \neq \overline{0}$. Розглянемо їх.

а) Нехай $a = \overline{0}$. Тоді $b \neq \overline{0}$. Елемент $(\overline{0}, b)$ є дільником нуля в K, оскільки завжди існує елемент $(m, \overline{0})$, де $m \neq \overline{0}$, який задовольняє умову (III.3).

б) Нехай $a \neq \overline{0}$. Тоді із умови $am = \overline{0}$ випливає, що або a і m – дільники нуля в $\mathbb{Z}_8$, або $m = \overline{0}$. Якщо a – дільник нуля в $\mathbb{Z}_8$, то кожен елемент $(m, \overline{0})$, де m – дільник нуля в $\mathbb{Z}_8$, задовольняє умову (III.3). Отже, елемент (a, b), де a – дільник нуля в $\mathbb{Z}_8$, є дільником нуля в K.

Якщо ж a не є дільником нуля в $\mathbb{Z}_8$, то $m = \overline{0}$, а значить, $n \neq \overline{0}$. Тоді b і n – дільники нуля в $\mathbb{Z}_8$. Отже, в цьому випадку дільник нуля в K може мати лише вигляд (a, b), де b – дільник нуля в $\mathbb{Z}_8$. Оскільки елемент $(\overline{0}, n)$, де n – дільник нуля в $\mathbb{Z}_8$, завжди існує в K, то кожен елемент (a, b), де b – дільник нуля в $\mathbb{Z}_8$, є дільником нуля в K.

Таким чином, дільниками нуля кільця K є: $(\overline{0}, b)$, де $b \neq \overline{0}$; $(a, \overline{0})$, де $a \neq \overline{0}$; (a, b), де a або b – дільник нуля в $\mathbb{Z}_8$. Інших дільників нуля в K немає.

Одиничним елементом кільця K є елемент $(\overline{1}, \overline{1})$, оскільки для довільного $(a, b) \in K$ справедливо, що $(a, b) \circ (\overline{1}, \overline{1}) = (\overline{1}, \overline{1}) \circ (a, b) = (a, b)$.

Знайдемо дільники одиниці кільця K. Нехай (a,b) – дільник одиниці в K, тоді для деякого $(m,n) \in K$ справедливо, що $(a,b) \circ (m,n) = (\overline{1},\overline{1})$. Звідси, $(am,bn) = (\overline{1},\overline{1})$. Отже, a і b – дільники одиниці в $\mathbb{Z}_8$. Таким чином, дільником одиниці є кожен елемент (a,b) кільця K, де $a,b \in \{\overline{1},\overline{3},\overline{5}\}$.

Розв'язання в Maple. Задаємо кільце і операції:

```
> K:={seq(seq([a,b],a=0..7),b=0..7)}:
> astra:=(X,Y)->[(X[1]+Y[1]) mod 8,(X[2]+Y[2]) mod 8]:
> circ:=(X, Y) -> [(X[1]*Y[1]) mod 8,(X[2]*Y[2]) mod 8]:
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Знаходимо дільники одиниці в K:

```
> divisorsId(K,circ);
```

{[1, 1], [1, 3], [1, 5], [1, 7], [3, 1], [3, 3], [3, 5], [3, 7], [5, 1], [5, 3], [5, 5], [5, 7], [7, 1], [7, 3], [7, 5], [7, 7]}

і дільники нуля:

```
> divisorsZero(K,astra,circ);
```

{[0, 1], [0, 2], [0, 3], [0, 4], [0, 5], [0, 6], [0, 7], [1, 0], [1, 2], [1, 4], [1, 6], [2, 0], [2, 1], [2, 2], [2, 3], [2, 4], [2, 5], [2, 6], [2, 7], [3, 0], [3, 2], [3, 4], [3, 6], [4, 0], [4, 1], [4, 2], [4, 3], [4, 4], [4, 5], [4, 6], [4, 7], [5, 0], [5, 2], [5, 4], [5, 6], [6, 0], [6, 1], [6, 2], [6, 3], [6, 4], [6, 5], [6, 6], [6, 7], [7, 0], [7, 2], [7, 4], [7, 6]}

Завдання 22. В кільці $\langle K; *, \circ \rangle$ знайти всі дільники нуля і, якщо є одиничний елемент, знайти всі дільники одиниці, якщо:

22.1. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (ac, \overline{2}bd).\end{aligned}$$

22.2. K – множина пар (a,b), де $a,b \in \mathbb{Z}_7$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.3. K – множина пар (a,b), де $a,b \in \mathbb{Z}_9$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.4. K – множина пар (a,b), де $a,b \in \mathbb{Z}_6$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (0,\overline{3}bd).\end{aligned}$$

22.5. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (ac+\overline{2}bd,ad+bc).\end{aligned}$$

22.6. K – множина пар (a,b), де $a,b \in \mathbb{Z}_9$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (bd,\overline{3}bd).\end{aligned}$$

22.7. K – множина пар (a,b), де $a,b \in \mathbb{Z}_3$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (-ac,\overline{2}bd).\end{aligned}$$

22.8. K – множина пар (a,b), де $a,b \in \mathbb{Z}_7$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.9. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (bd,\overline{2}bd).\end{aligned}$$

22.10. K – множина пар (a,b), де $a,b \in \mathbb{Z}_8$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.11. K – множина пар (a,b), де $a,b \in \mathbb{Z}_6$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (\overline{0}, \overline{0}).\end{aligned}$$

22.12. K – множина пар (a,b), де $a,b \in \mathbb{Z}_6$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (\overline{0}, ac).\end{aligned}$$

22.13. K – множина пар (a,b), де $a,b \in \mathbb{Z}_8$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (bd, \overline{2}bd).\end{aligned}$$

22.14. K – множина пар (a,b), де $a,b \in \mathbb{Z}_{10}$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (ac-\overline{6}bd, ad+bc).\end{aligned}$$

22.15. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (-ac, \overline{2}bd).\end{aligned}$$

22.16. K – множина пар (a,b), де $a,b \in \mathbb{Z}_8$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b) * (c,d) &= (a+c, b+d),\\ (a,b) \circ (c,d) &= (\overline{0}, \overline{3}bd).\end{aligned}$$

22.17. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.18. K – множина пар (a,b), де $a,b \in \mathbb{Z}_6$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (bd,\overline{3}bd).\end{aligned}$$

22.19. K – множина пар (a,b), де $a,b \in \mathbb{Z}_2$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.20. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

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

22.21. K – множина пар (a,b), де $a,b \in \mathbb{Z}_7$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (ac-\overline{2}bd,ad+bc).\end{aligned}$$

22.22. K – множина пар (a,b), де $a,b \in \mathbb{Z}_5$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (\overline{0},\overline{2}bd).\end{aligned}$$

22.23. K – множина пар (a,b), де $a,b \in \mathbb{Z}_8$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (-ac,\overline{2}bd).\end{aligned}$$

22.24. K – множина пар (a,b), де $a,b \in \mathbb{Z}_6$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (ac+\overline{2}bd,ad+bc).\end{aligned}$$

22.25. K – множина пар (a,b), де $a,b \in \mathbb{Z}_3$, і для довільних $(a,b),(c,d) \in K$ справедливо:

$$\begin{aligned}(a,b)*(c,d) &= (a+c,b+d),\\ (a,b)\circ(c,d) &= (\overline{0},\overline{2}ac).\end{aligned}$$

Приклад 23.1. Визначити, чи ділиться в кільці $\mathbb{Z}[\sqrt{3}]$:
а) елемент $17-10\sqrt{3}$ на елемент $2-\sqrt{3}$;
б) елемент $2+5\sqrt{3}$ на елемент $1-2\sqrt{3}$.

Розв'язання. Спосіб I. а) За означенням елемент $2-\sqrt{3}$ ділить елемент $17-10\sqrt{3}$, якщо в $\mathbb{Z}[\sqrt{3}]$ знайдеться такий елемент $x+y\sqrt{3}$, що $17-10\sqrt{3} = (2-\sqrt{3})(x+y\sqrt{3})$. Розкривши дужки в правій частині рівності, маємо:

$$17-10\sqrt{3} = (2x-3y)+(2y-x)\sqrt{3}.$$

Враховуючи умову рівності двох чисел із $\mathbb{Z}[\sqrt{3}]$, отримуємо систему:

$$\begin{cases} 17 = 2x-3y,\\ -10 = 2y-x.\end{cases}$$

Дана система рівнянь має розв'язок в цілих числах: $x=4$, $y=-3$, тому $x+y\sqrt{3} = 4-3\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, отже, $(17-10\sqrt{3}) \vdots (2-\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

б) Припустимо, що в кільці $\mathbb{Z}[\sqrt{3}]$ знайдеться такий елемент $x+y\sqrt{3}$, що

$$2+5\sqrt{3} = (1-2\sqrt{3})(x+y\sqrt{3}). \qquad \text{(III.4)}$$

Тоді, розкривши дужки, маємо: $2+5\sqrt{3} = (x-6y)+(y-2x)\sqrt{3}$. Звідси,

$$\begin{cases} 2 = x-6y,\\ 15 = y-2x.\end{cases}$$

Оскільки дана система рівнянь розв'язків в цілих числах не має, то в $\mathbb{Z}[\sqrt{3}]$ немає такого елемента $x+y\sqrt{3}$, який би задовольняв (III.4). Отже, $(2+5\sqrt{3}) \,\overline{\vdots}\, (1-2\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

Спосіб II. Кільце $\mathbb{Z}[\sqrt{3}]$ є підкільцем поля $\mathbb{R}$ дійсних чисел. Оскільки в полі кожний ненульовий елемент є дільником будь-якого іншого елемента цього поля (тобто операція ділення на ненульовий елемент завжди здійсненна), то в $\mathbb{R}$ знайдеться (причому єдине!) число z таке, що

$$17 - 10\sqrt{3} = (2 - \sqrt{3})z. \tag{III.5}$$

Знайдемо це число:

$$z = \frac{17 - 10\sqrt{3}}{2 - \sqrt{3}} = \frac{\left(17 - 10\sqrt{3}\right)\left(2 + \sqrt{3}\right)}{\left(2 - \sqrt{3}\right)\left(2 + \sqrt{3}\right)} = \frac{4 - 3\sqrt{3}}{4 - 3} = 4 - 3\sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

Таким чином, $z \in \mathbb{Z}[\sqrt{3}]$, значить, в $\mathbb{Z}[\sqrt{3}]$ виконується рівність (III.5), отже, $(17 - 10\sqrt{3}) \vdots (2 - \sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

б) Аналогічно отримуємо:

$$z = \frac{2 + 5\sqrt{3}}{1 - 2\sqrt{3}} = \frac{\left(2 + 5\sqrt{3}\right)\left(1 + 2\sqrt{3}\right)}{\left(1 - 2\sqrt{3}\right)\left(1 + 2\sqrt{3}\right)} = \frac{32 + 9\sqrt{3}}{-11} = -\frac{32}{11} - \frac{9}{11}\sqrt{3} \notin \mathbb{Z}[\sqrt{3}].$$

Таким чином, в $\mathbb{Z}[\sqrt{3}]$ не існує такого елемента z, що $2+5\sqrt{3} = (1-2\sqrt{3})z$. Це означає, що $(2 + 5\sqrt{3}) \vdots (1 - 2\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

Розв'язання в Maple. Використаємо спосіб II розв'язання: знайдемо частку елементів a і b в полі $\mathbb{R}$. Щоб позбавитись від ірраціональності в знаменнику дробу **z**, використаємо команду **rationalize(z)**. Для перетворення отриманого результату **r** із добутку в суму застосуємо команду **expand(r)** (§6 розд.I).

```
> z:=(17-10*sqrt(3))/(2-sqrt(3));
```

$$z := \frac{17 - 10\sqrt{3}}{2 - \sqrt{3}}$$

```
> rationalize(z);
```

$$-(-17 + 10\sqrt{3})(2 + \sqrt{3})$$

```
> expand(%);
```

$$4 - 3\sqrt{3}$$

Оскільки одержана частка z належить до кільця $\mathbb{Z}[\sqrt{3}]$, то $(17 - 10\sqrt{3}) \vdots (2 - \sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

Аналогічно,

```
> z:=(2+5*sqrt(3))/(1-2*sqrt(3));
```

$$z := \frac{2+5\sqrt{3}}{1-2\sqrt{3}}$$

```
> expand(rationalize(z));
```

$$-\frac{32}{11} - \frac{9\sqrt{3}}{11}$$

Оскільки одержана частка z не належить до кільця $\mathbb{Z}[\sqrt{3}]$, то $(2+5\sqrt{3}) \vdots (1-2\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

Для перевірки, чи належить отримана частка z до кільця $\mathbb{Z}[\sqrt{3}]$ в Maple можна (навіть не знаходячи самої частки), використати команду **patmatch(z,pattern)**, де **pattern** (англ. „шаблон, зразок") – певна форма запису. Результатом цієї команди є true, якщо вдається записати z у вигляді pattern. Для задання pattern використовують змінні, їхній тип зазначається після знаку :: (наприклад, запис x::realcons означає, що змінна x повинна мати тип realcons).

а) Задаємо числа:

```
> a:=17-10*sqrt(3):
  b:=2-sqrt(3):
```

Далі знаходимо частку z і перевіряємо, чи можна її записати у вигляді $x+y\sqrt{3}$, де $x, y \in \mathbb{Z}$:

```
> z:=expand(rationalize(a/b)):
  patmatch(z,x::integer+y::integer*sqrt(3));
```

true

Отже, частка z належить до кільця $\mathbb{Z}[\sqrt{3}]$, значить, $(17-10\sqrt{3}) \vdots (2-\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

б) Аналогічно:

```
> a:=2+5*sqrt(3):
  b:=1-2*sqrt(3):
  z:=expand(rationalize(a/b)):
  patmatch(z,x::integer+y::integer*sqrt(3));
```

false

Отже, $(2+5\sqrt{3}) \vdots (1-2\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$.

Приклад 23.2. Визначити, чи ділиться в кільці $\mathbb{Z}[\sqrt[3]{2}]$ елемент $a = 21+14\sqrt[3]{2}-2\sqrt[3]{4}$ на елемент $b = 4-\sqrt[3]{2}$;

Розв'язання. Спосіб I. Припустимо, що $a \vdots b$ в кільці $\mathbb{Z}[\sqrt[3]{2}]$. Тоді в $\mathbb{Z}[\sqrt[3]{2}]$ існує елемент $x+y\sqrt[3]{2}+z\sqrt[3]{4}$, $x, y, z \in \mathbb{Z}$, такий, що: $21+14\sqrt[3]{2}-2\sqrt[3]{4} =$

$(4-\sqrt[3]{2})(x+y\sqrt[3]{2}+z\sqrt[3]{4})$. Розкриємо дужки в правій частині рівності:

$$21+14\sqrt[3]{2}-2\sqrt[3]{4}=(4x-2z)+(-x+4y)\sqrt[3]{2}+(-y+4z)\sqrt[3]{4}.$$

В кільці $\mathbb{Z}[\sqrt[3]{2}]$ кожен елемент можна лише єдиним чином представити у вигляді $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, де $a,b,c\in\mathbb{Z}$, тому остання рівність можлива лише у випадку, коли:

$$\begin{cases} 4x-2z &= 21,\\ -x+4y &= 14,\\ -y+4z &= -2. \end{cases}$$

Єдиним розв'язком цієї системи є: $x=\frac{174}{31}$, $y=\frac{152}{31}$, $z=\frac{45}{62}$, що суперечить вибору x,y,z. Отже, припущення невірне і $a\,\vdots\, b$ в $\mathbb{Z}[\sqrt[3]{2}]$.

Спосіб II. Знайдемо частку елементів a і b в полі $\mathbb{R}$:

$$z=\frac{21+14\sqrt[3]{2}-2\sqrt[3]{4}}{4-\sqrt[3]{2}}.$$

Для цього домножимо чисельник і знаменник дробу на елемент $16+4\sqrt[3]{2}+\sqrt[3]{4}$:

$$z=\frac{21+14\sqrt[3]{2}-2\sqrt[3]{4}}{4-\sqrt[3]{2}}=\frac{(21+14\sqrt[3]{2}-2\sqrt[3]{4})(16+4\sqrt[3]{2}+\sqrt[3]{4})}{(4-\sqrt[3]{2})(16+4\sqrt[3]{2}+\sqrt[3]{4})}=$$
$$=\frac{348+304\sqrt[3]{2}+45\sqrt[3]{4}}{4^3-2}=\frac{174}{31}+\frac{152}{31}\sqrt[3]{2}+\frac{45}{62}\sqrt[3]{4}.$$

Оскільки частка z елементів a і b до кільця $\mathbb{Z}[\sqrt[3]{2}]$ не належить, то $a\,\vdots\, b$ в $\mathbb{Z}[\sqrt[3]{2}]$.

Розв'язання в Maple. Радикал $\sqrt[3]{2}$ в Maple вводимо у форматі: **root[3](2)**. Все інше аналогічно до попереднього прикладу.

Знаходимо частку z і перевіряємо, чи можна її записати у вигляді $x+y\sqrt[3]{2}+u\sqrt[3]{4}$, де $x,y,u\in\mathbb{Z}$:

```
> a:=21+14*root[3](2)-2*root[3](4):
  b:=4-root[3](2):
> z:=expand(rationalize(a/b)):
  patmatch(z,x::integer+y::integer*root[3](2)+
                                    u::integer*root[3](4));
```

false

Отже, частка z не належить до кільця $\mathbb{Z}[\sqrt[3]{2}]$, значить, $a\,\vdots\, b$ в $\mathbb{Z}[\sqrt[3]{2}]$.

Завдання 23. Визначити, чи ділиться:

23.1. а) елемент $21 + 14\sqrt{3}i$ на елемент $4 - \sqrt{3}i$;
б) елемент $22 + 3\sqrt{3}i$ на елемент $5 + 4\sqrt{3}i$
в кільці $\mathbb{Z}[\sqrt{3}i]$.

23.2. а) елемент $40 - 73i$ на елемент $11 + i$;
б) елемент $75 + 40i$ на елемент $6 - 7i$
в кільці $\mathbb{Z}[i]$.

23.3. а) елемент $-13 + 12\sqrt{5}$ на елемент $8 - 3\sqrt{5}$;
б) елемент $-3 + \sqrt{5}$ на елемент $1 - 2\sqrt{5}$
в кільці $\mathbb{Z}[\sqrt{5}]$.

23.4. а) елемент $5 - \sqrt[3]{3} - 2\sqrt[3]{9}$ на елемент $1 - \sqrt[3]{3}$;
б) елемент $6 - 4\sqrt[3]{9}$ на елемент $2 + \sqrt[3]{3}$
в кільці $\mathbb{Z}[\sqrt[3]{3}]$.

23.5. а) елемент $15 + 7\sqrt{3}$ на елемент $3 + 2\sqrt{3}$;
б) елемент $-6 + 5\sqrt{3}$ на елемент $3 + 7\sqrt{3}$
в кільці $\mathbb{Z}[\sqrt{3}]$.

23.6. а) елемент $91 - 32\sqrt{7}$ на елемент $7 - 3\sqrt{7}$;
б) елемент $-165 + \sqrt{7}$ на елемент $3 - 8\sqrt{7}$
в кільці $\mathbb{Z}[\sqrt{7}]$.

23.7. а) елемент $-13 - 11\sqrt{11}$ на елемент $4 - 3\sqrt{11}$;
б) елемент $-52 + 6\sqrt{11}$ на елемент $5 - 2\sqrt{11}$
в кільці $\mathbb{Z}[\sqrt{11}]$.

23.8. а) елемент $-5 + 4\sqrt{2}$ на елемент $1 + 2\sqrt{2}$;
б) елемент $-47 + 9\sqrt{2}$ на елемент $3 + 7\sqrt{2}$
в кільці $\mathbb{Z}[\sqrt{2}]$.

23.9. а) елемент $30 + 16\sqrt[3]{7} + 9\sqrt[3]{49}$ на елемент $5 + 2\sqrt[3]{7}$;
б) елемент $13 - 11\sqrt[3]{7}$ на елемент $3 - \sqrt[3]{7}$
в кільці $\mathbb{Z}[\sqrt[3]{7}]$.

23.10. а) елемент $41 - 19\sqrt{5}i$ на елемент $3 + \sqrt{5}i$;
б) елемент $-134 - 29\sqrt{5}i$ на елемент $2 - 7\sqrt{5}i$
в кільці $\mathbb{Z}[\sqrt{5}i]$.

23.11. а) елемент $11 - 3\sqrt{3}$ на елемент $-14 + \sqrt{3}$;
б) елемент $-54 + 7\sqrt{3}$ на елемент $2 + 5\sqrt{3}$
в кільці $\mathbb{Z}[\sqrt{3}]$.

23.12. а) елемент $25 - 5\sqrt{11}i$ на елемент $7 + \sqrt{11}i$;
б) елемент $44 - 5\sqrt{11}i$ на елемент $4 - 3\sqrt{11}i$
в кільці $\mathbb{Z}[\sqrt{11}i]$.

23.13. а) елемент $-151 + 43\sqrt{7}$ на елемент $5 + 7\sqrt{7}$;
б) елемент $-12 - 10\sqrt{7}$ на елемент $2 - 3\sqrt{7}$
в кільці $\mathbb{Z}[\sqrt{7}]$.

23.14. а) елемент $45 - 10\sqrt{5}$ на елемент $3 - \sqrt{5}$;
б) елемент $-159 + 26\sqrt{5}$ на елемент $8 - 7\sqrt{5}$
в кільці $\mathbb{Z}[\sqrt{5}]$.

23.15. а) елемент $19 + 2\sqrt{2}i$ на елемент $5 + 7\sqrt{2}i$;
б) елемент $34 + 44\sqrt{2}i$ на елемент $6 - \sqrt{2}i$
в кільці $\mathbb{Z}[\sqrt{2}i]$.

23.16. а) елемент $-25 + 3\sqrt{3}$ на елемент $7 - 5\sqrt{3}$;
б) елемент $16 + 7\sqrt{3}$ на елемент $-5 + 4\sqrt{3}$
в кільці $\mathbb{Z}[\sqrt{3}]$.

23.17. а) елемент $46 + 25\sqrt{5}i$ на елемент $4 - \sqrt{5}i$;
б) елемент $31 + 13\sqrt{5}i$ на елемент $2 + 5\sqrt{5}i$
в кільці $\mathbb{Z}[\sqrt{5}i]$.

23.18. а) елемент $48 + 9\sqrt{2}$ на елемент $-3 + 7\sqrt{2}$;
б) елемент $56 + 25\sqrt{2}$ на елемент $3 + 5\sqrt{2}$
в кільці $\mathbb{Z}[\sqrt{2}]$.

23.19. а) елемент $9+19\sqrt[3]{5}+4\sqrt[3]{25}$ на елемент $7-\sqrt[3]{5}$;
б) елемент $9-2\sqrt[3]{5}+8\sqrt[3]{25}$ на елемент $2+3\sqrt[3]{5}$
в кільці $\mathbb{Z}[\sqrt[3]{5}]$.

23.20. а) елемент $67+8\sqrt{3}i$ на елемент $2+7\sqrt{3}i$;
б) елемент $98-24\sqrt{3}i$ на елемент $3-7\sqrt{3}i$
в кільці $\mathbb{Z}[\sqrt{3}i]$.

23.21. а) елемент $93-7\sqrt{7}i$ на елемент $5+4\sqrt{7}i$;
б) елемент $29-10\sqrt{7}i$ на елемент $2-3\sqrt{7}i$
в кільці $\mathbb{Z}[\sqrt{7}i]$.

23.22. а) елемент $47-\sqrt{5}$ на елемент $11+3\sqrt{5}$;
б) елемент $-99-2\sqrt{5}$ на елемент $2+3\sqrt{5}$
в кільці $\mathbb{Z}[\sqrt{5}]$.

23.23. а) елемент $-45+\sqrt{11}$ на елемент $3+7\sqrt{11}$;
б) елемент $-269+5\sqrt{11}$ на елемент $2+5\sqrt{11}$
в кільці $\mathbb{Z}[\sqrt{11}]$.

23.24. а) елемент $22-\sqrt{3}$ на елемент $4-3\sqrt{3}$;
б) елемент $-55-2\sqrt{3}$ на елемент $4-7\sqrt{3}$
в кільці $\mathbb{Z}[\sqrt{3}]$.

23.25. а) елемент $51+9i$ на елемент $5-8i$;
б) елемент $20-17i$ на елемент $2-3i$
в кільці $\mathbb{Z}[i]$.

3. Ідеали кільця

ТЕОРЕТИЧНІ ВІДОМОСТІ

Означення (ідеалу)**.** Підкільце I кільця $\langle K;*,\circ\rangle$ називається лівим (відповідно правим) ідеалом цього кільця, якщо для будь-яких елементів $a\in I$ і $x\in K$ добуток $x\circ a$ (відповідно $a\circ x$) міститься в I.

Підмножина I кільця K, яка є одночасно лівим і правим ідеалом цього кільця, називається **двостороннім ідеалом** або просто **ідеалом** кільця K. У комутативному кільці кожен лівий і правий ідеал є двостороннім.

Одиничним ідеалом кільця K називається кільце K. **Нульовим ідеалом** кільця K називаєть нульове підкільце.

Теорема (критерій ідеалу)**.** *Непорожня підмножина I кільця $\langle K; *, \circ\rangle$ є лівим (відповідно правим) ідеалом цього кільця, якщо виконуються наступні умови:*

1) *операція $*$ є замкненою на I;*
2) *для довільного $a \in I$ елемент, симетричний до нього відносно операції $*$ в K, також належить до I;*
3) *для довільного $a \in I$ і довільного $x \in K$ справедливо, що $x \circ a \in I$ (відповідно $a \circ x \in I$).*

Означення (головного ідеалу)**.** Нехай K – комутативне кільце з одиницею, a – довільний елемент із K. Ідеал $\langle a\rangle = aK = Ka = \{xa | x \in K\}$ називають головним ідеалом кільця K, породженим елементом a.

В кільці $\mathbb{Z}$ цілих чисел всі ідеали головні.

Нехай K – комутативне кільце, $a_1, a_2, ..., a_s \in K$. Ідеал

$$\langle a_1, a_2, \ldots, a_s\rangle = \{a_1x_1 + a_2x_2 + \ldots + a_sx_s | x_1, x_2, \ldots, x_s \in K\}$$

називається ідеалом кільця K, породженим елементами $a_1, a_2, \ldots, a_s$; зокрема, $\langle a_1, a_2\rangle = \{a_1x + a_2y | x, y \in K\}$ – ідеал, породжений елементами a_1, a_2.

Операції над ідеалами:

Перерізом ідеалів I_1 і I_2 кільця K називається множина $I_1 \cap I_2 \stackrel{\text{df}}{=} \{a | a \in I_1, a \in I_2\}$ їхніх спільних елементів.

Сумою ідеалів I_1 і I_2 кільця K називається множина $I_1 + I_2 \stackrel{\text{df}}{=} \{a + b | a \in I_1, b \in I_2\}$.

Добутком ідеалів I_1 і I_2 кільця K називається множина $I_1I_2 \stackrel{\text{df}}{=} \{a_1b_1 + a_2b_2 + ... + a_sb_s | s \in \mathbb{N}, a_i \in I_1, b_i \in I_2, 1 \leqslant i \leqslant s\}$.

Теорема. *Переріз $I_1 \cap I_2$, сума $I_1 + I_2$ і добуток I_1I_2 ідеалів I_1 і I_2 кільця K є ідеалами цього кільця.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 24.1. Визначити, чи є ідеалом множина

$$T = \left\{ \left(\begin{array}{cc} a & \overline{0} \\ b & \overline{0} \end{array} \right) \middle| \, a, b \in \mathbb{Z}_7 \right\}$$

в кільці $K = M_2(\mathbb{Z}_7)$ матриць 2-го порядку над полем $\mathbb{Z}_7$.

Розв'язання. Оскільки $\begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix} \in T$, то $T \neq \varnothing$. Далі $T \subseteq K$. Використаємо критерій ідеалу. Нехай $A_1 = \begin{pmatrix} a_1 & \overline{0} \\ b_1 & \overline{0} \end{pmatrix}$, $A_2 = \begin{pmatrix} a_2 & \overline{0} \\ b_2 & \overline{0} \end{pmatrix}$, $a_1, b_1, a_2, b_2 \in \mathbb{Z}_7$, – довільні два елементи із T. Тоді:

1) $A_1 + A_2 = \begin{pmatrix} a_1 & \overline{0} \\ b_1 & \overline{0} \end{pmatrix} + \begin{pmatrix} a_2 & \overline{0} \\ b_2 & \overline{0} \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & \overline{0} \\ b_1 + b_2 & \overline{0} \end{pmatrix} \in T$,

оскільки $a_1 + a_2 \in \mathbb{Z}_7$, $b_1 + b_2 \in \mathbb{Z}_7$;

2) $-A_1 = -\begin{pmatrix} a_1 & \overline{0} \\ b_1 & \overline{0} \end{pmatrix} = \begin{pmatrix} -a_1 & \overline{0} \\ -b_1 & \overline{0} \end{pmatrix} \in T$,

оскільки $-a_1, -b_1 \in \mathbb{Z}_7$;

3) Нехай тепер $A = \begin{pmatrix} a & \overline{0} \\ b & \overline{0} \end{pmatrix}$ – довільний елемент із T, $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ – довільний елемент із $M_2(\mathbb{Z}_7)$, $x, y, z, t \in \mathbb{Z}_7$. Тоді

$$XA = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} a & \overline{0} \\ b & \overline{0} \end{pmatrix} = \begin{pmatrix} xa + yb & \overline{0} \\ za + tb & \overline{0} \end{pmatrix} \in T,$$

оскільки $xa + yb \in \mathbb{Z}_7$, $za + tb \in \mathbb{Z}_7$.

$$AX = \begin{pmatrix} a & \overline{0} \\ b & \overline{0} \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax & ay \\ bx & by \end{pmatrix} \notin T \text{ при } ay \neq \overline{0} \text{ і } by \neq \overline{0}.$$

Отже, T є лівим і не є правим ідеалом кільця $M_2(\mathbb{Z}_7)$.

Розробка процедур. Для того, щоб непорожня множина T була ідеалом кільця $\langle K; *, \circ \rangle$, необхідно, щоб T була підмножиною множини K. Для перевірки, чи є множина A підмножиною множини B, використовують команду **subset**. Формат команди **A subset B** або **'subset'(A,B)**.

Для перевірки умови 1) критерію ідеалу використовуватимемо процедуру **isClosed** із Прикладу 21.1.

Для перевірки умови 2) критерію ідеалу створимо процедуру **belongsSym**. При цьому задаватимемо безпосередньо правило пошуку симетричного елемента (в якості параметра процедури). Зауважимо, що використання процедури **Sym** із Прикладу 21.1 для пошуку симетричного елемента в цьому випадку не є бажаним: воно призводить до досить громіздких тривалих обчислень.

В ході процедури **belongsSym** для всіх елементів $T[i]$ множини T послідовно перевіряємо, чи належить елемент c, симетричний до $T[i]$ в K відносно операції **operation1**:

```
> c:=symElement(T[i]);
```

до множини T:

```
> if member(c,T)=true
```

Якщо умова виконується, то переходимо до дослідження наступного елемента $T[i]$ множини T, якщо ж не виконується, перевірка закінчується (break). Якщо в результаті лічильник s набув значення, рівного t, то для всіх елементів $T[i]$ із T елемент, симетричний відносно операції **operation1** в K, належить до T.

Код процедури наступний:

```
belongsSym:=proc(T,symElement)
local i,s,t,c;
   t:=nops(T);
   s:=0;
   for i from 1 to t do
      c:=symElement(T[i]);
      if member(c,T)=true then s:=s+1; else break; end if;
   end do;
   evalb(s=t);
end proc:
```

Тепер створимо процедури для перевірки умови 3) критерію ідеалу. Процедура **belongsL** досліджуватиме добутки $q = x \circ a$, де $x = K[j]$, $a = T[i]$. Якщо добуток q належить до T:

```
> if member(q, T)=true
```

то розглядаємо наступну пару елементів $K[j]$ і $T[i]$.

Код процедури наступний:

```
belongsL:=proc(T,K,operation2)
local i,j,s,t,m,q;
   s:=0;
   t:=nops(K); m:=nops(T);
   for i from 1 to m do
      for j from 1 to t do
         q:=operation2(K[j],T[i]);
         if member(q, T)=true then s:=s+1; else break; end if;
      end do;
   end do;
   evalb(s=m*t);
end proc:
```

Аналогічна процедура **belongsR** досліджує добутки $a \circ x$, де $x = K[j]$, $a = T[i]$.

```
belongsR:=proc(T,K,operation2)
local i,j,s,t,m,q;
   s:=0;
   t:=nops(K); m:=nops(T);
   for i from 1 to m do
      for j from 1 to t do
         q:=operation2(T[i],K[j]);
         if member(q, T)=true then s:=s+1; else break; end if;
      end do;
   end do;
   evalb(s=m*t);
end proc:
```

На основі процедур **isClosed**, **belongsSym**, **belongsL**, **belongsR** можна створити процедуру **isIdeal** для перевірки, чи є задана множина T ідеалом кільця K із операціями **operation1,operation2**. Її код наступний:

```
isIdeal:=proc(T,K,operation1,symElement,operation2)
   if (T subset K=true) and isClosed(T,operation1)=true and
         belongsSym(T,symElement)=true then
      if belongsL(T,K,operation2)=true and
         belongsR(T,K,operation2)=true then return("ideal");
      elif belongsL(T,K,operation2)=true and
         belongsR(T,K,operation2)=false then return("livyi ideal");
      elif belongsL(T,K,operation2)=true and
         belongsR(T,K,operation2)=false then return("pravyi ideal");
      else return false
      end if;
   else return false
   end if;
end proc:
```

Розв'язання в Maple. Як було зазначено вище, Maple швидше оперує із об'єктами типу List, ніж із об'єктами типу Matrix, тому множини матриць (як і множини пар в Прикладі 21.1) також задаватимемо за допомогою списків:

```
> K:={seq(seq(seq(seq([[x,y],[z,t]],x=0..6),y=0..6),
                                        z=0..6),t=0..6)}:
```

Побачити всі елементи множини в звичному записі можна, ввівши команду:

```
> map(matrix,K);
```

Щоб побачити лише i-тий елемент множини K, вводимо **matrix(K[i])**, наприклад

```
> matrix(K[68]);
```

$$\begin{bmatrix} 0 & 1 \\ 2 & 4 \end{bmatrix}$$

Тепер задаємо операції додавання **mplus** і множення **mmult** матриць:

```
> mplus:=(A,B)->
  [[A[1,1]+B[1,1] mod 7, A[1,2]+B[1,2] mod 7],
  [A[2,1]+B[2,1] mod 7,A[2,2]+B[2,2] mod 7]]:
> mmult:=(A,B)->
  [[A[1,1]*B[1,1]+A[1,2]*B[2,1] mod 7,
  A[1,1]*B[1,2]+A[1,2]*B[2,2] mod 7],
  [A[2,1]*B[1,1]+A[2,2]*B[2,1] mod 7,
  A[2,1]*B[1,2]+A[2,2]*B[2,2] mod 7]]:
```

Далі задаємо множину T:

```
> T:={seq(seq([[a,0],[b,0]],a=0..6),b=0..6)}:
```

Перевіримо, чи виконується умова $T \subseteq K$:

```
> T subset K;
```

true

Отже, $T \subseteq K$. Тепер переходимо до перевірки умов 1)-3) критерію ідеалу. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Умова 1):

```
> isClosed(T,mplus);
```

true

Отже, операція додавання матриць замкнена на на T.

Умова 2):

Спочатку задаємо правило пошуку симетричного відносно операції **mplus** елемента. В кільці матриць протилежним елементом (симетричним відносно операції додавання матриць) до матриці $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ є матриця $\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$. Задаємо її:

```
> symElement:=A->
  [[-A[1,1] mod 7,-A[1,2]] mod 7,
  [-A[2,1] mod 7,-A[2,2] mod 7]]:
```

Застосовуємо процедуру **belongsSym**:

```
> belongsSym(T,symElement);
```

true

Отже, для кожного елемента із T елемент, протилежний до нього в K, належить до T.

Умова 3):

```
> belongsL(T,K,mmult);
```

$$true$$

Отже, $xa \in T$ для всіх $x \in K$, $a \in T$.

```
> belongsR(T,K,mmult);
```

$$false$$

Отже, існує хоча б один добуток ax, де $x \in K$, $a \in T$, який не належить до T.

```
> isIdeal(T,K,mplus,symElement,mmult);
```

$$"livyi\ ideal"$$

Таким чином, T є лівим і не є правим ідеалом кільця K.

Приклад 24.2. Визначити, чи є ідеалом множина

$$T = \left\{ \begin{pmatrix} \overline{0} & a \\ \overline{0} & \overline{0} \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_4 \right\}$$

в кільці $K = \left\{ \begin{pmatrix} c & d \\ \overline{0} & c \end{pmatrix} \middle| \, c, d \in \mathbb{Z}_n \right\}$ при: а) $n = 4$, б) $n = 5$.

Розв'язання. а) Маємо: $I \neq \varnothing$ і $T \subseteq K$. Використаємо критерій ідеалу. Нехай $A, B \in T$, тоді $A = \begin{pmatrix} \overline{0} & a \\ \overline{0} & \overline{0} \end{pmatrix}$, $B = \begin{pmatrix} \overline{0} & b \\ \overline{0} & \overline{0} \end{pmatrix}$, де $a, b \in \mathbb{Z}_4$. Тоді:

1) $A + B = \begin{pmatrix} \overline{0} & a \\ \overline{0} & \overline{0} \end{pmatrix} + \begin{pmatrix} \overline{0} & b \\ \overline{0} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{0} & a+b \\ \overline{0} & \overline{0} \end{pmatrix} \in T,$

оскільки $a + b \in \mathbb{Z}_4$;

2) $-A = -\begin{pmatrix} \overline{0} & a \\ \overline{0} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{0} & -a \\ \overline{0} & \overline{0} \end{pmatrix} \in T,$

оскільки $-a \in \mathbb{Z}_4$;

3) Нехай тепер X – довільний елемент із K, тоді $X = \begin{pmatrix} c & d \\ \overline{0} & c \end{pmatrix}$, де $x, y, z, t \in \mathbb{Z}_4$. Тоді

$$XA = \begin{pmatrix} c & d \\ \overline{0} & c \end{pmatrix} \begin{pmatrix} \overline{0} & a \\ \overline{0} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{0} & ca \\ \overline{0} & \overline{0} \end{pmatrix} \in T,$$

оскільки $ca \in \mathbb{Z}_4$.

$$AX = \begin{pmatrix} \overline{0} & a \\ \overline{0} & \overline{0} \end{pmatrix} \begin{pmatrix} c & d \\ \overline{0} & c \end{pmatrix} = \begin{pmatrix} \overline{0} & ac \\ \overline{0} & \overline{0} \end{pmatrix} \in T, \text{ оскільки } ca \in \mathbb{Z}_4.$$

Отже, T є ідеалом кільця K.

б) В цьому випадку множина T не є підмножиною множини K, а значить, T не є ідеалом в K.

Розв'язання в Maple. Повторюємо хід розв'язання Прикладу 24.1. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

а) Задаємо множину K і операції:

```
> K:={seq(seq([[c,d],[0,c]],c=0..3),d=0..3)}:
> mplus:=(A,B)->
  [[A[1,1]+B[1,1] mod 4,A[1,2]+B[1,2] mod 4],
  [A[2,1]+B[2,1] mod 4,A[2,2]+B[2,2] mod 4]]:
> mmult:=(A,B)->
  [[A[1,1]*B[1,1]+A[1,2]*B[2,1] mod 4,
  A[1,1]*B[1,2]+A[1,2]*B[2,2] mod 4],
  [A[2,1]*B[1,1]+A[2,2]*B[2,1] mod 4,
  A[2,1]*B[1,2]+A[2,2]*B[2,2] mod 4]]:
```

Далі задаємо множину T:

```
> T:={seq(seq([[0,a],[0,0]],a=0..3),b=0..3)}:
> T subset K;
```

true

Отже, $T \subseteq K$. Перевіряємо, чи виконуються умови 1)-3) критерію ідеалу:

```
> isClosed(T,mplus);
```

true

Операція додавання матриць замкнена на T.

Задаємо протилежний елемент:

```
> symElement:=A-> [[-A[1,1] mod 4,-A[1,2]] mod 4,
                   [-A[2,1] mod 4,-A[2,2] mod 4]]:
> belongsSym(T,symElement);
```

true

Таким чином, для довільного елемента із T протилежний до нього елемент в K належить до T.

```
> belongsL(T,K,mmult); belongsR(T,K,mmult);
```

true

true

Добутки xa і ax належать до T для всіх $x \in K$, $a \in T$.

```
> isIdeal(T,K,mplus,symElement,mmult);
```

"*ideal*"

Таким чином, T є ідеалом кільця K.

б) Кільце K і операції, задані на K, залишаються ті ж самі. Тому їх не потрібно вводити заново. Задаємо лише множину T:

```
> T:={seq(seq([[0,a],[0,0]],a=0..4),b=0..4)}:
```

Маємо:

```
> T subset K;
```

false

Отже, $T \not\subseteq K$, а значить, T не є ідеалом:

```
> isIdeal(T,K,mplus,symElement,mmult);
```

false

Приклад 24.3. Визначити, чи є ідеалом кільця $K = M_3(\mathbb{Z}_7)$ множина

$$T = \left\{ \left(\begin{array}{ccc} a & \overline{0} & \overline{0} \\ \overline{0} & a & \overline{0} \\ \overline{0} & \overline{0} & a \end{array} \right) \middle| \, a \in \mathbb{Z}_3 \right\}$$

.

Розв'язання. а) Маємо: $T \neq \varnothing$ і $T \subseteq K$. Використаємо критерій ідеалу. Нехай $A, B \in I$, тоді $A = \begin{pmatrix} a & \overline{0} & \overline{0} \\ \overline{0} & a & \overline{0} \\ \overline{0} & \overline{0} & a \end{pmatrix}$, $B = \begin{pmatrix} b & \overline{0} & \overline{0} \\ \overline{0} & b & \overline{0} \\ \overline{0} & \overline{0} & b \end{pmatrix}$, де $a, b \in \mathbb{Z}_3$. Тоді:

1) $A + B = \begin{pmatrix} a & \overline{0} & \overline{0} \\ \overline{0} & a & \overline{0} \\ \overline{0} & \overline{0} & a \end{pmatrix} + \begin{pmatrix} b & \overline{0} & \overline{0} \\ \overline{0} & b & \overline{0} \\ \overline{0} & \overline{0} & b \end{pmatrix} = \begin{pmatrix} a+b & \overline{0} & \overline{0} \\ \overline{0} & a+b & \overline{0} \\ \overline{0} & \overline{0} & a+b \end{pmatrix} \in T,$

оскільки $a + b \in \mathbb{Z}_3$;

2) $-A = -\begin{pmatrix} a & \overline{0} & \overline{0} \\ \overline{0} & a & \overline{0} \\ \overline{0} & \overline{0} & a \end{pmatrix} = \begin{pmatrix} -a & \overline{0} & \overline{0} \\ \overline{0} & -a & \overline{0} \\ \overline{0} & \overline{0} & -a \end{pmatrix} \in T$, оскільки $-a \in \mathbb{Z}_3$;

3) Нехай тепер X – довільний елемент із K, тоді $X = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}$,

де $x_i \in \mathbb{Z}_3$ для всіх $i \in \overline{1,7}$. Тоді

$$XA = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} \begin{pmatrix} a & \overline{0} & \overline{0} \\ \overline{0} & a & \overline{0} \\ \overline{0} & \overline{0} & a \end{pmatrix} = \begin{pmatrix} x_1a & x_2a & x_3a \\ x_4a & x_5a & x_6a \\ x_7a & x_8a & x_9a \end{pmatrix} \notin T,$$

при $x_ia \neq \overline{0}$, $i \in \{4, 7, 2, 8, 3, 6\}$.

$$AX = \begin{pmatrix} a & \overline{0} & \overline{0} \\ \overline{0} & a & \overline{0} \\ \overline{0} & \overline{0} & a \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} = \begin{pmatrix} ax_1 & ax_2 & ax_3 \\ ax_4 & ax_5 & ax_6 \\ ax_7 & ax_8 & ax_9 \end{pmatrix} \notin T,$$

при $ax_i \neq \overline{0}$, $i \in \{4, 7, 2, 8, 3, 6\}$.

Отже, T не є ні лівим, ні правим ідеалом кільця K.

Розв'язання в Maple. Задаємо множину K і операції додавання і множення матриць безпосередньо:

```
> K:={seq(seq(seq(seq(seq(seq(seq(seq(seq(
  [[x1,x2,x3],[x4,x5,x6],[x7,x8,x9]],x1=0..2),x2=0..2),x3=0..2),
  x4=0..2),x5=0..2),x6=0..2), x7=0..2),x8=0..2),x9=0..2)}:
> mplus:=(A,B)->
  [[A[1,1]+B[1,1] mod 3,A[1,2]+B[1,2] mod 3, A[1,3]+B[1,3] mod3],
  [A[2,1]+B[2,1] mod 3,A[2,2]+B[2,2] mod 3,A[2,3]+B[2,3] mod 3],
  [A[3,1]+B[3,1] mod 3,A[3,2]+B[3,2] mod 3,A[3,3]+B[3,3] mod 3]]:
> mmult:=(A,B)->
  [[A[1,1]*B[1,1]+A[1,2]*B[2,1]+A[1,3]*B[3,1] mod 3,
  A[1,1]*B[1,2]+A[1,2]*B[2,2]+A[1,3]*B[3,2] mod 3,
  A[1,1]*B[1,3]+A[1,2]*B[2,3]+A[1,3]*B[3,3] mod 3],
  [A[2,1]*B[1,1]+A[2,2]*B[2,1]+A[2,3]*B[3,1] mod 3,
  A[2,1]*B[1,2]+A[2,2]*B[2,2]+A[2,3]*B[3,2] mod 3,
  A[2,1]*B[1,3]+A[2,2]*B[2,3]+A[2,3]*B[3,3] mod 3],
  [A[3,1]*B[1,1]+A[3,2]*B[2,1]+A[3,3]*B[3,2] mod 3,
  A[3,1]*B[1,2]+A[3,2]*B[2,2]+A[3,3]*B[3,2] mod 3,
  A[3,1]*B[1,3]+A[3,2]*B[2,3]+A[1,3]*B[3,3] mod 3]]:
```

Далі задаємо множину T:

```
> T:={seq([[a,0,0],[0,a,0],[0,0,a]],a=0..2)}:
```

Тепер застосовуємо алгоритм розв'язання Прикладів 24.1. і 24.2.

```
> T subset K;
```

true

Отже, $T \subseteq K$. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> isClosed(T,mplus);
```

true

```
> symMatrix:=A->
  [[-A[1,1] mod 3,-A[1,2] mod 3,-A[1,3] mod 3],
  [-A[2,1] mod 3,-A[2,2] mod 3,-A[2,3] mod 3],
  [-A[3,1] mod 3,-A[3,2] mod 3,-A[3,3] mod 3]]:
> belongsSym(T,K,mplus);
```

true

```
> belongsL(T,K,mmult); belongsR(T,K,mmult);
```

false

false

```
> isIdeal(T,K,mplus,mmult);
```

false

Отже, T не є ні лівим, ні правим ідеалом кільця K.

Завдання 24. Визначити, чи є ідеалом кільця K множина T, якщо:

24.1. $T = \left\{ \begin{pmatrix} a & \overline{2}b \\ \overline{3}b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_7 \right\}$;

$K = \left\{ \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \middle| c, d \in \mathbb{Z}_7 \right\}$.

24.2. $T = \left\{ \begin{pmatrix} a & b & c \\ \overline{0} & a & b \\ \overline{0} & \overline{0} & a \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_3 \right\}$

$K = M_3(\mathbb{Z}_3)$ – кільце квадратних матриць 3-го порядку над полем $\mathbb{Z}_3$.

24.3. $T = \left\{ \begin{pmatrix} a & \overline{0} \\ \overline{0} & b \end{pmatrix} \middle| a, b \in \mathbb{Z}_5 \right\}$;

$K = M_2(\mathbb{Z}_5)$ – кільце квадратних матриць 2-го порядку над полем $\mathbb{Z}_5$.

24.4. $T = \left\{ \begin{pmatrix} \overline{2}a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_7 \right\}$;

$K = M_2(\mathbb{Z}_7)$ – кільце квадратних матриць 2-го порядку над полем $\mathbb{Z}_7$.

24.5. $T = \left\{ \begin{pmatrix} a & a \\ -a & a \end{pmatrix} \middle| a \in \mathbb{Z}_6 \right\}$;

$$K = \left\{ \left(\begin{array}{cc} c & d \\ -d & c \end{array} \right) \middle| \, c, d \in \mathbb{Z}_6 \right\}.$$

24.6. $T = \left\{ \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{array} \right) \middle| \, a \in \mathbb{Z}_4 \right\};$

$K = M_3(\mathbb{Z}_4)$ – кільце квадратних матриць 3-го порядку над кільцем $\mathbb{Z}_4$.

24.7. $T = \left\{ \left(\begin{array}{cc} a & \overline{3}b \\ \overline{4}b & a \end{array} \right) \middle| \, a, b \in \mathbb{Z}_7 \right\};$

$$K = \left\{ \left(\begin{array}{cc} c & d \\ -d & c \end{array} \right) \middle| \, c, d \in \mathbb{Z}_7 \right\}.$$

24.8. $T = \left\{ \left(\begin{array}{cc} a & \overline{2}b \\ \overline{2}b & a \end{array} \right) \middle| \, a, b \in \mathbb{Z}_4 \right\};$

$K = M_2(\mathbb{Z}_4)$ – кільце квадратних матриць 2-го порядку над кільцем $\mathbb{Z}_4$.

24.9. $T = \left\{ \left(\begin{array}{cc} a & b \\ \overline{0} & \overline{0} \end{array} \right) \middle| \, a, b \in \mathbb{Z}_8 \right\};$

$K = M_2(\mathbb{Z}_8)$ – кільце квадратних матриць 2-го порядку над кільцем $\mathbb{Z}_8$.

24.10. $T = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| \, a, b, c, d \in \mathbb{Z}_5^* \right\}$, де $\mathbb{Z}_5^*$ – множина дільників одиниці кільця $\mathbb{Z}_5$;

$K = M_2(\mathbb{Z}_5)$ – кільце квадратних матриць 2-го порядку над полем $\mathbb{Z}_5$.

24.11. $T = \left\{ \left(\begin{array}{cc} \overline{0} & a \\ -a & \overline{0} \end{array} \right) \middle| \, a \in \mathbb{Z}_3 \right\};$

$$K = \left\{ \left(\begin{array}{cc} c & d \\ -d & c \end{array} \right) \middle| \, c, d \in \mathbb{Z}_3 \right\}.$$

24.12. $T = \left\{ \left(\begin{array}{cc} a & \overline{0} \\ b & \overline{0} \end{array} \right) \middle| \, a, b \in \mathbb{Z}_8 \right\};$

$K = M_2(\mathbb{Z}_8)$ – кільце квадратних матриць 2-го порядку над кільцем $\mathbb{Z}_8$.

24.13. $T = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_3 \right\};$

$K = M_3(\mathbb{Z}_3)$ – квадратних матриць 3-го порядку над полем $\mathbb{Z}_3$.

24.14. $T = \left\{ \begin{pmatrix} \overline{0} & \overline{4}a \\ a & b \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_7 \right\};$

$K = \left\{ \begin{pmatrix} c & \overline{4}d \\ d & c \end{pmatrix} \middle| \, c, d \in \mathbb{Z}_7 \right\}.$

24.15. м $T = \left\{ \begin{pmatrix} \overline{0} & \overline{0} \\ a & b \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_6 \right\};$

$K = M_2(\mathbb{Z}_6)$ – кільце квадратних матриць 2-го порядку над кільцем $\mathbb{Z}_6$.

24.16. $T = \left\{ \begin{pmatrix} a & b & c \\ \overline{2}b & a & \overline{0} \\ \overline{2}c & \overline{0} & a \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z}_3 \right\}$

$K = M_3(\mathbb{Z}_3)$ – кільце квадратних матриць 3-го порядку над полем $\mathbb{Z}_3$.

24.17. $T = \left\{ \begin{pmatrix} \overline{5}a & \overline{5}b \\ -\overline{5}b & \overline{5}a \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_7 \right\};$

$K = \left\{ \begin{pmatrix} c & \overline{4}d \\ d & c \end{pmatrix} \middle| \, c, d \in \mathbb{Z}_7 \right\}.$

24.18. $T = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| \, a \in \mathbb{Z}_8 \right\};$

$K = M_2(\mathbb{Z}_8)$ – кільце квадратних матриць 2-го порядку над кільцем $\mathbb{Z}_8$.

24.19. $T = \left\{ \begin{pmatrix} \overline{0} & a & \overline{0} \\ \overline{0} & b & \overline{0} \\ \overline{0} & c & \overline{0} \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z}_3 \right\}$

$K = M_3(\mathbb{Z}_3)$ – кільце квадратних матриць 3-го порядку над полем $\mathbb{Z}_3$.

24.20. $T = \left\{ \begin{pmatrix} \overline{0} & \overline{0} & b \\ \overline{0} & \overline{0} & \overline{0} \\ a & \overline{0} & \overline{0} \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_2 \right\};$

$K = M_3(\mathbb{Z}_2)$ – кільце квадратних матриць 3-го порядку над полем $\mathbb{Z}_2$.

24.21. $T = \left\{ \begin{pmatrix} a & \overline{0} \\ \overline{0} & -a \end{pmatrix} \middle| a \in \mathbb{Z}_4 \right\}$;

$K = \left\{ \begin{pmatrix} c & d \\ d & c \end{pmatrix} \middle| a \in \mathbb{Z}_4 \right\}$.

24.22. $T = \left\{ \begin{pmatrix} \overline{0} & \overline{0} \\ a & \overline{0} \end{pmatrix} \middle| a \in \mathbb{Z}_7 \right\}$;

$K = M_2(\mathbb{Z}_7)$ кільце квадратних матриць 2-го порядку над кільцем $\mathbb{Z}_7$.

24.23. $T = \left\{ \begin{pmatrix} a & \overline{1} \\ -\overline{1} & a \end{pmatrix} \middle| a \in \mathbb{Z}_5 \right\}$;

$K = \left\{ \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \middle| a \in \mathbb{Z}_5 \right\}$.

24.24. $T = \left\{ \begin{pmatrix} \overline{0} & a & 2b \\ \overline{0} & \overline{0} & 2c \\ \overline{0} & \overline{0} & \overline{0} \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_4 \right\}$;

$K = \left\{ \begin{pmatrix} \overline{0} & m & n \\ \overline{0} & \overline{0} & \overline{2}s \\ \overline{0} & \overline{0} & \overline{0} \end{pmatrix} \middle| m, n, s \in \mathbb{Z}_4 \right\}$.

24.25. $T = \left\{ \begin{pmatrix} \overline{0} & a \\ b & \overline{0} \end{pmatrix} \middle| a, b \in \mathbb{Z}_9 \right\}$;

$K = M_2(\mathbb{Z}_9)$ кільце квадратних матриць 3-го порядку над кільцем $\mathbb{Z}_9$.

Приклад 25. У кільці $\mathbb{Z}$ цілих чисел знайти ідеали:

а) $\langle 6, 8\rangle$; б) $\langle -40, 60, 16\rangle$.

Розв'язання. а) Покажемо, що 2 (найбільший спільний дільник чисел 6 і 8) належить до ідеалу $\langle 6, 8\rangle$. За теоремою про лінійне представлення найбільшого спільного дільника двох цілих чисел існують $x_0, y_0 \in \mathbb{Z}$ такі, що $6x_0 + 8y_0 = 2$. Значить, $2 \in \{6x + 8y | x, y \in \mathbb{Z}\} = \langle 6, 8\rangle$. Тоді

$$\langle 2\rangle \subseteq \langle 6, 8\rangle. \tag{III.6}$$

З іншого боку,

$$\langle 6, 8\rangle = \{6x + 8y | x, y \in \mathbb{Z}\} = \{2(3x + 4y) | x, y \in \mathbb{Z}\} \subseteq \{2k | k \in \mathbb{Z}\} = \langle 2\rangle.$$

Тобто

$$\langle 6, 8\rangle \subseteq \langle 2\rangle. \tag{III.7}$$

Із (III.6) і (III.7) випливає, що:

$$\langle 6, 8\rangle = \langle 2\rangle.$$

б) Покажемо, що 4 (найбільший спільний дільник чисел $-40, 60$ і 16) належить до ідеалу $\langle -40, 60, 16\rangle$. За властивістю найбільшого спільного дільника кількох цілих чисел $(-40, 60, 16) = \big((-40, 60), 16\big)$. Введемо позначення. Нехай

$$(-40, 60) = d. \tag{III.8}$$

Тоді

$$(d, 16) = 4. \tag{III.9}$$

За теоремою про лінійне представлення найбільшого спільного дільника двох цілих чисел існують такі цілі числа u і v, що $-40u + 60v = d$ (див. (III.8)), а також цілі числа s і t такі, що $ds + 16t = 4$ (див. (III.9)). Тоді

$$(-40u + 60v)s + 16t = 4.$$

Звідси, $-40us + 60vs + 16t = 4$. Отже, $4 \in \{-40x + 60y + 16z | x, y, z \in \mathbb{Z}\} = \langle -40, 60, 16\rangle$, значить,

$$\langle 4\rangle \subseteq \langle -40, 60, 16\rangle. \tag{III.10}$$

З іншого боку,

$$\begin{aligned}\langle -40, 60, 16\rangle &= \{-40x + 60y + 16z | x, y, z \in \mathbb{Z}\} = \\ &= \{4(-10x + 15y + 4z) | x, y, z \in \mathbb{Z}\} \subseteq \{4k | k \in \mathbb{Z}\} = \langle 4\rangle.\end{aligned}$$

Тобто

$$\langle -40, 60, 16\rangle \subseteq \langle 4\rangle. \tag{III.11}$$

Із співвідношень (III.10) і (III.11) випливає, що

$$\langle -40, 60, 16\rangle = \langle 4\rangle.$$

Розробка процедур. Міркування, проведені при розв'язанні даного прикладу, можна узагальнити: для довільних двох цілих чисел a і b справедливо, що головний ідеал $\langle a, b\rangle$ кільця $\mathbb{Z}$ породжується найбільшим спільним дільником $d = (a, b)$ цих чисел: $\langle a, b\rangle = \langle d\rangle$. Аналогічно для довільної кількості елементів в $\mathbb{Z}$: $\langle a_1, a_2, ..., a_n\rangle = \langle d\rangle$, де $d = (a_1, a_2, ..., a_n)$.

Створимо процедуру **genIdeal**, яку можна буде застосовувати до довільної кількості елементів із $\mathbb{Z}$. Для цього елементи $a_1, a_2, ..., a_n$ задаватимемо як елементи послідовності **seq(integer)** (тобто процедура матиме один аргумент a типу **seq(integer)**). За означенням для $n \geqslant 2$ $(a_1, a_2, ..., a_n) = (d_{n-1}, a_n)$, де $d_{n-1} = (a_1, a_2, ..., a_n) = (d_{n-1}, a_n)$. При рекурентних співвідношеннях зручно використовувати цикл **for**.

Код процедури наступний:

```
genIdeal:=proc( a::seq(integer))
local d,i;
   d := 0;
   for i in a do d := igcd(d,i) end do;
   return(d);
end proc:
```

На початку циклу локальній змінній d надано значення 0. В ході виконання циклу змінна d поступово набуває значень $a_1, (a_1, a_2), (a_1, a_2, a_3), ...$ Цикл буде виконуватись, доки не буде вичерпано послідовність a.

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо команду **genIdeal**:

```
> genIdeal(6,8);
```

$$2$$

```
> genIdeal(-40,60,16);
```

$$4$$

Отже, $\langle 6, 8\rangle = \langle 2\rangle$, $\langle -40, 60, 16\rangle = \langle 4\rangle$.

Завдання 25. У кільці $\mathbb{Z}$ цілих чисел знайти ідеали:

25.1. а) $\langle -10, 15\rangle$; б) $\langle 105, 12, 97\rangle$.

25.2. а) $\langle 7, 12\rangle$; б) $\langle 44, -64, 32\rangle$.

25.3. а) $\langle 48, -50\rangle$; б) $\langle -8, 57, 14\rangle$.

25.4. а) $\langle -2, 15\rangle$; б) $\langle 126, 99, 27\rangle$.

25.5. а) $\langle 36, 54\rangle$; б) $\langle 80, -32, 16\rangle$.

25.6. а) $\langle 44, 98\rangle$; б) $\langle 23, 46, -14\rangle$.

25.7. а) $\langle 16, -27\rangle$; б) $\langle 70, 42, 112\rangle$.

25.8. а) $\langle 40, 64\rangle$; б) $\langle -34, 35, 36\rangle$.

25.9. а) $\langle 123, 126\rangle$; б) $\langle 7, -28, 22\rangle$.

25.10. а) $\langle 15, -20\rangle$; б) $\langle 14, 125, 163\rangle$.

25.11. а) $\langle 12, 17\rangle$; б) $\langle 154, 128, -16\rangle$.

25.12. а) $\langle -96, 98\rangle$; б) $\langle 12, 18, 31\rangle$.

25.13. а) $\langle 30, 14\rangle$; б) $\langle 153, 161, -99\rangle$.

25.14. а) $\langle 28, 70\rangle$; б) $\langle 22, 44, 7\rangle$.

25.15. а) $\langle 34, -3\rangle$; б) $\langle -49, 147, 63\rangle$.

25.16. а) $\langle 75, 105\rangle$; б) $\langle -30, 5, 18\rangle$.

25.17. а) $\langle -101, 57\rangle$; б) $\langle 55, 11, 121\rangle$.

25.18. а) $\langle 35, 18\rangle$; б) $\langle -93, 153, 62\rangle$.

25.19. а) $\langle -21, 28\rangle$; б) $\langle 105, 63, 17\rangle$.

25.20. а) $\langle 13, 24\rangle$; б) $\langle -145, 70, 35\rangle$.

25.21. а) $\langle 36, -34\rangle$; б) $\langle 215, 20, 210\rangle$.

25.22. а) $\langle -25, 10\rangle$; б) $\langle 212, 88, 76\rangle$.

25.23. а) $\langle 84, 24\rangle$; б) $\langle 62, -31, 14\rangle$.

25.24. а) $\langle 5, 32\rangle$; б) $\langle 128, 1024, 256\rangle$.

25.25. а) $\langle 42, -63\rangle$; б) $\langle -96, 92, 100\rangle$.

Приклад 26. В кільці $\mathbb{Z}$ цілих чисел виконати дії над його ідеалами:
а) $\langle 6\rangle + \langle 8\rangle$; б) $\langle 6\rangle \cap \langle 8\rangle$; в) $\langle 6\rangle \cdot \langle 8\rangle$.

Розв'язання. а) За означенням суми двох ідеалів

$$\langle 6\rangle + \langle 8\rangle = \{6k | k \in \mathbb{Z}\} + \{8s | s \in \mathbb{Z}\} = \{6k + 8s | k, s \in \mathbb{Z}\} =$$
$$= \{2(3k + 4s) | k, s \in \mathbb{Z}\} \subseteq \{2m | \forall m \in \mathbb{Z}\} = \langle 2\rangle.$$

Тобто

$$\langle 6\rangle + \langle 8\rangle \subseteq \langle 2\rangle. \qquad \text{(III.12)}$$

З іншого боку, $2 = 6 \cdot (-1) + 8 \cdot 1 \in \langle 6\rangle + \langle 8\rangle$, а значить,

$$\langle 2\rangle \subseteq \langle 6\rangle + \langle 8\rangle. \qquad \text{(III.13)}$$

Із співвідношень (III.12) і (III.13) випливає, що

$$\langle 6\rangle + \langle 8\rangle = \langle 2\rangle.$$

б) За означенням перерізу двох ідеалів

$$\langle 6\rangle \cap \langle 8\rangle = \{6k | k \in \mathbb{Z}\} \cap \{8s | s \in \mathbb{Z}\} = \langle [6, 8]\rangle = \langle 24\rangle.$$

в) За означенням добутку двох ідеалів

$$\langle 6\rangle \cdot \langle 8\rangle = \{6k | k \in \mathbb{Z}\} \cdot \{8s | s \in \mathbb{Z}\} =$$
$$= \{6k_1 \cdot 8s_1 + 6k_2 \cdot 8s_2 + \ldots + 6k_n \cdot 8s_n | k_i, s_j \in \mathbb{Z}, n \in \mathbb{N}\} =$$
$$= \{48(k_1 \cdot s_1 + k_2 \cdot s_2 + \ldots + k_n \cdot s_n) | k_i, s_j \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq \{48m | \forall m \in \mathbb{Z}\} = \langle 48\rangle.$$

Тобто

$$\langle 6\rangle \cdot \langle 8\rangle \subseteq \langle 48\rangle. \qquad \text{(III.14)}$$

З іншого боку, $48 = 6 \cdot 8 \in \langle 6\rangle \cdot \langle 8\rangle$, а значить,

$$\langle 48\rangle \subseteq \langle 6\rangle \cdot \langle 8\rangle. \qquad \text{(III.15)}$$

Із співвідношень (III.14) і (III.15) випливає, що

$$\langle 6\rangle \cdot \langle 8\rangle = \langle 48\rangle.$$

Розробка процедур. Міркування, проведені при розв'язанні даного прикладу, можна узагальнити: для довільних двох цілих чисел a і b справедливо, що:

1) сума двох ідеалів $\langle a\rangle$ і $\langle b\rangle$ кільця $\mathbb{Z}$ є головним ідеалом, породженим найбільшим спільним дільником $d=(a,b)$ чисел a і b: $\langle a\rangle+\langle b\rangle=\langle d\rangle$;

2) переріз двох ідеалів $\langle a\rangle$ і $\langle b\rangle$ кільця $\mathbb{Z}$ є головним ідеалом, породженим найменшим спільним кратним $m=[a,b]$ чисел a і b: $\langle a\rangle\cap\langle b\rangle=\langle m\rangle$;

3) добуток двох ідеалів $\langle a\rangle$ і $\langle b\rangle$ кільця $\mathbb{Z}$ є головним ідеалом, породженим добутком $g=ab$ чисел a і b: $\langle a\rangle\cdot\langle b\rangle=\langle g\rangle$.

Відповідні процедури **addIdeals**, **capIdeals**, **prodIdeals** мають вигляд:

а) сума ідеалів:

```
addIdeals:=proc(a,b)
local d;
   d:=igcd(a,b);
   return(d);
end proc:
```

б) перетин ідеалів:

```
capIdeals:=proc(a,b)
local m;
   m:=ilcm(a,b);
   return(m);
end proc:
```

в) добуток ідеалів:

```
prodIdeals:=proc(a,b)
local g;
   g:=a*b;
   return(g);
end proc:
```

Відмітимо, що дані процедури повертають елемент, який породжує відповідні ідеали (сума, перетин, добуток заданих ідеалів).

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо розроблені процедури.

а) Сума ідеалів:

```
> addIdeals(6,8);
```

2

б) Перетин ідеалів:

```
> capIdeals(6,8);
```

24

в) Добуток ідеалів:

```
> prodIdeals(6,8);
```

48

Отже, $\langle 6\rangle + \langle 8\rangle = \langle 2\rangle$, $\langle 6\rangle \cap \langle 8\rangle = \langle 24\rangle$, $\langle 6\rangle \cdot \langle 8\rangle = \langle 48\rangle$.

Завдання 26. В кільці $\mathbb{Z}$ цілих чисел виконати дії над його ідеалами:

26.1. а) $\langle 10\rangle + \langle 12\rangle$; б) $\langle 10\rangle \cap \langle 12\rangle$; в) $\langle 10\rangle \cdot \langle 12\rangle$.

26.2. а) $\langle 19\rangle + \langle 14\rangle$; б) $\langle 19\rangle \cap \langle 14\rangle$; в) $\langle 19\rangle \cdot \langle 14\rangle$.

26.3. а) $\langle 24\rangle + \langle 12\rangle$; б) $\langle 24\rangle \cap \langle 12\rangle$; в) $\langle 24\rangle \cdot \langle 12\rangle$.

26.4. а) $\langle 36\rangle + \langle 48\rangle$; б) $\langle 36\rangle \cap \langle 48\rangle$; в) $\langle 36\rangle \cdot \langle 48\rangle$.

26.5. а) $\langle 28\rangle + \langle 60\rangle$; б) $\langle 28\rangle \cap \langle 60\rangle$; в) $\langle 28\rangle \cdot \langle 60\rangle$.

26.6. а) $\langle 20\rangle + \langle 27\rangle$; б) $\langle 20\rangle \cap \langle 27\rangle$; в) $\langle 20\rangle \cdot \langle 27\rangle$.

26.7. а) $\langle 64\rangle + \langle 48\rangle$; б) $\langle 64\rangle \cap \langle 48\rangle$; в) $\langle 64\rangle \cdot \langle 48\rangle$.

26.8. а) $\langle 16\rangle + \langle 18\rangle$; б) $\langle 16\rangle \cap \langle 18\rangle$; в) $\langle 16\rangle \cdot \langle 18\rangle$.

26.9. а) $\langle 21\rangle + \langle 10\rangle$; б) $\langle 21\rangle \cap \langle 10\rangle$; в) $\langle 21\rangle \cdot \langle 10\rangle$.

26.10. а) $\langle 12\rangle + \langle 36\rangle$; б) $\langle 12\rangle \cap \langle 36\rangle$; в) $\langle 12\rangle \cdot \langle 36\rangle$.

26.11. а) $\langle 24\rangle + \langle 40\rangle$; б) $\langle 24\rangle \cap \langle 40\rangle$; в) $\langle 24\rangle \cdot \langle 40\rangle$.

26.12. а) $\langle 63\rangle + \langle 27\rangle$; б) $\langle 63\rangle \cap \langle 27\rangle$; в) $\langle 63\rangle \cdot \langle 27\rangle$.

26.13. а) $\langle 16\rangle + \langle 5\rangle$; б) $\langle 16\rangle \cap \langle 5\rangle$; в) $\langle 16\rangle \cdot \langle 5\rangle$.

26.14. а) $\langle 35\rangle + \langle 14\rangle$; б) $\langle 35\rangle \cap \langle 14\rangle$; в) $\langle 35\rangle \cdot \langle 14\rangle$.

26.15. а) $\langle 26\rangle + \langle 39\rangle$; б) $\langle 26\rangle \cap \langle 39\rangle$; в) $\langle 26\rangle \cdot \langle 39\rangle$.

26.16. а) $\langle 20\rangle + \langle 22\rangle$; б) $\langle 20\rangle \cap \langle 22\rangle$; в) $\langle 20\rangle \cdot \langle 22\rangle$.

26.17. а) $\langle 13\rangle + \langle 18\rangle$; б) $\langle 13\rangle \cap \langle 18\rangle$; в) $\langle 13\rangle \cdot \langle 18\rangle$.

26.18. а) $\langle 6\rangle + \langle 24\rangle$; б) $\langle 6\rangle \cap \langle 24\rangle$; в) $\langle 6\rangle \cdot \langle 24\rangle$.

26.19. а) $\langle 33\rangle + \langle 22\rangle$; б) $\langle 33\rangle \cap \langle 22\rangle$; в) $\langle 33\rangle \cdot \langle 22\rangle$.

26.20. а) $\langle 19\rangle + \langle 17\rangle$; б) $\langle 19\rangle \cap \langle 17\rangle$; в) $\langle 19\rangle \cdot \langle 17\rangle$.

26.21. а) $\langle 30\rangle + \langle 46\rangle$; б) $\langle 30\rangle \cap \langle 46\rangle$; в) $\langle 30\rangle \cdot \langle 46\rangle$.

26.22. а) $\langle 52\rangle + \langle 28\rangle$; б) $\langle 52\rangle \cap \langle 28\rangle$; в) $\langle 52\rangle \cdot \langle 28\rangle$.

26.23. а) $\langle 27\rangle + \langle 9\rangle$; б) $\langle 27\rangle \cap \langle 9\rangle$; в) $\langle 27\rangle \cdot \langle 9\rangle$.

26.24. а) $\langle 18\rangle + \langle 11\rangle$; б) $\langle 18\rangle \cap \langle 11\rangle$; в) $\langle 18\rangle \cdot \langle 11\rangle$.

26.25. а) $\langle 14\rangle + \langle 16\rangle$; б) $\langle 14\rangle \cap \langle 16\rangle$; в) $\langle 14\rangle \cdot \langle 16\rangle$.

4. Фактор-кільце

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай K – кільце, I – його ідеал. Елемент $a \in K$ називається конгруентним елементу b цього кільця за ідеалом I (або за модулем I), якщо $(a - b) \in I$. Пишуть:

$$a \equiv b (\mathrm{mod} I). \tag{III.16}$$

Запис (III.16) називається конгруенцією.

Властивості конгруенцій за ідеалом I в кільці K:

1. Якщо $a \equiv b \,(\mathrm{mod}\, I)$, $n \in \mathbb{Z}$, то $na \equiv nb \,(\mathrm{mod}\, I)$
2. Якщо $a_1 \equiv b_1 \,(\mathrm{mod}\, I)$, $a_2 \equiv b_2 \,(\mathrm{mod} I)$, то $a_1 \pm a_2 \equiv b_1 \pm b_2 \,(\mathrm{mod} I)$.
3. Якщо $a \equiv b \,(\mathrm{mod}\, I)$, c – довільний елемент із K, то $a + c \equiv b + c \,(\mathrm{mod}\, I)$.
4. Якщо $a_1 \equiv b_1 \,(\mathrm{mod} I)$, $a_2 \equiv b_2 \,(\mathrm{mod} I)$, то $a_1 a_2 \equiv b_1 b_2 \,(\mathrm{mod}\, I)$.

Відношення конгруентності, задане на елементах кільця K, за ідеалом I цього кільця є відношенням еквівалентності. Клас еквівалентності, породжений елементом a, позначають символом $\overline{a}$ або $K_a^{(I)}$, тобто $\overline{a} = \{x \in K | x \equiv a \,(\mathrm{mod} I)\}$, і називають **класом лишків** кільця K за ідеалом I із представником a, а кожен елемент класу лишків – просто **лишком**.

Нехай a – довільний елемент, I – ідеал кільця K. Тоді:

1°. $\overline{a} = a + I = \{a + h | h \in I\}$.
2°. Якщо $a \in I$, то $a + I = I = \overline{a} = \overline{0}$, де 0 – нуль-елемент кільця K.
3°. Клас лишків $\overline{a} = a + I$ є ідеалом кільця K тоді і лише тоді, коли $a \in I$.
4°. Якщо $b \in \overline{a}$, то $\overline{b} = \overline{a}$.
5°. Або $\overline{a} \cap \overline{b} = \varnothing$, або $\overline{a} = \overline{b}$.
6°. Об'єднання всіх різних класів лишків кільця K за ідеалом I рівне K.

У зв'язку із властивістю 1°, наведене означення класу лишків кільця за ідеалом рівносильне наступному: класом лишків кільця K за ідеалом I із представником a називається множина $a+I$ (або $I+a$) елементів виду $a+h$, де $h \in I$.

Множину всіх різних класів лишків кільця K за ідеалом I позначають K/I, тобто $K/I = \left\{\overline{a}, \overline{b}, \overline{c}, ...\right\}$. Відносно операцій додавання і множення класів лишків:

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

множина K/I утворює кільце, яке називають фактор-кільцем кільця K за ідеалом I (або за модулем I).

ПРИКЛАДИ І ЗАДАЧІ

Приклад 27.1. Побудувати фактор-кільце $\mathbb{Z}/\langle 6\rangle$ кільця $\mathbb{Z}$ за головним ідеалом $\langle 6\rangle$, породженим числом 6. Знайти дільники нуля цього фактор-кільця і дільники одиниці.

Розв'язання. Нехай $\overline{a} = a + \langle 6\rangle$ – довільний клас лишків із $\mathbb{Z}/\langle 6\rangle$. В силу теореми про ділення з остачею, для цілих чисел a і b існує єдина пара цілих чисел q і r така, що $a = 6q + r$, де $0 \leqslant r \leqslant 5$. Тоді

$$\overline{a} = a + \langle 6\rangle = 6q + r + \langle 6\rangle = r + \langle 6\rangle = \overline{r}, \quad \text{де } r = 0, 1, 2, 3, 4, 5.$$

Таким чином, маємо 6 різних класів лишків кільця $\mathbb{Z}$ цілих чисел за ідеалом $\langle 6\rangle$:

$$\begin{aligned}
&\overline{0} = 0 + \langle 6\rangle = \{6k | k \in \mathbb{Z}\} = \{0; \pm 6; \pm 12; \ldots\};\\
&\overline{1} = 1 + \langle 6\rangle = \{6k+1 | k \in \mathbb{Z}\} = \left\{ \begin{array}{l} 1, 7, 13, \ldots \\ -5, -11, -17, \ldots \end{array} \right\};\\
&\overline{2} = 2 + \langle 6\rangle = \{6k+2 | k \in \mathbb{Z}\} = \left\{ \begin{array}{l} 2, 8, 14, \ldots \\ -4, -10, -16, \ldots \end{array} \right\};\\
&\overline{3} = 3 + \langle 6\rangle = \{6k+3 | k \in \mathbb{Z}\} = \left\{ \begin{array}{l} 3, 9, 15, \ldots \\ -3, -9, -15, \ldots \end{array} \right\};\\
&\overline{4} = 4 + \langle 6\rangle = \{6k+4 | k \in \mathbb{Z}\} = \left\{ \begin{array}{l} 4, 10, 16, \ldots \\ -2, -8, -14, \ldots \end{array} \right\};\\
&\overline{5} = 5 + \langle 6\rangle = \{6k+5 | k \in \mathbb{Z}\} = \left\{ \begin{array}{l} 5, 11, 17, \ldots \\ -1, -7, -13, \ldots \end{array} \right\},
\end{aligned}$$

тобто

$$\mathbb{Z}/\langle 6\rangle = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

Знайдемо дільники нуля і дільники одиниці.

Спосіб I (за допомогою таблиці Келі). Цей спосіб доцільно використовувати для фактор-кілець із невеликою кількістю елементів.

Таблицею Келі для бінарної операції $*$ на n-елементній множині G є квадратна таблиця порядку $(n+1) \times (n+1)$. В її лівому верхньому куті записують знак операції. В першому рядку і першому стовпці записують усі елементи даної множини (по 1 в клітинку, причому зручно записувати в однаковому порядку):

$*$	a_1	a_2	...	a_n
a_1				
a_2				
a_3				
...				
a_n				

Решта клітинок заповнюються в наступний спосіб: якщо рядок, в якому знаходиться вибрана клітинка відповідає елементу a_i, а стовпчик – елементу a_j, то у вибрану клітинку записують результат операції $a_i * a_j$.

$*$	a_1	a_2	...	a_j	...	a_n
a_1						
a_2						
...						
a_i				$a_i * a_j$		
...						
a_n						

Складемо таблицю Келі для операції множення на множині $\mathbb{Z}/\langle 6\rangle$. Оскільки нульовий елемент не є дільником нуля і не може бути оберненим до жодного елемента, рядочок і стовпчик, що відповідають $\overline{0}$, можемо не писати.

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

(III.17)

(наприклад, $\overline{2}\cdot\overline{4}=\overline{2\cdot 4}=\overline{8}=\overline{2}$).

Із таблиці видно, що дільниками нуля є елементи $\overline{2}$, $\overline{3}$, $\overline{4}$, оскільки $\overline{2}\neq\overline{0}$, $\overline{3}\neq\overline{0}$, $\overline{4}\neq\overline{0}$, але $\overline{2}\cdot\overline{3}=\overline{0}$ і $\overline{3}\cdot\overline{4}=\overline{0}$.

Дільником одиниці нульовий елемент не є. Дільниками одиниці не є дільники нуля. Помічаємо, що для $\overline{1}$ оберненим є $\overline{1}$, а оберненим до $\overline{5}$ є $\overline{5}$ (оскільки $\overline{1}\cdot\overline{1}=\overline{1}$, $\overline{5}\cdot\overline{5}=\overline{1}$). Отже, дільниками одиниці є $\overline{1}$, $\overline{5}$.

Спосіб II. З огляду на зауваження в прикладі 12, в $\mathbb{Z}_6$ клас $K_a^{(6)}$ при $a\neq 0$ є дільником нуля тоді і лише тоді, коли $(a,6)\neq 1$. Оскільки $K_a^{(6)}=\overline{a}$, то дільниками нуля фактор-кільця $\mathbb{Z}/\langle 6\rangle$ є елементи $\overline{2}$, $\overline{3}$, $\overline{4}$.

Відомо, що дільник нуля не може бути дільником одиниці. Значить, дільниками одиниці можуть бути лише $\overline{1}$ і $\overline{5}$. Знайдемо обернені до них елементи. Зрозуміло, що $\overline{1}^{-1}=\overline{1}$. Нехай $\overline{x}$ – елемент, обернений до $\overline{5}$. Тоді $\overline{x}\cdot\overline{5}=\overline{1}$, значить, $\overline{5x}=\overline{1}$. Звідси випливає, що $5x\equiv 1(\mathrm{mod}\,6)$. Розв'язком даної конгруенції є клас лишків $\overline{5}$. Отже, $\overline{5}^{-1}=\overline{5}$. Таким чином, $\overline{1}$, $\overline{5}$ є дільниками одиниці.

Спосіб III. Число $m=6$ – складене: $6=2\cdot 3$, тоді $\overline{2}\cdot\overline{3}=\overline{6}=\overline{0}$, $\overline{4}\cdot\overline{3}=\overline{12}=\overline{0}$. Отже, дільниками нуля є: $\overline{2}$, $\overline{3}$, $\overline{4}$.

Зрозуміло, що $\overline{1}^{-1}=\overline{1}$. Знайдемо елемент, обернений до $\overline{5}$. Оскільки $(5,6)=1$, то, в силу теореми про лінійне представлення НСД двох цілих чисел, існують такі цілі числа u і v, що $5u+6v=1$. Знаходимо, що $u=-1$, $v=1$. Тоді $5\cdot(-1)+6\cdot 1=1$, звідси $\overline{5\cdot(-1)+6\cdot 1}=\overline{1}$. Отже, $\overline{5}\cdot\overline{-1}+\overline{6}\cdot\overline{1}=\overline{1}$. Але $\overline{6}=\overline{0}$, значить, $\overline{5}\cdot\overline{-1}=\overline{1}$. Таким чином, $\overline{5}^{-1}=\overline{-1}=\overline{5}$. Отже, $\overline{1}$, $\overline{5}$ є дільниками одиниці.

Розробка процедур. Створимо процедуру **cayleyTable**, яка для заданих множини **G** і операції **operation** будуватиме таблицю Келі. В якості таблиці Келі виступатиме квадратна матриця порядку t (де t – кількість елементів множини G), кожен елемент $M[i,j]$ якої є результатом операції **operation** над елементами $G[i]$ та $G[j]$ множини G (I-ий рядочок і I-ий стовпчик таблиці Келі не задаємо):

```
cayleyTable:=proc(G,operation)
local i,j,t,M;
   t:=nops(G);
   M:=Matrix(t);
   for i from 1 to t do
      for j from 1 to t do M[i,j]:=operation(G[i],G[j]); end do;
   end do;
   return(M);
end proc:
```

Розв'язання в Maple. Елементами фактор-кільця $\mathbb{Z}/\langle m\rangle$, як було показано в процесі розв'язування даного прикладу є класи лишків $\overline{r}$, де r – остача від ділення цілого числа на число m (тобто $r \in \{0, 1, ..., m-1\}$). Нехай FR – фактор-кільце $\mathbb{Z}/\langle m\rangle$:

```
> m:=6; FR:={$0..m-1};
```

$$m := 6$$

$$FR := \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$$

Для відшукання дільників одиниці і дільників нуля будуємо таблицю Келі за допомогою процедури **cayleyTable**. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Оскільки нульовий елемент $\overline{0}$ не є дільником нуля і не може бути дільником одиниці, рядочок і стовпчик, які відповідають $\overline{0}$, можемо не заносити в таблицю. Тому в якості аргумента G процедури **cayleyTable** можемо взяти множину

```
> FR minus {0};
```

$$\{1,\ 2,\ 3,\ 4,\ 5\}$$

Задаємо операцію **operation** (в даному випадку множення за модулем m):

```
> mult:=(X,Y)->X*Y mod m:
```

і будуємо таблицю Келі:

```
> cayleyTable(FR minus {0},mult);
```

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 0 & 2 & 4 \\ 3 & 0 & 3 & 0 & 3 \\ 4 & 2 & 0 & 4 & 2 \\ 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Визначаємо елементи, які в добутку дають $\overline{0}$. Нуль маємо на перетині 2-го рядочка і 3-го стовпчика, тому дільниками нуля є $G[2]$ і $G[3]$. Аналогічно дільниками нуля є $G[3]$ і $G[2]$, $G[3]$ і $G[4]$, $G[4]$ і $G[3]$. Оскільки $G[2] = \overline{2}$, $G[3] = \overline{3}$, $G[4] = \overline{4}$, то дільниками нуля в $\mathbb{Z}/\langle m\rangle$ є елементи $\overline{2}, \overline{3}, \overline{4}$.

Визначаємо тепер, для яких елементів $G[i]$ знайдеться елемент $G[j]$ такий, що $G[i] \cdot G[j] = \overline{1}$. Такими елементами є $G[1] = \overline{1}$, $G[5] = \overline{5}$. Отже, дільниками одиниці в $\mathbb{Z}/\langle m\rangle$ є $\overline{1}, \overline{5}$.

Зауваження. У випадку, коли матриця (яка репрезентує таблицю Келі) має порядок більше ніж 10, на екран (за замовчуванням) виводиться результат, на зразок наступного (фактор-кільце $\mathbb{Z}/\langle 12\rangle$):

```
> cayleyTable(FR minus {0},mult);
```

$$\begin{bmatrix} \text{11 x 11 Matrix} \\ \text{Data Type : anything} \\ \text{Storage : rectangular} \\ \text{Order : Fortran\_order} \end{bmatrix}$$

Для того, щоб в такому випадку побачити матрицю, необхідно збільшити значення параметра interface (вказавши потрібну кількість рядків таблиці):

```
> interface(rtablesize=11):
> cayleyTable(FR minus {0},mult);
```

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 4 & 6 & 8 & 10 & 0 & 2 & 4 & 6 & 8 & 10 \\ 3 & 6 & 9 & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9 \\ 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 & 0 & 4 & 8 \\ 5 & 10 & 3 & 8 & 1 & 6 & 11 & 4 & 9 & 2 & 7 \\ 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 \\ 7 & 2 & 9 & 4 & 11 & 6 & 1 & 8 & 3 & 10 & 5 \\ 8 & 4 & 0 & 8 & 4 & 0 & 8 & 4 & 0 & 8 & 4 \\ 9 & 6 & 3 & 0 & 9 & 6 & 3 & 0 & 9 & 6 & 3 \\ 10 & 8 & 6 & 4 & 2 & 0 & 10 & 8 & 6 & 4 & 2 \\ 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Приклад 27.2. Побудувати фактор-кільце $2\mathbb{Z}/10\mathbb{Z}$ кільця $2\mathbb{Z}$ (парних цілих чисел) за ідеалом $10\mathbb{Z}$ (кільцем цілих чисел, кратних 10).

Розв'язання. Нехай $K_a^{(10)} = a + 10\mathbb{Z}$ – довільний клас лишків із $2\mathbb{Z}/10\mathbb{Z}$. Оскільки $a \in 2\mathbb{Z}$, то $a = 2k$, $k \in \mathbb{Z}$. За теоремою про ділення з остачею для чисел k і 5 існує єдина пара цілих чисел q і r, що $k = 5q + r$, де $0 \leqslant r \leqslant 4$. Тоді

$$K_a^{(10)} = a + 10\mathbb{Z} = 2k + 10\mathbb{Z} = 2(5q + r) + 10\mathbb{Z} = \\ = 10q + 2r + 10\mathbb{Z} = 2r + 10\mathbb{Z} = K_{2r}^{(10)}, \quad \text{де } r = 0, 1, 2, 3, 4.$$

Таким чином, маємо 5 різних класів лишків кільця $2\mathbb{Z}$ цілих чисел за ідеалом $10\mathbb{Z}$:

$$K_0^{(10)} = 0 + 10\mathbb{Z} = \{10s | s \in \mathbb{Z}\};$$
$$K_2^{(10)} = 2 + 10\mathbb{Z} = \{10s + 2 | s \in \mathbb{Z}\};$$
$$K_4^{(10)} = 4 + 10\mathbb{Z} = \{10s + 4 | s \in \mathbb{Z}\};$$
$$K_6^{(10)} = 6 + 10\mathbb{Z} = \{10s + 6 | s \in \mathbb{Z}\};$$
$$K_8^{(10)} = 8 + 10\mathbb{Z} = \{10s + 8 | s \in \mathbb{Z}\},$$

тобто

$$2\mathbb{Z}/10\mathbb{Z} = \{K_0^{(10)}, K_2^{(10)}, K_4^{(10)}, K_6^{(10)}, K_8^{(10)}\}.$$

Розробка процедур. Провівши загальні міркування при побудові фактор-кільця $n\mathbb{Z}/m\mathbb{Z}$ (де $n|m$), отримуємо, що:

$$n\mathbb{Z}/m\mathbb{Z} = \{nr + m\mathbb{Z} | r = 0, 1, 2, ..., \frac{m}{n} - 1\} = \{K_0^{(m)}, K_n^{(m)}, K_{2n}^{(m)}, ..., K_{(\frac{m}{n}-1)n}^{(m)}\}.$$

Створимо процедуру **factorRingZ(n,m)**, результатом якої буде множина M чисел $0, n, 2n, ..., (\frac{m}{n} - 1)n$ (множина представників класів лишків фактор-кільця $n\mathbb{Z}/m\mathbb{Z}$). Для цього використаємо цикл **for**. На початку циклу $M = \varnothing$. В ході виконання циклу до множини M поступово додаються елементи – числа $n, 2n, ..., (m - 1)n$:

```
factorRingZ:=proc(n,m::integer)
local i,M:
   M:={};
   for i from 0 to (m/n-1) do M:=M union {i*n} end do;
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо розроблену процедуру:

```
> factorRingZ(2,10);
```

$$\{0,\ 2,\ 4,\ 6,\ 8\}$$

$$2\mathbb{Z}/10\mathbb{Z} = \{K_0^{(10)}, K_2^{(10)}, K_4^{(10)}, K_6^{(10)}, K_8^{(10)}\}.$$

Зауваження. Зрозуміло, що процедура **factorRingZ** не є універсальною для побудови фактор-кільця: вона може бути використана лише для побудови фактор-кілець $n\mathbb{Z}/m\mathbb{Z}$.

Завдання 27.

27.1. Побудувати фактор-кільце $\mathbb{Z}/\langle 8\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 8\rangle$, породженим числом 8. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{3}$.

27.2. Побудувати фактор-кільце $4\mathbb{Z}/12\mathbb{Z}$ кільця $4\mathbb{Z}$ цілих чисел, кратних 4, за ідеалом $12\mathbb{Z}$ (кільцем цілих чисел, кратних 12).

27.3. Побудувати фактор-кільце $\mathbb{Z}/\langle 20\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 20\rangle$, породженим числом 20. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{17}$.

27.4. Побудувати фактор-кільце $3\mathbb{Z}/18\mathbb{Z}$ кільця $3\mathbb{Z}$ цілих чисел, кратних 3, за ідеалом $18\mathbb{Z}$ (кільцем цілих чисел, кратних 18).

27.5. Побудувати фактор-кільце $\mathbb{Z}/\langle 12\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 12\rangle$, породженим числом 12. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{7}$.

27.6. Побудувати фактор-кільце $2\mathbb{Z}/20\mathbb{Z}$ кільця $2\mathbb{Z}$ цілих чисел, кратних 2, за ідеалом $20\mathbb{Z}$ (кільцем цілих чисел, кратних 20).

27.7. Побудувати фактор-кільце $\mathbb{Z}/\langle 4\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 4\rangle$, породженим числом 4. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{3}$.

27.8. Побудувати фактор-кільце $5\mathbb{Z}/25\mathbb{Z}$ кільця $5\mathbb{Z}$ цілих чисел, кратних 5, за ідеалом $25\mathbb{Z}$ (кільцем цілих чисел, кратних 25).

27.9. Побудувати фактор-кільце $\mathbb{Z}/\langle 16\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 16\rangle$, породженим числом 16. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{5}$.

27.10. Побудувати фактор-кільце $3\mathbb{Z}/24\mathbb{Z}$ кільця $3\mathbb{Z}$ цілих чисел, кратних 3, за ідеалом $24\mathbb{Z}$ (кільцем цілих чисел, кратних 24).

27.11. Побудувати фактор-кільце $\mathbb{Z}/\langle 30\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 30\rangle$, породженим числом 30. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{19}$.

27.12. Побудувати фактор-кільце $4\mathbb{Z}/24\mathbb{Z}$ кільця $4\mathbb{Z}$ цілих чисел, кратних 4, за ідеалом $24\mathbb{Z}$ (кільцем цілих чисел, кратних 24).

27.13. Побудувати фактор-кільце $\mathbb{Z}/\langle 14\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 14\rangle$, породженим числом 14. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{3}$.

27.14. Побудувати фактор-кільце $3\mathbb{Z}/15\mathbb{Z}$ кільця $3\mathbb{Z}$ цілих чисел, кратних 3, за ідеалом $15\mathbb{Z}$ (кільцем цілих чисел, кратних 15).

27.15. Побудувати фактор-кільце $\mathbb{Z}/\langle 18\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 18\rangle$, породженим числом 18. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{5}$.

27.16. Побудувати фактор-кільце $5\mathbb{Z}/20\mathbb{Z}$ кільця $5\mathbb{Z}$ цілих чисел, кратних 5, за ідеалом $20\mathbb{Z}$ (кільцем цілих чисел, кратних 20).

27.17. Побудувати фактор-кільце $\mathbb{Z}/\langle 21\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 21\rangle$, породженим числом 21. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{16}$.

27.18. Побудувати фактор-кільце $2\mathbb{Z}/10\mathbb{Z}$ кільця $2\mathbb{Z}$ цілих чисел, кратних 2, за ідеалом $10\mathbb{Z}$ (кільцем цілих чисел, кратних 10).

27.19. Побудувати фактор-кільце $\mathbb{Z}/\langle 15\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 15\rangle$, породженим числом 15. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{4}$.

27.20. Побудувати фактор-кільце $4\mathbb{Z}/16\mathbb{Z}$ кільця $4\mathbb{Z}$ цілих чисел, кратних 4, за ідеалом $16\mathbb{Z}$ (кільцем цілих чисел, кратних 16).

27.21. Побудувати фактор-кільце $\mathbb{Z}/\langle 24\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 24\rangle$, породженим числом 24. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{5}$.

27.22. Побудувати фактор-кільце $3\mathbb{Z}/9\mathbb{Z}$ кільця $3\mathbb{Z}$ цілих чисел, кратних 3, за ідеалом $9\mathbb{Z}$ (кільцем цілих чисел, кратних 9).

27.23. Побудувати фактор-кільце $\mathbb{Z}/\langle 25\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 25\rangle$, породженим числом 25. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{18}$.

27.24. Побудувати фактор-кільце $2\mathbb{Z}/12\mathbb{Z}$ кільця $2\mathbb{Z}$ цілих чисел, кратних 2, за ідеалом $12\mathbb{Z}$ (кільцем цілих чисел, кратних 12).

27.25. Побудувати фактор-кільце $\mathbb{Z}/\langle 10\rangle$ кільця $\mathbb{Z}$ цілих чисел за головним ідеалом $\langle 10\rangle$, породженим числом 10. Знайти дільники нуля цього фактор-кільця і елемент, обернений до елемента $\overline{7}$.

5. Гомоморфізми кілець

ТЕОРЕТИЧНІ ВІДОМОСТІ

Кільце $\langle K; *, \circ\rangle$ називається **гомоморфним** кільцю $\langle K_1; \oplus, \otimes\rangle$, якщо можна задати відображення φ множини K на множину K_1, при якому зберігаються операції, тобто якщо виконуються умови:

1) для довільного $a \in K$ елемент $\varphi(a) = a_1$ існує, належить до K_1 і визначається однозначно;
2) для довільного $b_1 \in K_1$ існує в K елемент b такий, що $\varphi(b) = b_1$;
3) для довільних $a, b \in K$ справедливо:

$$\varphi(a * b) = \varphi(a) \oplus \varphi(b);$$
$$\varphi(a \circ b) = \varphi(a) \otimes \varphi(b).$$

Якщо кільце K гомоморфне кільцю K_1, то пишуть: $K \simeq K_1$.

Властивості гомоморфізму кілець:

1. Якщо φ – гомоморфізм кільця K на кільце K_1, $a \in K$, то:

1) якщо 0 і $0'$ – нулі кілець K і K_1 відповідно, то $\varphi(0) = 0'$;
2) $\varphi(-a) = -\varphi(a)$;
3) якщо e і e_1 – одиниці кілець K і K_1 відповідно, то $\varphi(e) = e_1$;
4) якщо до елемента $a \in K$ обернений елемент a^{-1} існує і належить K, то $\varphi(a^{-1}) = [\varphi(a)]^{-1}$.

2. Гомоморфний образ $\varphi(K)$ кільця K є кільцем. Якщо K – комутативне, то $\varphi(K)$ також комутативне, якщо K – кільце з одиницею, то $\varphi(K)$ – також кільце з одиницею.

Кільце $\langle K; *, \circ\rangle$ називається **ізоморфним** кільцю $\langle K_1; \oplus, \otimes\rangle$, якщо можна задати таке взаємно однозначне відображення φ кільця K на K_1, при якому зберігаються операції кільця K, тобто виконуються умови:

1) для довільного $a \in K$ елемент $\varphi(a) = a_1$ існує, належить до K_1 і визначається однозначно;
2) для довільного $b_1 \in K_1$ існує в K елемент b такий, що $\varphi(b) = b_1$;
3) для довільних $a, b \in K$ справедливо:
$$\varphi(a * b) = \varphi(a) \oplus \varphi(b);$$
$$\varphi(a \circ b) = \varphi(a) \otimes \varphi(b).$$
4) для довільних $a, b \in K$ таких, що $a \neq b$ справедливо: $\varphi(a) \neq \varphi(b)$.

Таким чином, взаємно однозначний гомоморфізм K на K_1 є їхнім ізоморфізмом.

Якщо кільце K ізоморфне кільцю K_1, то пишуть: $K \cong K_1$.

Поле P називається гомоморфним полю P_1, якщо кільце P гомоморфне кільцю P_1. Поля P і P_1 називаються ізоморфними, якщо вони ізоморфні як кільця.

Нехай φ – гомоморфізм кільця K в кільце K'. Множина H всіх елементів кільця K, які гомоморфізмом φ відображаються в нуль-елемент $0'$ кільця K', називається **ядром гомоморфізму** φ і позначається: $H = \operatorname{Ker}\varphi$. Ядро гомоморфізму φ кільця K в кільце K' є ідеалом кільця K.

Теорема (основна теорема про гомоморфізми кілець)**.** *Якщо* $\operatorname{Ker}\varphi$ *– ядро гомоморфізму* φ *кільця* K *на кільце* K'*, то фактор-кільце* $K/\operatorname{Ker}\varphi$ *ізоморфне кільцю* K'*.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 28.1. Нехай φ – відображення кільця K пар (a, b), $a, b \in \mathbb{Z}_7$, в якому операції додавання $*$ і множення $\circ$ задано наступним чином:
$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 + b_2);$$
$$(a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, b_1 b_2),$$
на кільце $L = \mathbb{Z}_7$ цілих чисел, причому $\varphi\Big((a, b)\Big) = b$. Визначити, чи є φ гомоморфізмом. Якщо так, знайти ядро $\operatorname{Ker}\varphi$ цього гомоморфізму. Чи є φ ізоморфізмом?

Розв'язання. Очевидно, при відображенні φ кожному елементу (a, b) кільця K відповідає певний конкретний елемент b із $\mathbb{Z}_7$, і, навпаки, для довільного елемента $c \in \mathbb{Z}_7$ в K знайдеться прообраз (наприклад, $(\overline{0}, c)$), тобто умови 1) і 2) означення гомоморфізму виконуються. Перевіримо, чи зберігаються операції додавання і множення (умова 3)).

Нехай (a_1, b_1) і (a_2, b_2) – довільні два елементи із K. Знайдемо

$$\varphi\Big((a_1, b_1) * (a_2, b_2)\Big) = \varphi\Big((a_1 + a_2, b_1 + b_2)\Big) = b_1 + b_2 = \varphi\Big((a_1, b_1)\Big) + \varphi\Big((a_2, b_2)\Big);$$
$$\varphi\Big((a_1, b_1) \circ (a_2, b_2)\Big) = \varphi\Big((a_1 a_2, b_1 b_2)\Big) = b_1 b_2 = \varphi\Big((a_1, b_1)\Big) \cdot \varphi\Big((a_2, b_2)\Big).$$

Операції додавання і множення при відображенні φ зберігаються, значить, φ – гомоморфізм кільця K на кільце $\mathbb{Z}$. Знайдемо ядро цього гомоморфізму.

За означенням ядро $\operatorname{Ker}\varphi$ гомоморфізму – це множина всіх тих елементів (a, b) із K, що відображаються в нульовий елемент кільця $\mathbb{Z}_7$, тобто

$$\varphi\Big((a, b)\Big) = \overline{0}.$$

В силу задання гомоморфізму, $\varphi\Big((a, b)\Big) = b$, значить, $b = \overline{0}$. Тоді $\operatorname{Ker}\varphi = \big\{(a, \overline{0}) | a \in \mathbb{Z}_7\big\}$.

Визначити, чи є φ ізоморфізмом можна двома способами.

Спосіб I (за означенням): перевіримо, чи виконується умова 4) означення ізоморфізму. Нехай $(a_1, b_1), (a_2, b_2) \in K$, причому $(a_1, b_1) \neq (a_2, b_2)$, і нехай $\varphi((a_1, b_1)) = \varphi((a_2, b_2))$. Тоді, за заданням відображення φ, $b_1 = b_2$. Таким чином, два пари (a, b_1) і (a_2, b_2) матимуть однакові образи, якщо їхні другі компоненти однакові. Але в K існують різні елементи із однаковими другими компонентами, наприклад $(\overline{0}, \overline{2})$ і $(\overline{1}, \overline{2})$. Отже, гомоморфізм φ кільця K на L не є ізоморфізмом.

Спосіб II. Гомоморфізм φ кільця K на кільце L є їхнім ізоморфізмом тоді і лише тоді, коли ядро $\operatorname{Ker}\varphi$ цього гомоморфізму складається лише із нульового елемента кільця K. Оскільки $\operatorname{Ker}\varphi \neq \{\overline{0}\}$, то гомоморфізм φ кільця K на L не є ізоморфізмом.

Розробка процедур. Створимо процедури для перевірки умов означення гомоморфізму.

Процедура **existsIm** для всіх елементів $K[i]$ кільця K ($i = 1, 2, ..., t$ – кількість елементів кільця K) перевіряє, чи міститься елемент $\varphi(K[i])$ в L.

```
existsIm:=proc(PHI,K,L)
local i,s,t;
   t:=nops(K);
   s:=0;
   for i from 1 to t do
      if member(PHI(K[i]),L)=true then s:=s+1; end if;
   end do;
   evalb(s=t);
end proc:
```

Зауважимо, що оскільки правило φ задаватимемо як функцію, то одночасно здійснюється також перевірка, чи є образ $\varphi(a)$ єдиним, і чи завжди існує. Якщо образ існує не для кожного елемента із K, то з'являється попередження на зразок наступного:

```
Error, (in PHI) numeric exception: division by zero
```

(неможливість ділення на 0).

Наступна процедура **existsProim**, навпаки, для всіх елементів $L[i]$ кільця L перевіряє, чи існує в K елемент, образом якого є $L[i]$. При цьому фіксується елемент $L[i]$ ($i \in \overline{1,n}$, де n – кількість елементів кільця L) і для всіх елементів $K[j]$ кільця K, почергово перевіряється, чи виконується умова $\varphi(K[j]) = L[i]$. Як тільки елемент $K[j]$, що задовольняє дану умову, знайдено, перевірка припиняється, лічильник s збільшується на 1, і переходимо до розгляду наступного елемента із L. Після закінчення виконання циклів перевіряється, чи збігається кількість s елементів, для яких прообраз існує, із кількістю t елементів в L.

```
existsProim:=proc(PHI,K,L)
local i,j,s,t,n;
   t:=nops(K);
   n:=nops(L);
   s:=0;
   for i from 1 to n do
      j:=1;
      while j<=t do
         if PHI(K[j])=L[i] then s:=s+1; break; else j:=j+1; end if;
      end do;
   end do;
   evalb(s=n);
end proc:
```

Процедура **savesOperation** перевіряє, чи зберігається при відображенні φ операція. Для зручності операції кільця K і L позначено через operationK і operationL відповідно. Досліджуємо кожну пару елементів $K[i]$ і $K[j]$ кільця K: якщо для елементів $K[i]$ і $K[j]$ умова $\varphi(operationK(K[i], K[j])) = operationL(\varphi(K[i]), \varphi(K[j]))$ виконується, лічильник s збільшується на 1. Операція зберігається, якщо дана умова виконується для всіх пар елементів $K[i]$ і $K[j]$ ($i, j \in \overline{1,t}$), тоді в результаті $s = t^2$, де t – кількість елементів кільця K.

```
savesOperation:=proc(PHI,K,L,operationK,operationL)
local i,j,s,t;
   t:=nops(K);
   s:=0;
   for i from 1 to t do
      for j from 1 to t do
         if PHI(operationK(K[i],K[j]))=operationL(PHI(K[i]),PHI(K[j]))
            then s:=s+1; end if;
      end do;
   end do;
   evalb(s=t^2);
end proc:
```

На базі розроблених процедур створимо процедуру **isHomomorphism**, яка визначатиме, чи є відображення $\varphi : K \to L$ гомоморфізмом. Така процедура перевірятиме, чи виконуються одночасно умови 1)-3) означення гомоморфізму (тобто чи кожна із процедур **existsIm**, **existsProim**, **savesOperation** повертає значення **true**).

```
isHomomorphism:=proc(PHI,K,L,operationK1,operationK2,
      operationL1,operationL2)
   if existsIm(PHI,K,L)=true and existsProim(PHI,K,L)=true and
      savesOperation(PHI,K,L,operationK1,operationL1)=true and
      savesOperation(PHI,K,L,operationK2,operationL2)=true then
      return(true);
   else return(false);
   end if;
end proc:
```

Для відшукання ядра гомоморфізму φ створимо процедуру **kerPHI**, в ході якої для всіх елементів $K[i]$ кільця K визначається, чи є образ $\varphi(K[i])$ нульовим елементом кільця L:

```
> PHI(K[i])=Id(L,operationL1)
```

(Про процедуру **Id** див. Приклад 21.1). Якщо для елемента $K[i]$ виконується дана умова, то елемент $K[i]$ додається до множини Ker :

```
> Ker:=Ker union {K[i]};
```

Результатом процедури є множина Ker

Код процедури наступний:

```
kerPHI:=proc(PHI,K,L,operationL1)
local i,t,Ker;
   t:=nops(K);
   Ker:={};
   for i from 1 to t do
      if PHI(K[i])=Id(L,operationL1) then Ker:=Ker union {K[i]}; end if;
   end do;
   return(Ker);
end proc:
```

Для перевірки умови 4) означення ізоморфізму створимо процедуру **diffIm**, в ході якої спочатку порівнюємо образи елемента $K[1]$ із образами елементів $K[2], K[3], ..., K[t]$, далі образ елемента $K[2]$ із образами елементів $K[3], K[4], ..., K[t]$, потім образ елемента $K[3]$ із образами елементів $K[4], K[5], ..., K[t]$ і т.д. Якщо образи елементів $K[i]$ і $K[j]$ різні (за такого підходу $i \neq j$), лічильник s збільшуємо на 1. Якщо для всіх пар елементів $K[i]$ і $K[j]$ справедливо, що $\varphi(K[i]) \neq \varphi(K[j])$, то в результаті лічильник s повинен збільшитись на $(t-1)+(t-2)+...+2+1=\frac{(t-1)t}{2}$.

```
diffIm:=proc(PHI,K)
local i,j,s,t;
   s:=0;
   t:=nops(K);
   for i from 1 to t do
      for j from i+1 to t do
         if PHI(K[i])<>PHI(K[j]) then s:=s+1; end if;
      end do;
   end do;
   evalb(s=1/2*t*(t-1));
end proc:
```

На основі процедур **isHomomorphism** і **diffIm** можна розробити процедуру **isIsomorphism**, яка перевірятиме, чи є відображення $\varphi : K \to L$ ізоморфізмом:

```
isIsomorphism:=proc(PHI,K,L,operationK1,operationK2,
      operationL1,operationL2)
   if isHomomorphism(PHI,K,L,operationK1,operationK2,
      operationL1,operationL2) =true and
      diffIm(PHI,K,L)=true then return(true);
   else return(false);
   end if;
end proc:
```

Розв'язання в Maple. Задаємо множину K і операції $*$, $\circ$:

```
> K:={seq(seq([a,b],a=0..6),b=0..6)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 7,X[2]+Y[2] mod 7]:
> circ:=(X,Y)->[X[1]*Y[1] mod 7,X[2]*Y[2] mod 7]:
```

та множину L і операції pl, ml (додавання і множення за модулем m):

```
> L:={seq(c,c=0..6)}:
> pl:=(C,D)->C+D mod 7:
> ml:=(C,D)->C*D mod 7:
```

Правило φ задаємо як функцію: парі $A = (A[1], A[2])$ ставимо у відповідність другу компоненту пари $A[2]$:

```
> PHI:=A -> A[2]:
```

Далі підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);
> with(atchlib):
```

і перевіряємо, чи виконуються умови 1)-3) означення гомоморфізму:

```
> existsIm(PHI,K,L);
```

true

Для кожного елемента $a \in K$ образ $\varphi(a)$ існує і належить до K.

```
> existsProim(PHI,K,L);
```

true

Для кожного елемента із L в K існує прообраз.

```
> savesOperation(PHI,K,L,astra,pl);
```

true

Перша операція зберігається.

```
> savesOperation(PHI,K,L,circ,ml);
```

true

Друга операція також зберігається.

Таким чином, всі умови означення гомоморфізму виконуються, значить,

```
> isHomomorphism(PHI,K,L,astra,circ,pl,ml);
```

true

φ – гомоморфізм кільця K на кільце L.

Знаходимо $\mathrm{Ker}\,\varphi$:

```
> kerPHI(PHI,K,L);
```

{[0, 0], [1, 0], [2, 0], [3, 0], [4, 0], [5, 0], [6, 0]}

Таким чином, $\operatorname{Ker}\varphi = \{(a,\overline{0})|a \in \mathbb{Z}_7\}$.

Визначимо, чи виконується умова 4) означення ізоморфізму:

```
> diffIm(PHI,K);
```

false

Умова 4) означення ізоморфізму не виконується, значить, гомоморфізм кільця K на кільце L не є ізоморфізмом:

```
> isIsomorphism(PHI,K,L,astra,circ,pl,ml);
```

false

Зауваження. Суму $\sum_{i=m}^{n} f$ в Maple можна знайти за допомогою команди **sum(f,i=m..n)**.

```
> sum(i,i=1..t-1);
```

$$\frac{1}{2}t^2 - \frac{1}{2}t$$

Приклад 28.2. Довести, що кільце $K = \{(m,n)|m,n \in \mathbb{Z}_5\}$, в якому операції $*$ і $\circ$ задані наступним чином: $(m,n) * (k,l) = (m+k, n+l)$, $(m,n) \circ (k,l) = (mk + \overline{4}nl, ml + nk)$, ізоморфне кільцю L матриць виду $\begin{pmatrix} a & b \\ \overline{4}b & a \end{pmatrix}$, де $a, b \in \mathbb{Z}_5$.

Розв'язання. Довільному елементу $(m,n) \in K$ (де $m,n \in \mathbb{Z}_5$) поставимо у відповідність матрицю

$$A = \begin{pmatrix} m & n \\ \overline{4}n & m \end{pmatrix}.$$

Маємо:

1) Для довільного $(m,n) \in K$ справедливо, що образ $\varphi((m,n))$ існує, належить до L і єдиний.

2) Для довільного елемента $\begin{pmatrix} a & b \\ \overline{4}b & a \end{pmatrix} \in L$ прообразом в кільці K є елемент (a,b).

3) Покажемо, що зберігаються операції. Нехай (m_1,n_1) і (m_2,n_2) – довільні два елементи із K. Тоді:

$$\varphi\left((m_1,n_1) * (m_2,n_2)\right) = \varphi\left((m_1+m_2, n_1+n_2)\right) = \begin{pmatrix} m_1+m_2 & n_1+n_2 \\ \overline{4}\,(n_1+n_2) & m_1+m_2 \end{pmatrix} =$$

$$= \begin{pmatrix} m_1 & n_1 \\ \overline{4}n_1 & m_1 \end{pmatrix} + \begin{pmatrix} m_2 & n_2 \\ \overline{4}n_2 & m_2 \end{pmatrix} = \varphi\left((m_1,n_1)\right) + \varphi\left((m_2,n_2)\right);$$

$$\varphi\left((m_1,n_1)\circ(m_2,n_2)\right)=\varphi\left((m_1m_2+\overline{4}n_1n_2,m_1n_2+n_1m_2)\right)=$$
$$=\begin{pmatrix} m_1m_2+\overline{4}n_1n_2 & m_1n_2+n_1m_2 \\ \overline{4}(m_1n_2+n_1m_2) & m_1m_2+\overline{4}n_1n_2 \end{pmatrix};$$

$$\varphi\left((m_1,n_1)\right)\cdot\varphi\left((m_2,n_2)\right)=\begin{pmatrix} m_1 & n_1 \\ \overline{4}n_1 & m_1 \end{pmatrix}\cdot\begin{pmatrix} m_2 & n_2 \\ \overline{4}n_2 & m_2 \end{pmatrix}=$$
$$=\begin{pmatrix} m_1m_2+\overline{4}n_1n_2 & m_1n_2+n_1m_2 \\ \overline{4}m_1n_2+\overline{4}n_1m_2 & m_1m_2+\overline{4}n_1n_2 \end{pmatrix};$$

Отже, $\varphi\left((m_1,n_1)\circ(m_2,n_2)\right)=\varphi\left((m_1,n_1)\right)\cdot\varphi\left((m_2,n_2)\right)$.

Таким чином, відображення φ зберігає операції.

4) Нехай (m_1,n_1), (m_2,n_2) – довільні два елементи із K такі, що $(m_1,n_1)\neq(m_2,n_2)$. Тоді $m_1\neq m_2$ або $n_1\neq n_2$. Отже,

$$\varphi\left((m_1,n_1)\right)=\begin{pmatrix} m_1 & n_1 \\ \overline{4}n_1 & m_1 \end{pmatrix}\neq\begin{pmatrix} m_2 & n_2 \\ \overline{4}n_2 & m_2 \end{pmatrix}=\varphi\left((m_2,n_2)\right).$$

За означенням, $K\overset{\varphi}{\cong}L$.

Розв'язання в Maple. Задаємо множину K і операції $*$, $\circ$:

```
> K:={seq(seq([a,b],a=0..4),b=0..4)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 5,X[2]+Y[2] mod 5]:
> circ:=(X,Y)->[X[1]*Y[1]-X[2]*Y[2] mod 5,
  X[1]*Y[2]+X[2]*Y[1] mod 5]:
```

і множину L та операції додавання і множення матриць mplus і mmult:

```
> L:={seq(seq([[a,b],[4*b mod 5,a]],a=0..4),b=0..4)}:
> mplus:=(A,B)->[[A[1,1]+B[1,1] mod 5,A[1,2]+B[1,2] mod 5],
  [A[2,1]+B[2,1] mod 5,A[2,2]+B[2,2] mod 5]]:
> mmult:=(A,B)-> [[A[1,1]*B[1,1]+A[1,2]*B[2,1] mod 5,
  A[1,1]*B[1,2]+A[1,2]*B[2,2] mod 5],
  [A[2,1]*B[1,1]+A[2,2]*B[2,1] mod 5,
  A[2,1]*B[1,2]+A[2,2]*B[2,2] mod 5]]:
```

Тепер задаємо відображення φ:

```
> PHI:=X -> [[X[1],X[2]],[4*X[2] mod 5,X[1]]];
```

$$PHI := X \to [[X_1,\ X_2],\ [(4\,X_2) \bmod 5,\ X_1]]$$

Далі використовуємо процедури, створені при розв'язанні Прикладу 28.1. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);
> with(atchlib):
```

і перевіряємо, чи виконуються умови 1)-3) означення гомоморфізму:

```
> existsIm(PHI,K,L);
```

true

```
> existsProim(PHI,K,L);
```

true

```
> savesOperation(PHI,K,L,astra,mplus);
```

true

```
> savesOperation(PHI,K,L,circ,mmult);
```

true

```
> diffIm(PHI,K);
```

true

Відображення $\varphi : K \to L$ задовольняє всі 4 умови означення ізоморфізму. Отже, φ – ізоморфізм кільця K на кільце L. Дійсно,

```
> isIsomorphism(PHI,K,L,astra,circ,mplus,mmult);
```

true

Завдання 28.

28.1. Визначити, чи є гомоморфізмом відображення $\varphi : M_2(\mathbb{Z}_5) \to \mathbb{R}$ кільця $M_2(\mathbb{Z}_5)$ квадратних матриць 2-го порядку над полем $\mathbb{Z}_5$ на поле $\mathbb{Z}_5$, яке кожній матриці із $M_2(\mathbb{Z}_5)$ ставить у відповідність її визначник. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.2. Довести, що ізоморфними між собою є кільця $K = \{(a, b)|a, b \in \mathbb{Z}_7\}$ із операціями, заданими наступним чином: $(a, b) * (c, d) = (a + c, b + d)$, $(a, b) \circ (c, d) = (ac + \overline{5}bd, ad + bc)$ та кільце $L = \left\{ \begin{pmatrix} x & y \\ \overline{5}y & x \end{pmatrix} \middle| x, y \in \mathbb{Z}_7 \right\}$.

28.3. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_5$ кільця $K = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_5 \right\}$ на кільце $\mathbb{Z}_5$, при якому $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = ab$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.4. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_5$ кільця $K = \{(a, b)|a, b \in \mathbb{Z}_8\}$ із операціями, заданими наступним чином: $(a, b) * (c, d) = (a + c, b + d)$, $(a, b) \circ (c, d) = (\overline{0}, \overline{2}ac)$ на кільце $\mathbb{Z}_8$, при якому $\varphi\Big((a, b)\Big) = a + b$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.5. Довести, що поле $\langle P; *, \circ\rangle$ і поле $\langle F; \oplus, \odot\rangle$ ізоморфні, де:

$P = \{(a,b)|a,b \in \mathbb{Z}_7\}$ із операціями: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (ac + \overline{3}bd, ad + bc)$;

$F = \{(x,y)|x,y \in \mathbb{Z}_7\}$ із операціями: $(x,y) * (u,v) = (x+u, y+v)$, $(x,y) \circ (u,v) = (xu + \overline{6}yv, xv + yu)$;

28.6. Задати гомоморфізм кільця $K = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a,b \in \mathbb{Z}_9 \right\}$ на кільце $L = \left\{ \begin{pmatrix} x & \overline{0} \\ \overline{0} & x \end{pmatrix} \middle| x \in \mathbb{Z}_9 \right\}$. Знайти ядро цього гомоморфізму.

28.7. Довести, що ізоморфними між собою є кільця $K = \{(a,b)|a,b \in \mathbb{Z}_3\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (ac + \overline{2}bd, ad + bc)$ та кільце $L = \left\{ \begin{pmatrix} x & y \\ \overline{2}y & x \end{pmatrix} \middle| x,y \in \mathbb{Z}_3 \right\}$.

28.8. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_4$ кільця діагональних матриць $K = \left\{ \begin{pmatrix} a & \overline{0} \\ \overline{0} & b \end{pmatrix} \middle| a,b \in \mathbb{Z}_4 \right\}$ на кільце $\mathbb{Z}_4$, при якому $\varphi\left(\begin{pmatrix} a & \overline{0} \\ \overline{0} & b \end{pmatrix} \right) = b$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.9. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_4$ кільця $K = \{(a,b)|a,b \in \mathbb{Z}_4\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (\overline{3}ac, bd)$ на кільце $\mathbb{Z}_4$, при якому $\varphi\Big((a,b)\Big) = a + \overline{2}b$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.10. Довести, що кільце матриць виду $\left\{ \begin{pmatrix} m & \overline{0} \\ \overline{0} & n \end{pmatrix} \middle| m,n \in \mathbb{Z}_7 \right\}$ і кільце $\langle L; \oplus, \odot\rangle$ пар (a,b), $a,b \in \mathbb{Z}_7$, в якому операції додавання $\oplus$ і множення $\odot$ задано наступним чином: $(a,b) \oplus (c,d) = (a+c, b+d)$; $(a,b) \odot (c,d) = (ac, bd)$, ізоморфні.

28.11. Нехай $K = \{(a,b,c)|a,b,c \in \mathbb{Z}_6\}$ – кільце відносно операцій, заданих наступним чином: $(a,b,c) * (m,n,l) = (a+m, b+n, c+l)$, $(a,b,c) \circ (m,n,l) = (am+bl+cn, an+bm+cl, al+bn+cm)$. Визначити, чи є відображення $\varphi((a,b,c)) = (a,c,b)$ гомоморфним відображенням кільця K на себе. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.12. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_5$ кільця $K = \{(a,b)|a,b \in \mathbb{Z}_5\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (\overline{2}ac, bd)$ на кільце $\mathbb{Z}_5$, при якому $\varphi\Big((a,b)\Big) = \frac{a}{b}$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.13. Довести, що ізоморфними між собою є кільця $K = \{(a,b)|a,b \in \mathbb{Z}_4\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (ac + \overline{2}bd, ad + bc)$ та кільце $L = \left\{ \begin{pmatrix} x & \overline{2}y \\ y & x \end{pmatrix} \middle| x, y \in \mathbb{Z}_4 \right\}$.

28.14. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_8$ кільця $K = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_8 \right\}$ на кільце $\mathbb{Z}_8$ цілих чисел, при якому $\varphi\Big(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\Big) = a + b$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.15. Задати гомоморфізм φ кільця $M_2(\mathbb{Z}_7)$ квадратних матриць 2-го порядку над полем $\mathbb{Z}_7$ на поле $\mathbb{Z}_7$. Знайти ядро цього гомоморфізму.

28.16. Довести, що кільце матриць виду $\left\{ \begin{pmatrix} m & n \\ \overline{3}n & m \end{pmatrix} \middle| m, n \in \mathbb{Z}_9 \right\}$ і кільце $\langle L; \oplus, \odot \rangle$ впорядкованих пар (a,b), $a,b \in \mathbb{Z}_9$, в якому операції додавання $\oplus$ і множення $\odot$ задано наступним чином:

$$(a,b) \oplus (c,d) = (a+c, b+d); \quad (a,b) \odot (c,d) = (ac + \overline{3}bd, ad + bc),$$

ізоморфні.

28.17. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_9$ кільця $K = \{(a,b)|a,b \in \mathbb{Z}_9\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (bd, \overline{3}bd)$ на кільце $\mathbb{Z}_9$, при якому $\varphi\Big((a,b)\Big) = \overline{2}ab$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.18. Довести, що ізоморфними між собою є кільця $K = \{(a,b)|a,b \in \mathbb{Z}_2\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (ac + bd, ad + bc)$ та кільце $L = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} \middle| x, y \in \mathbb{Z}_2 \right\}$.

28.19. Визначити, чи задає відображення $\varphi((a,b)) = (a, \overline{4}b)$ ізоморфізм кільця $\langle K; *, \circ\rangle$ на себе, де $K = \{(a,b)|a,b \in \mathbb{Z}_5\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (ac + \overline{3}bd, ad + bc)$.

28.20. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_6$ кільця $K = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a,b \in \mathbb{Z}_6 \right\}$ на кільце $\mathbb{Z}_6$, при якому $\varphi\Big(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\Big) = a + \overline{5}b$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.21. Нехай $K = \{(a,b,c)|a,b,c \in \mathbb{Z}_6\}$ – кільце відносно операцій, заданих наступним чином: $(a,b,c) * (m,n,l) = (a+m, b+n, c+l)$, $(a,b,c) \circ (m,n,l) = (am+bl+cn, an+bm+cl, al+bn+cm)$. Визначити, чи є відображення $\varphi((a,b,c)) = (a,b,\overline{0})$ ізоморфним відображенням кільця K на себе.

28.22. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_5$ кільця $K = \{(a,b)|a,b \in \mathbb{Z}_5\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (\overline{0}, \overline{0})$ на кільце $\mathbb{Z}_5$, при якому $\varphi\Big((a,b)\Big) = \overline{0}$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

28.23. Довести, що кільце матриць виду $\left\{ \begin{pmatrix} m & n \\ \overline{5}n & m \end{pmatrix} \middle| m,n \in \mathbb{Z}_7 \right\}$ і кільце $\langle L; \oplus, \odot\rangle$ впорядкованих пар (a,b), $a,b \in \mathbb{Z}_7$, в якому операції додавання $\oplus$ і множення $\odot$ задано наступним чином:

$$(a,b) \oplus (c,d) = (a+c, b+d); \quad (a,b) \odot (c,d) = (ac + \overline{5}bd, ad + bc),$$

ізоморфні.

28.24. Задати гомоморфізм φ кільця $K = \{(a,b)|a,b \in \mathbb{Z}_5\}$ відносно операцій $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (ac + \overline{3}bd, ad + bc)$ на кільце L матриць виду $\left\{ \begin{pmatrix} m & \overline{3}n \\ n & m \end{pmatrix} \middle| m,n \in \mathbb{Z}_7 \right\}$. Знайти ядро цього гомоморфізму.

28.25. Визначити, чи є гомоморфізмом відображення $\varphi : K \to \mathbb{Z}_5$ кільця $K = \{(a,b)|a,b \in \mathbb{Z}_5\}$ із операціями, заданими наступним чином: $(a,b) * (c,d) = (a+c, b+d)$, $(a,b) \circ (c,d) = (bd, \overline{3}bd)$ на кільце $\mathbb{Z}_5$, при якому $\varphi\Big((a,b)\Big) = -ab$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

Приклад 29. Довести, що $\mathbb{Z}_{12}/3\mathbb{Z}_{12} \cong \mathbb{Z}_3$.

Розв'язання. Маємо:

$$\mathbb{Z}_{12} = \left\{K_0^{(12)}, K_1^{(12)}, K_2^{(12)}, \ldots, K_{11}^{(12)}\right\}, \quad \mathbb{Z}_3 = \left\{K_0^{(3)}, K_1^{(3)}, K_2^{(3)}\right\}.$$

Задамо відображення $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ наступним чином:

$$\text{нехай} \quad \varphi(K_a^{(12)}) = K_r^{(3)}, \quad \text{де } r \equiv a \,(\mathrm{mod}\, 3\,),\ r = 0, 1, 2.$$

Очевидно, що φ – однозначне відображення $\mathbb{Z}_{12}$ на $\mathbb{Z}_3$. Покажемо, що зберігаються операції додавання і множення.

Нехай $K_a^{(12)}, K_b^{(12)}$ – довільні два елементи із $\mathbb{Z}_{12}$ і нехай $a + b \equiv r_1 \,(\mathrm{mod}\, 3\,)$, $ab \equiv r_2 \,(\mathrm{mod}\, 3\,)$, $r_1, r_2 \in \{0, 1, 2\}$. Тоді:

$$\varphi(K_a^{(12)}+K_b^{(12)}) = \varphi(K_{a+b}^{(12)}) = K_{r_1}^{(3)} = K_{a+b}^{(3)} = K_a^{(3)}+K_b^{(3)} = \varphi(K_a^{(12)})+\varphi(K_b^{(12)});$$

$$\varphi(K_a^{(12)} \cdot K_b^{(12)}) = \varphi(K_{ab}^{(12)}) = K_{r_2}^{(3)} = K_{ab}^{(3)} = K_a^{(3)} \cdot K_b^{(3)} = \varphi(K_a^{(12)}) \cdot \varphi(K_b^{(12)}).$$

Таким чином, операції зберігаються, значить, φ – гомоморфізм кільця $\mathbb{Z}_{12}$ на кільце $\mathbb{Z}_3$. Ядром цього гомоморфізму є множина таких класів лишків $K_a^{(12)} \in \mathbb{Z}_{12}$, що відображаються в нульовий елемент кільця, тобто

$$\varphi(K_a^{(12)}) = K_0^{(3)}.$$

В силу задання відображення φ, $a \equiv 0 \,(\mathrm{mod}\, 3\,)$, $0 \leqslant a \leqslant 11$. Тоді $a = 0, 3, 6, 9$ і $\mathrm{Ker}\,\varphi = \left\{K_0^{(12)}, K_3^{(12)}, K_6^{(12)}, K_9^{(12)}\right\} = 3\mathbb{Z}_{12}$.

В силу основної теореми про гомоморфізми кілець, фактор-кільце $\mathbb{Z}_{12}/3\mathbb{Z}_{12}$ ізоморфне кільцю $\mathbb{Z}_3$.

Розв'язання в Maple. Задаємо кільця $K = \mathbb{Z}_{12}$ і $L = \mathbb{Z}_3$:

```
> K:={$0..11}:
  plus1:=(A,B)->A+B mod 12:
  mult1:=(A,B)->A*B mod 12:
> L:={$0..2}:
> plus2:=(X,Y)->X+Y mod 3:
> mult2:=(X,Y)->X*Y mod 3:
```

Тепер задаємо відображення $\varphi : K \to L$:

```
> PHI:=X -> X mod 3:
```

Покажемо, що φ – гомоморфізм кільця K на кільце L. Для цього використовуємо процедури, створені при розв'язанні Прикладу 28.1. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Маємо:

```
> existsIm(PHI,K,L);
```

true

```
> existsProim(PHI,K,L);
```

true

```
> savesOperation(PHI,K,L,plus1,plus2);
```

true

```
> savesOperation(PHI,K,L,mult1,mult2);
```

true

Отже, φ – гомоморфізм кільця K на кільце L. Знайдемо ядро цього гомоморфізму:

```
> kerPHI(PHI,K,L,plus1);
```

$\{0, 3, 6, 9\}$

Але $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = 3\mathbb{Z}_{12}$. Тому, в силу основної теореми про гомоморфізм кілець, $\mathbb{Z}_{12}/3\mathbb{Z}_{12} \cong 3\mathbb{Z}_3$.

Завдання 29. Довести, що:

29.1. $\mathbb{Z}_{16}/4\mathbb{Z}_{16} \cong \mathbb{Z}_4$.

29.2. $\mathbb{Z}_{10}/5\mathbb{Z}_{10} \cong \mathbb{Z}_5$.

29.3. $\mathbb{Z}_{15}/3\mathbb{Z}_{15} \cong \mathbb{Z}_3$.

29.4. $\mathbb{Z}_8/4\mathbb{Z}_8 \cong \mathbb{Z}_4$.

29.5. $\mathbb{Z}_{20}/10\mathbb{Z}_{20} \cong \mathbb{Z}_{10}$.

29.6. $\mathbb{Z}_6/2\mathbb{Z}_6 \cong \mathbb{Z}_2$.

29.7. $\mathbb{Z}_{18}/9\mathbb{Z}_{18} \cong \mathbb{Z}_9$.

29.8. $\mathbb{Z}_{12}/4\mathbb{Z}_{12} \cong \mathbb{Z}_4$.

29.9. $\mathbb{Z}_{21}/3\mathbb{Z}_{21} \cong \mathbb{Z}_3$.

29.10. $\mathbb{Z}_{14}/7\mathbb{Z}_{14} \cong \mathbb{Z}_7$.

29.11. $\mathbb{Z}_{20}/5\mathbb{Z}_{20} \cong \mathbb{Z}_5$.

29.12. $\mathbb{Z}_{16}/2\mathbb{Z}_{16} \cong \mathbb{Z}_2$.

29.13. $\mathbb{Z}_{18}/3\mathbb{Z}_{18} \cong \mathbb{Z}_3$.

29.14. $\mathbb{Z}_{12}/2\mathbb{Z}_{12} \cong \mathbb{Z}_2$.

29.15. $\mathbb{Z}_6/3\mathbb{Z}_6 \cong \mathbb{Z}_3$.

29.16. $\mathbb{Z}_{14}/2\mathbb{Z}_{14} \cong \mathbb{Z}_2$.

29.17. $\mathbb{Z}_{15}/5\mathbb{Z}_{15} \cong \mathbb{Z}_5$.

29.18. $\mathbb{Z}_{21}/7\mathbb{Z}_{21} \cong \mathbb{Z}_7$.

29.19. $\mathbb{Z}_{18}/6\mathbb{Z}_{18} \cong \mathbb{Z}_6$.

29.20. $\mathbb{Z}_8/2\mathbb{Z}_8 \cong \mathbb{Z}_2$.

29.21. $\mathbb{Z}_{20}/4\mathbb{Z}_{20} \cong \mathbb{Z}_4$.

29.22. $\mathbb{Z}_{12}/6\mathbb{Z}_{12} \cong \mathbb{Z}_6$.

29.23. $\mathbb{Z}_{10}/2\mathbb{Z}_{10} \cong \mathbb{Z}_2$.

29.24. $\mathbb{Z}_{16}/8\mathbb{Z}_{16} \cong \mathbb{Z}_8$.

29.25. $\mathbb{Z}_{24}/4\mathbb{Z}_{24} \cong \mathbb{Z}_4$.

6. Кільця, що є областями цілісності

ТЕОРЕТИЧНІ ВІДОМОСТІ

Комутативне кільце з одиницею без дільників нуля називається **областю цілісності.** Елементи a і b області цілісності K називаються **асоційованими** в K (пишуть $a \sim b$), якщо $a = b\varepsilon$, де ε – дільник одиниці K.

Нехай K – область цілісності. Тоді:

1°. $a \sim b$ в K тоді і лише тоді, коли $a \vdots b$ і $b \vdots a$ в K (критерій асоційованості).
2°. $a \sim b$ в K тоді і лише тоді, коли $\langle a \rangle = \langle b \rangle$ в K.
3°. $\langle a \rangle = K$ тоді і лише тоді, коли $a|1$ в K.

Елемент c області цілісності K називається спільним дільником елементів a і b із K, якщо $a \vdots c$ і $b \vdots c$ в K. **Найбільшим спільним дільником** елементів a і b області цілісності K називається такий спільний дільник цих елементів, який ділиться на будь-який їхній спільний дільник. Якщо d – найбільший спільний дільник елементів a і b, то пишуть: $d \sim (a, b)$.

Елементи a і b області цілісності K називаються взаємно простими (пишуть: $(a, b) \sim 1$), якщо вони не мають спільних дільників, відмінних від дільників одиниці.

Елемент g області цілісності K називається спільним кратним елементів a і b із K, якщо $g \vdots a$ і $g \vdots b$ в K. **Найменшим спільним кратним** елементів a і b області цілісності K називається таке спільне кратне цих елементів, яке є дільником будь-якого їхнього спільного кратного. Якщо m – найменше спільне кратне елементів a і b, то це позначають так: $m \sim [a, b]$.

Нехай a, b – довільні елементи області цілісності K. Тоді:

1$^\flat$. Якщо d і d_1 – найбільші спільні дільники чисел a і b, то $d = d_1\varepsilon$, де ε – дільник одиниці кільця K.
2$^\flat$. Якщо d – найбільший спільний дільник чисел a і b, а $\varepsilon_1, \varepsilon_2, ..., \varepsilon_s, ...$ – дільники одиниці цього кільця, то найбільшими спільними дільниками елементів a і b є також елементи: $d\varepsilon_1, d\varepsilon_2, ..., d\varepsilon_s, ...$.
3$^\flat$. Якщо m і m_1 – найменші спільні кратні елементів a і b, то $m = m_1\varepsilon$, де ε – дільник одиниці області цілісності K.
4$^\flat$. Якщо $m = [a, b]$, $\varepsilon_1, \varepsilon_2, ..., \varepsilon_s, ...$ – дільники одиниці цього кільця, то найменшими спільними кратними елементів a і b є також елементи: $m\varepsilon_1, m\varepsilon_2, ..., m\varepsilon_s, ...$.

Нехай a – довільний елемент, ε – довільний дільник одиниці області цілісності K. Тоді завжди $a \vdots \varepsilon$ і $a \vdots a\varepsilon$. Дільники елемента a в K, відмінні від ε і $a\varepsilon$, називаються **нетривіальними** (або **власними**) дільниками елемента a.

Елемент $0 \neq a \in K$, що не є дільником одиниці, називається **простим** в K, якщо він не має нетривіальних дільників в K. Елемент $0 \neq a \in K$ називається **складеним** в K, якщо він має нетривіальні дільники. Елемент $0 \neq a \in K$ є простим в K тоді і лише тоді, коли запис $a = b \cdot c$, де $b, c \in K$, можливий лише за умови, що хоча б один із співмножників b або c є дільником одиниці кільця K. Елемент $0 \neq a \in K$ є складеним в K, якщо $a = b \cdot c$, де b, c – відмінні від дільників одиниці елементи із K. Поняття простоти та складеності є відносним. Все залежить від того, до якої області цілісності належить даний елемент.

Область цілісності, в якій всі ідеали головні, називається **кільцем головних ідеалів.** Якщо K – кільце головних ідеалів, то для довільних елементів $a, b \in K$ в K завжди існує найбільший спільний дільник d елементів a і b, причому $d = au + bv$, де $u, v \in K$.

Область цілісності K називається **евклідовим кільцем**, якщо можна задати правило Nr, яке кожному ненульовому елементу кільця K ставить у відповідність деяке невід'ємне ціле число так, що виконуються умови:

1) якщо $a, b \in K\backslash\{0\}$ і $a \vdots b$ в K, то $\mathrm{Nr}(a) \geqslant \mathrm{Nr}(b)$;
2) для будь-яких a, b із K, $b \neq 0$, існують в K елементи q і r такі, що $a = bq + r$, де або $r = 0$, або $\mathrm{Nr}(r) < \mathrm{Nr}(b)$.

Число $\mathrm{Nr}(a)$ називається евклідовою нормою елемента a.

В евклідовому кільці K з евклідовою нормою $\mathrm{Nr}(x)$ розділити елемент a на елемент $b \neq 0$ з остачею означає представити його у вигляді

$$a = bq + r, \text{ де } q, r \in K \text{ і } \mathrm{Nr}(r) < \mathrm{Nr}(b) \text{ або } r = 0.$$

При цьому елементи q і r називаються відповідно неповною часткою і остачею від ділення a на b.

Теорема. *Найбільший спільний дільник двох ненульових елементів a і b евклідового кільця K асоційований з останньою, відмінною від нуля, остачею алгоритму Евкліда.*

Говорять, що елемент a області цілісності K володіє однозначним розкладом на прості множники, якщо виконуються умови:

1) в K існують прості елементи $p_1,\ p_2,\ \ldots,\ p_s$ такі, що $a = p_1 p_2 \ldots p_s$;
2) якщо $a = q_1 q_2 \ldots q_t$ – інший розклад, в якому $q_1, q_2, \ldots, q_t$ – прості елементи в K, то $s = t$ і, при відповідній нумерації, $p_i \sim q_i$ для $i = 1, 2, ..., s$.

Кільце K називається **факторіальним**, якщо воно є областю цілісності і всякий відмінний від нуля елемент, що не є дільником одиниці, володіє однозначним розкладом на прості множники.

Нехай a, b – довільні елементи факторіального кільця K. Тоді:

$1^\flat$. Якщо $a = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$, де $p_1, p_2, ..., p_s$ – попарно не асоційовані прості елементи кільця K, $k_i \in \mathbb{N}$, $1 \leqslant i \leqslant s$, $s \in \mathbb{N}$, то множина дільників елемента a вичерпується елементами d виду: $d = \varepsilon p_1^{l_1} p_2^{l_2} ... p_s^{l_s}$, де $0 \leqslant l_i \leqslant k_i$, $1 \leqslant i \leqslant s$, ε – дільник одиниці кільця K.

$2^\flat$. Нехай $a = \varepsilon_1 p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, $b = \varepsilon_2 p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s}$, де $p_1, p_2, ..., p_s$ – попарно не асоційовані елементи кільця K, ε_1, ε_2 – дільники одиниці цього кільця, $k_1, k_2, ..., k_s$, $l_1, l_2, ..., l_s$ – натуральні числа або нуль, $s \in \mathbb{N}$. Тоді

$$(a, b) \sim p_1^{t_1} p_2^{t_2} ... p_s^{t_s}, \text{ де } t_i = \min_{1 \leqslant i \leqslant s} \{k_i, l_i\},$$
$$[a, b] \sim p_1^{m_1} p_2^{m_2} ... p_s^{m_s}, \text{ де } m_i = \max_{1 \leqslant i \leqslant s} \{k_i, l_i\}.$$

$3^\flat$. Якщо a, b – ненульові елементи факторіального кільця K, то

$$[a, b] \sim \frac{ab}{(a, b)}. \tag{III.18}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 30.1. Визначити, чи є асоційованими в області цілісності $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} | a, b \in \mathbb{Z}\right\}$ елементи $25 - 17\sqrt{2}$ і $7 - \sqrt{2}$.

Розв'язання. Перевіримо спочатку, чи ділиться елемент $25 - 17\sqrt{2}$ на елемент $7 - \sqrt{2}$:

$$\frac{25 - 17\sqrt{2}}{7 - \sqrt{2}} = \frac{(25 - 17\sqrt{2})(7 + \sqrt{2})}{(7 - \sqrt{2})(7 + \sqrt{2})} = \frac{141 - 94\sqrt{2}}{47} = 3 - 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$

значить, в $\mathbb{Z}[\sqrt{2}]$ знайдеться елемент $c = 3 - 2\sqrt{2}$ такий, що $25 - 17\sqrt{2} = (7 - \sqrt{2}) \cdot c$. Отже, $(25 - 17\sqrt{2}) \vdots (7 - \sqrt{2})$ в $\mathbb{Z}[\sqrt{2}]$.

Перевіримо тепер, чи ділиться елемент $7 - \sqrt{2}$ на елемент $25 - 17\sqrt{2}$:

$$\frac{7 - \sqrt{2}}{25 - 17\sqrt{2}} = \frac{(7 - \sqrt{2})(25 + 17\sqrt{2})}{(25 - 17\sqrt{2})(25 + 17\sqrt{2})} = \frac{141 + 94\sqrt{2}}{47} = 3 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Отже, $(7 - \sqrt{2}) \vdots (25 - 17\sqrt{2})$ в $\mathbb{Z}[\sqrt{2}]$.

В силу критерію асоційованості, $(25 - 17\sqrt{2}) \sim (7 - \sqrt{2})$ в $\mathbb{Z}[\sqrt{2}]$.

Розробка процедур. Для створення процедури **areAssociated**, яка для заданих елементів a і b визначатиме, чи виконується умова $a \sim b$ в K, використаємо команду **patmatch** (див. Приклад 23.1). В ході процедури перевіряємо, чи виконується умова критерію асоційованості: $a \vdots b$ і $b \vdots a$ в K. Кільце K задаємо за допомогою шаблону pattern.

```
areAssociated:=proc(a,b,pattern)
local z1,z2;
   z1:=expand(rationalize(a/b));
   z2:=expand(rationalize(b/a));
   patmatch(z1,pattern) and patmatch(z2,pattern);
end proc:
```

Розв'язання в Maple. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і застосовуємо розроблену процедуру:

```
> areAssociated(25-17*sqrt(2),7-sqrt(2),
                      x::integer+y::integer*sqrt(2));
```

true

Отже, $(25 - 17\sqrt{2}) \sim (7 - \sqrt{2})$ в $\mathbb{Z}[\sqrt{2}]$

Приклад 30.2. Визначити, чи є асоційованими в області цілісності $\mathbb{Z}[i] = \left\{a + b\sqrt{i} | a, b \in \mathbb{Z}\right\}$ елементи $5 + 4i$ та $-2 + 23i$.

Розв'язання. Спосіб I. Перевіримо, чи ділиться елемент $5 + 4i$ на елемент $2 + 23i$ в $\mathbb{Z}[i]$:

$$\frac{5+4i}{2+23i} = \frac{(5+4i)(2-23i)}{(2+23i)(2-23i)} = \frac{82-123i}{533} = \frac{82}{533} - \frac{123}{533}i \notin \mathbb{Z}[i],$$

отже, $(5+4i) \vdots (2+23i)$ в $\mathbb{Z}[i]$, значить, в силу означення, елементи $5 + 4i$ та $-2 + 23i$ не є асоційованими в $\mathbb{Z}[i]$.

Спосіб II. В силу 2°, елементи $5 + 4i$ та $-2 + 23i$ є асоційованими в $\mathbb{Z}[i]$ тоді і лише тоді, коли виконується умова

$$5 + 4i = (-2 + 23i) \cdot \varepsilon, \tag{III.19}$$

де ε – дільник одиниці кільця $\mathbb{Z}[i]$. Дільниками одиниці кільця $\mathbb{Z}[i]$ є лише елементи $1, -1, i, -i$. Безпосередньою перевіркою неважко переконатись, що жоден із цих елементів не задовольняє рівність (III.19). Отже, елементи $5 + 4i$ та $-2 + 23i$ не є асоційованими в $\mathbb{Z}[i]$.

Розв'язання в Maple. Використовуємо процедуру **areAssociated**, створену при розв'язанні Прикладу 30.1. Зауважимо, що при заданні шаблону **pattern** використовуємо тип complex(integer) – ціле гаусове число.

```
> read(‘e:/atchlib.m‘); with(atchlib):
> areAssociated(5+4*I,2+23*I,x::complex(integer));
```

false

Завдання 30. Визначити, чи є асоційованими в області цілісності K елементи a і b, якщо:

30.1. $a = 50 + 29\sqrt{3}$, $b = 2 + 3\sqrt{3}$, $K = \mathbb{Z}[\sqrt{3}]$.

30.2. $a = 3 - 7\sqrt{5}$, $b = 113 + 51\sqrt{5}$, $K = \mathbb{Z}[\sqrt{5}]$.

30.3. $a = 5 + 2i$, $b = 17 + i$, $K = \mathbb{Z}[i]$.

30.4. $a = -7 + 6\sqrt{2}$, $b = 70 - 37\sqrt{2}$, $K = \mathbb{Z}[\sqrt{2}]$.

30.5. $a = 55 + 6\sqrt{7}$, $b = 4 + 3\sqrt{7}$, $K = \mathbb{Z}[\sqrt{7}]$.

30.6. $a = 25 - 24\sqrt{5}$, $b = 15 + 2\sqrt{5}$, $K = \mathbb{Z}[\sqrt{5}]$.

30.7. $a = 47 + 10\sqrt{2}$, $b = 11 - 4\sqrt{2}$, $K = \mathbb{Z}[\sqrt{2}]$.

30.8. $a = -45 - 59\sqrt{3}$, $b = 5 - 7\sqrt{3}$, $K = \mathbb{Z}[\sqrt{3}]$.

30.9. $a = 12 + 7\sqrt{5}$, $b = 11 - 2\sqrt{5}$, $K = \mathbb{Z}[\sqrt{5}]$.

30.10. $a = 3 + 5i$, $b = -5 + 3i$, $K = \mathbb{Z}[i]$.

30.11. $a = 9 + 11\sqrt{2}$, $b = 5 + 3\sqrt{2}$, $K = \mathbb{Z}[\sqrt{2}]$

30.12. $a = 96 - 29\sqrt{11}$, $b = 3 - 2\sqrt{11}$, $K = \mathbb{Z}[\sqrt{11}]$.

30.13. $a = 3 + 7\sqrt{3}$, $b = 15 - 11\sqrt{3}$, $K = \mathbb{Z}[\sqrt{3}]$.

30.14. $a = -17 + 9\sqrt{5}$, $b = 7 - 3\sqrt{5}$, $K = \mathbb{Z}[\sqrt{5}]$.

30.15. $a = 6 - 7i$, $b = 6 + 7i$, $K = \mathbb{Z}[i]$.

30.16. $a = 13 - 9\sqrt{2}$, $b = 5 + 3\sqrt{2}$, $K = \mathbb{Z}[\sqrt{2}]$

30.17. $a = 5 + 2\sqrt{7}$, $b = 82 + 31\sqrt{7}$, $K = \mathbb{Z}[\sqrt{7}]$.

30.18. $a = 46 - 32\sqrt{3}$, $b = 2 + 9\sqrt{3}$, $K = \mathbb{Z}[\sqrt{3}]$.

30.19. $a = 6 - 5\sqrt{2}$, $b = 18 + 13\sqrt{2}$, $K = \mathbb{Z}[\sqrt{2}]$.

30.20. $a = 13 + 4\sqrt{5}$, $b = 6 - 5\sqrt{5}$, $K = \mathbb{Z}[\sqrt{5}]$.

30.21. $a = 2 - i$, $b = 7 + 4i$, $K = \mathbb{Z}[i]$.

30.22. $a = 5 + 2\sqrt{11}$, $b = 29 + 4\sqrt{11}$, $K = \mathbb{Z}[\sqrt{11}]$.

30.23. $a = 84 + 17\sqrt{2}$, $b = 3 + 5\sqrt{2}$, $K = \mathbb{Z}[\sqrt{2}]$.

30.24. $a = 2 - 5\sqrt{5}$, $b = 118 - 53\sqrt{5}$, $K = \mathbb{Z}[\sqrt{5}]$.

30.25. $a = -31 + 18\sqrt{3}$, $b = 4 + 3\sqrt{3}$, $K = \mathbb{Z}[\sqrt{3}]$.

Приклад 31.1. Визначити, чи виконується для елемента $2 + \sqrt{3}$ кільця $\mathbb{Z}[\sqrt{3}]$ умова: $\langle 2 + \sqrt{3} \rangle = \mathbb{Z}[\sqrt{3}]$.

Розв'язання. Кільце $\mathbb{Z}[\sqrt{3}]$ є комутативним кільцем з одиницею $1+0\sqrt{3} = 1$, елемент $2+\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Покажемо, що елемент $2+\sqrt{3}$ є дільником одиниці кільця $\mathbb{Z}[\sqrt{3}]$. Дійсно,

$$\frac{1}{2+\sqrt{3}} = \frac{2-\sqrt{3}}{(2+\sqrt{3})(2-\sqrt{3})} = \frac{2-\sqrt{3}}{4-3} = 2 - \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

тобто $1 \vdots (2+\sqrt{3})$ в $\mathbb{Z}[\sqrt{3}]$. Значить, $2+\sqrt{3} = \varepsilon \in \mathbb{Z}[\sqrt{3}]$. В силу властивості 3°, $\langle 2+\sqrt{3}\rangle = \langle \varepsilon \rangle = \mathbb{Z}[\sqrt{3}]$.

Розв'язання в Maple. В силу властивості 3°, елемент $a \in K$ задовольняє умову $\langle a \rangle = K$ тоді і лише тоді, коли $a|1$ в K (тобто $a \sim 1$ в K). Тому для перевірки заданої умови можна застосувати процедуру **areAssociated**, створену при розв'язанні Прикладу 30.1:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> areAssociated(2+sqrt(3),1,x::integer+y::integer*sqrt(3));
```

true

Отже, $\langle 2+\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$.

Приклад 31.2. Визначити, чи один і той самий головний ідеал кільця $\mathbb{Z}[i]$ породжують елементи $5+2i$ і $2-5i$ (тобто чи виконується умова $\langle 5+2i\rangle = \langle 2-5i\rangle$ в $\mathbb{Z}[i]$).

Розв'язання. Оскільки $5+2i = (2-5i)(-i)$, $-i = \varepsilon$ – дільник одиниці кільця $\mathbb{Z}[i]$, то, в силу твердження 2°,

$$5+2i \sim (2-5i).$$

Тоді за твердженням 1° $\langle 5+2i\rangle = \langle 2-5i\rangle$ в $\mathbb{Z}[i]$).

Розв'язання в Maple. За твердженням 1°, для елементів a і b кільця K виконується умова $\langle a\rangle = \langle b\rangle$ тоді і лише тоді, коли $a \sim b$ в K. Тому для перевірки заданої умови достатньо, як і у Прикладі 31.1, застосувати процедуру **areAssociated**:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> areAssociated(5+2*I,2-5*I,x::complex(integer));
```

true

Отже, $\langle 5+2i\rangle = \langle 2-5i\rangle$ в $\mathbb{Z}[i]$.

Завдання 31. Визначити, чи виконуються умови:

31.1. а) $\langle 9-4\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 5+i\rangle = \langle -1+4i\rangle$ в $\mathbb{Z}[i]$.

31.2. а) $\langle -10+\sqrt{101}\rangle = \mathbb{Z}[\sqrt{101}]$;
б) $\langle 2-3i\rangle = \langle 3+i\rangle$ в $\mathbb{Z}[i]$.

31.3. а) $\langle -7+4\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle 1+4i\rangle = \langle 4-i\rangle$ в $\mathbb{Z}[i]$.

31.4. а) $\langle 10-2\sqrt{11}\rangle = \mathbb{Z}[\sqrt{11}]$;
б) $\langle 7-2i\rangle = \langle 4+5i\rangle$ в $\mathbb{Z}[i]$.

31.5. а) $\langle -16+\sqrt{257}\rangle = \mathbb{Z}[\sqrt{257}]$;
б) $\langle 3+5i\rangle = \langle -5+3i\rangle$ в $\mathbb{Z}[i]$.

31.6. а) $\langle -2+\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 2+i\rangle = \langle 1-2i\rangle$ в $\mathbb{Z}[i]$.

31.7. а) $\langle 199+60\sqrt{11}\rangle = \mathbb{Z}[\sqrt{11}]$;
б) $\langle 7+3i\rangle = \langle -3+7i\rangle$ в $\mathbb{Z}[i]$.

31.8. а) $\langle 8+3\sqrt{7}\rangle = \mathbb{Z}[\sqrt{7}]$;
б) $\langle 5-4i\rangle = \langle 4+5i\rangle$ в $\mathbb{Z}[i]$.

31.9. а) $\langle 26-15\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle 1-6i\rangle = \langle 6+i\rangle$ в $\mathbb{Z}[i]$.

31.10. а) $\langle 2+\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 2+7i\rangle = \langle 7-2i\rangle$ в $\mathbb{Z}[i]$.

31.11. а) $\langle -6+\sqrt{37}\rangle = \mathbb{Z}[\sqrt{37}]$;
б) $\langle 5-2i\rangle = \langle 2+5i\rangle$ в $\mathbb{Z}[i]$.

31.12. а) $\langle 97+6\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle 3-2i\rangle = \langle -3+2i\rangle$ в $\mathbb{Z}[i]$.

31.13. а) $\langle 8-3\sqrt{7}\rangle = \mathbb{Z}[\sqrt{7}]$;
б) $\langle 1-2i\rangle = \langle 2+i\rangle$ в $\mathbb{Z}[i]$.

31.14. а) $\langle 7-4\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle 7-i\rangle = \langle 1-7i\rangle$ в $\mathbb{Z}[i]$.

31.15. а) $\langle -14+\sqrt{195}\rangle = \mathbb{Z}[\sqrt{195}]$;
б) $\langle 5+2i\rangle = \langle 2-5i\rangle$ в $\mathbb{Z}[i]$.

31.16. а) $\langle 9+4\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 8-3i\rangle = \langle -3-8i\rangle$ в $\mathbb{Z}[i]$.

31.17. а) $\langle 10+3\sqrt{11}\rangle = \mathbb{Z}[\sqrt{11}]$;
б) $\langle -1+3i\rangle = \langle -3-i\rangle$ в $\mathbb{Z}[i]$.

31.18. а) $\langle 26+15\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle 3-7i\rangle = \langle 7+3i\rangle$ в $\mathbb{Z}[i]$.

31.19. а) $\langle 2-\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 6-5i\rangle = \langle -5+6i\rangle$ в $\mathbb{Z}[i]$.

31.20. а) $\langle -9+4\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 1+4i\rangle = \langle -4+i\rangle$ в $\mathbb{Z}[i]$.

31.21. а) $\langle 6+4\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle -11+2i\rangle = \langle 2+11i\rangle$ в $\mathbb{Z}[i]$.

318.22. а) $\langle -10+3\sqrt{11}\rangle = \mathbb{Z}[\sqrt{11}]$;
б) $\langle 6-i\rangle = \langle 1+6i\rangle$ в $\mathbb{Z}[i]$.

31.23. а) $\langle 38-17\sqrt{5}\rangle = \mathbb{Z}[\sqrt{5}]$;
б) $\langle 3+8i\rangle = \langle -8+3i\rangle$ в $\mathbb{Z}[i]$.

31.24. а) $\langle -8+3\sqrt{7}\rangle = \mathbb{Z}[\sqrt{7}]$;
б) $\langle -2+9i\rangle = \langle 9+2i\rangle$ в $\mathbb{Z}[i]$.

31.25. а) $\langle -2-\sqrt{3}\rangle = \mathbb{Z}[\sqrt{3}]$;
б) $\langle -1-7i\rangle = \langle 7-i\rangle$ в $\mathbb{Z}[i]$.

Приклад 32.1. Визначити, простим чи складеним є число 13, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел;
б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

Розв'язання. а) Число 13 не є дільником одиниці кільця $\mathbb{Z}$ цілих чисел, і його дільниками є лише числа $1, -1, 13, -13$, тобто цей елемент в $\mathbb{Z}$ має лише тривіальні дільники. За означенням число 13 є простим в $\mathbb{Z}$.

б) Як відомо, дільниками одиниці кільця $\mathbb{Z}[i]$ цілих гаусових чисел є: $i, -i, 1, -1$. Оскільки $13 = 2^2 + 3^2$, то число 13 можна записати у вигляді:

$$13 = (2 - 3i)\,(2 + 3i)\,,$$

де числа $2 - 3i$ і $2 + 3i$ не є дільниками одиниці кільця $\mathbb{Z}[i]$. Отже, число 13 є складеним елементом кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

Розв'язання в Maple. Визначимо спочатку, чи є число 13 простим елементом кільця $\mathbb{Z}$ цілих чисел:

```
> with(numtheory):
  isprime(13);
```

true

Отже, 13 є простим в $\mathbb{Z}$.

Для роботи з цілими гаусовими числами в Maple створено спеціальний пакет **GaussInt**. Визначимо, чи є число 13 простим елементом кільця $\mathbb{Z}[i]$:

```
> with(GaussInt):
  GIprime(13);
```

false

В кільці $\mathbb{Z}[i]$ елемент 13 не є простим. Команда **GIfactor(a)** дозволяє знайти один із можливих розкладів числа $a \in \mathbb{Z}[i]$ в добуток простих елементів кільця $\mathbb{Z}[i]$.

```
> GIfactor(13);
```

$$(-3 - 2\,I)\ \ (-3 + 2\,I)$$

Приклад 32.2. Визначити, простим чи складеним в кільці $\mathbb{Z}[i]$ цілих гаусових чисел є:

а) елемент $2 + i$; б) елемент $5 - 3i$.

Розв'язання. а) Заданий елемент $2 + i$ не є дільником одиниці в кільці $\mathbb{Z}[i]$ (оскільки, як відомо, в кільці $\mathbb{Z}[i]$ дільниками одиниці є лише числа $1, -1, i, -i$). Нехай

$$2 + i = (a + bi)(c + di), \tag{III.20}$$

де $a, b, c, d \in \mathbb{Z}$. Використаємо норму цілого гаусового числа:

$$\text{якщо } z = a + bi \in \mathbb{Z}[i], \quad \text{то } \mathrm{Nr}(z) = |z|^2 = a^2 + b^2.$$

Із рівності (III.20) маємо: $\mathrm{Nr}(2 + i) = \mathrm{Nr}\big((a + bi)(c + di)\big)$. Оскільки $\mathrm{Nr}(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 |z_2|^2 = \mathrm{Nr}(z_1)\mathrm{Nr}(z_2)$, то

$$\mathrm{Nr}(2 + i) = \mathrm{Nr}(a + bi)\mathrm{Nr}(c + di),$$

значить,

$$5 = (a^2 + b^2)(c^2 + d^2).$$

Для цілих чисел a, b, c, d остання рівність можлива тоді і лише тоді, коли

$$\begin{cases} a^2 + b^2 = 5, \\ c^2 + d^2 = 1; \end{cases} \quad \text{або навпаки:} \quad \begin{cases} a^2 + b^2 = 1, \\ c^2 + d^2 = 5. \end{cases}$$

Очевидно, достатньо розглянути лише одну із даних систем. Із другого рівняння першої системи випливає, що або $c = \pm 1$, $d = 0$, або $c = 0$, $d = \pm 1$, звідки

$$c + di = \pm 1 + 0i = \pm 1, \qquad \text{або} \qquad c + di = 0 \pm 1i = \pm i,$$

тобто $c + di$ є дільником одиниці. Це означає, що число $2 + i$ – просте в $\mathbb{Z}[i]$.

б) Очевидно, елемент $5 - 3i$ не є дільником одиниці в $\mathbb{Z}[i]$. Доведемо, що він є складеним в $\mathbb{Z}[i]$. Нехай

$$5 - 3i = (a + bi)(c + di),$$

де $a, b, c, d \in \mathbb{Z}$. Знайдемо норму від обох частин останньої рівності: $\mathrm{Nr}(5 - 3i) = \mathrm{Nr}\big((a + bi)(c + di)\big)$. Тоді $\mathrm{Nr}(5 - 3i) = \mathrm{Nr}(a + bi)\mathrm{Nr}(c + di)$, звідки

$$34 = (a^2 + b^2)(c^2 + d^2).$$

Легко бачити, що одним із розв'язків останнього рівняння є такий: $a = 4$, $b = -1$, $c = 1$, $d = 1$. Тоді

$$5 - 3i = (4 - i)(1 + i),$$

де елементи $4 - i$, $1 + i$ не є дільниками одиниці кільця $\mathbb{Z}[i]$. Отже, елемент $5 - 3i$ є складеним в $\mathbb{Z}[i]$.

Розв'язання в Maple. Аналогічно до попереднього прикладу:

```
> with(GaussInt):
  GIprime(2+I);
```

true

Елемент $2 + i$ є простим в $\mathbb{Z}[i]$.

```
> GIprime(5-3*I);
```

false

Елемент $5 - 3i$ є складеним в $\mathbb{Z}[i]$; один із його розкладів в добуток простих в $\mathbb{Z}[i]$ елементів має вигляд:

```
> GIfactor(5-3*I);
```

$$(1 + I)\ (1 - 4\,I)$$

Приклад 32.3. Визначити, простим чи складеним в кільці $\mathbb{Z}[\sqrt{3}i]$ є елемент $2+\sqrt{3}i$.

Розв'язання. Заданий елемент $2+\sqrt{3}i$ не є дільником одиниці в кільці $\mathbb{Z}[\sqrt{3}i]$ (оскільки, як відомо, в кільці $\mathbb{Z}[\sqrt{p}i]$, p – просте, дільниками одиниці є лише числа $1, -1$). Нехай

$$2+\sqrt{3}i = (a+b\sqrt{3}i)(c+d\sqrt{3}i).$$

де $a, b, c, d \in \mathbb{Z}$. Тоді

$$|2+\sqrt{3}i|^2 = |(a+b\sqrt{3}i)(c+d\sqrt{3}i)|^2,$$

тобто

$$|2+\sqrt{3}i|^2 = |a+b\sqrt{3}i|^2|c+d\sqrt{3}i|^2.$$

Звідси,

$$7 = (a^2+3b^2)(c^2+3d^2).$$

Оскільки a, b, c, d – цілі числа, то остання рівність можлива лише у двох випадках:

$$1)\ \begin{cases} a^2+3b^2=7, \\ c^2+3d^2=1; \end{cases} \quad \text{або} \quad 2)\ \begin{cases} a^2+3b^2=1, \\ c^2+3d^2=7. \end{cases}$$

Із другого рівняння системи 1) випливає, що або $c=1$, $d=0$, або $c=-1$, $d=0$. Але тоді $c+d\sqrt{3}i = 1+0\sqrt{3}i = 1$, або $c+d\sqrt{3}i = -1+0\sqrt{3}i = -1$, тобто $c+d\sqrt{3}i$ є дільником одиниці в $\mathbb{Z}[\sqrt{3}i]$. Аналогічно у другому випадку елемент $a+b\sqrt{3}i$ є дільником одиниці. Це означає, що елемент $2+\sqrt{3}i$ є простим в $\mathbb{Z}[\sqrt{3}i]$.

Розв'язання в Maple. Команди для перевірки на простоту елемента кільця $\mathbb{Z}[\sqrt{3}i]$ в Maple немає. Використаємо команду **factorEQ(a,d)** (із пакету **numtheory**), за допомогою якої можна знайти розклад елемента $a \in \mathbb{Z}[\sqrt{d}]$ (де $d \in \mathbb{Z}$) на прості множники. Відмітимо, що $\mathbb{Z}[\sqrt{d}i] = \mathbb{Z}[\sqrt{-d}]$.

```
> with(numtheory):
  factorEQ(2+sqrt(3)*I,-3);
```

$$(2+\sqrt{3}\,I)$$

Це означає, що елемент $2+\sqrt{3}i$ є простим в $\mathbb{Z}[\sqrt{3}i]$.

Завдання 32. Визначити, простим чи складеним:

32.1. в кільці $\mathbb{Z}[i]$ є елемент $3+2i$.

32.2. є число 5, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.3. в кільці $\mathbb{Z}[\sqrt{5}i]$ є елемент $3 + 2\sqrt{5}i$.

32.4. в кільці $\mathbb{Z}[i]$ є елемент $4 - i$.

32.5. є число 19, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.6. в кільці $\mathbb{Z}[\sqrt{3}i]$ є елемент $1 + 2\sqrt{3}i$.

32.7. в кільці $\mathbb{Z}[i]$ є елемент $3 + 5i$.

32.8. є число 3, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.9. в кільці $\mathbb{Z}[\sqrt{7}i]$ є елемент $2 + \sqrt{7}i$.

32.10. в кільці $\mathbb{Z}[i]$ є елемент $2 - 3i$.

32.11. в кільці $\mathbb{Z}[\sqrt{3}i]$ є елемент $11 + 3\sqrt{3}i$.

32.12. є число 23, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.13. в кільці $\mathbb{Z}[i]$ є елемент $3 + i$.

32.14. в кільці $\mathbb{Z}[\sqrt{5}i]$ є елемент $3 - \sqrt{5}i$.

32.15. є число 7, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.16. в кільці $\mathbb{Z}[i]$ є елемент $1 + 2i$.

32.17. в кільці $\mathbb{Z}[\sqrt{3}i]$ є елемент $4 - 3\sqrt{3}i$.

32.18. є число 11, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.19. в кільці $\mathbb{Z}[i]$ є елемент $4 - 3i$.

32.20. в кільці $\mathbb{Z}[\sqrt{7}i]$ є елемент $5 - 2\sqrt{7}i$.

32.21. є число 17, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.22. в кільці $\mathbb{Z}[i]$ є елемент $1-3i$.

32.23. в кільці $\mathbb{Z}[\sqrt{5}i]$ є елемент $3+\sqrt{5}i$.

32.24. є число 2, якщо його розглядати як: а) елемент кільця $\mathbb{Z}$ цілих чисел; б) елемент кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

32.25. в кільці $\mathbb{Z}[i]$ є елемент $5+4i$.

Приклад 33. Знайти найбільший спільний дільник і найменше спільне кратне цілих гаусових чисел $z_1 = 7+24i$ та $z_2 = 22+19i$.

Розв'язання. Кільце $\mathbb{Z}[i]$ цілих гаусових чисел є евклідовим, причому однією із можливих норм цілого гаусового числа $z = a+bi$, $a, b \in \mathbb{Z}$, є число $\mathrm{Nr}(z) = a^2+b^2$. Оскільки $z_1 \neq 0$ і $z_2 \neq 0$, то для знаходження найбільших спільних дільників чисел z_1 і z_2 можемо використати алгоритм Евкліда. Маємо:

$$\mathrm{Nr}(z_1) = \mathrm{Nr}(7+24i) = 7^2+24^2 = 625,$$
$$\mathrm{Nr}(z_2) = \mathrm{Nr}(22+19i) = 22^2+19^2 = 845.$$

Оскільки $\mathrm{Nr}(z_2) > \mathrm{Nr}(z_1)$, то ділимо з остачею z_2 на z_1. При цьому використовуємо правило ділення комплексних чисел, записаних в алгебраїчній формі:

$$\frac{z_2}{z_1} = \frac{22+19i}{7+24i} = \frac{(22+19i)(7-24i)}{(7+24i)(7-24i)} = \frac{610-395i}{625} = \frac{610}{625} - \frac{395}{625}i.$$

Виділимо цілу частину дійсної та уявної частин комплексного числа $\frac{610}{625} - \frac{395}{625}i$ таким чином, щоб в дробовій частині модулі дійсної та уявної частин не перевищували $\frac{1}{2}$ (див. приклад 3 п.10 §3 Розд. 4 [1]):

$$\frac{z_2}{z_1} = \frac{610}{625} - \frac{395}{625}i = \left(1-\frac{15}{625}\right) - \left(1-\frac{230}{625}\right)i = (1-i) + \left(-\frac{15}{625}+\frac{230}{625}i\right),$$
$$\text{де } \left|-\frac{15}{625}\right| < \frac{1}{2}, \left|\frac{230}{625}\right| < \frac{1}{2}.$$

Тоді

$$z_2 = z_1(1-i) + z_1\left(-\frac{15}{625}+\frac{230}{625}i\right) = z_1(1-i) + \frac{(7+24i)(-15+230i)}{625} =$$
$$= z_1(1-i) + (-9+2i).$$

Оскільки $\mathrm{Nr}(-9+2i) = 9^2+2^2 = 85 < 625 = \mathrm{Nr}(z_1)$, то $q_0 = 1-i$, $r_1 = -9+2i$ – перша остача.

Ділимо далі z_1 на r_1:

$$\frac{z_1}{r_1} = \frac{7+24i}{-9+2i} = \frac{(7+24i)(-9-2i)}{(-9+2i)(-9-2i)} = \frac{-15-230i}{85} = -\frac{15}{85} - \frac{230i}{85} =$$
$$= -\frac{15}{85} - \left(3 - \frac{25}{85}\right)i = -3i + \left(-\frac{15}{85} + \frac{25}{85}i\right), \text{ де } \left|-\frac{13}{65}\right| < \frac{1}{2}, \left|-\frac{26}{377}\right| < \frac{1}{2}.$$

Тоді

$$z_1 = r_1(-3i) + r_1\left(-\frac{15}{85} + \frac{25}{85}i\right) = r_1(-3i) + \frac{(-9+2i)(-15+25i)}{85} =$$
$$= r_1(-3i) + (1-3i).$$

Оскільки $\mathrm{Nr}(1-3i) = 1^2+3^2 = 10 < 85 = \mathrm{Nr}(r_1)$, то $q_1 = -3i$, $r_2 = 1-3i$ – друга остача.

Ділимо далі r_1 на r_2:

$$\frac{r_1}{r_2} = \frac{-9+2i}{1-3i} = \frac{(-9+2i)(1+3i)}{(1-3i)(1+3i)} = \frac{-15-25i}{10} =$$
$$= -\frac{3}{2} - \frac{5}{2}i = (-1-2i) + \left(-\frac{1}{2} - \frac{1}{2}i\right).$$

Тоді

$$r_1 = r_2(-1-2i) + r_2\left(-\frac{1}{2} - \frac{1}{2}i\right) = r_2(-1-2i) + \frac{(1-3i)(-1-i)}{2} =$$
$$= r_2(-1-2i) + (-2+i).$$

Оскільки $\mathrm{Nr}(-2+i) = 2^2+1^2 = 5 < 10 = \mathrm{Nr}(r_2)$, то $q_2 = -1-2i$, $r_3 = -2+i$ – третя остача.

Ділимо тепер r_2 на r_3:

$$\frac{r_2}{r_3} = \frac{1-3i}{-2+i} = \frac{(1-3i)(-2-i)}{(-2+i)(-2-i)} = \frac{-5+5i}{5} = -1+i \in \mathbb{Z}[i].$$

Отже, $r_2 \vdots r_3$, тоді $r_4 = 0$, остання відмінна від 0 остача алгоритму Евкліда: $r_3 = -2+i$. Отже, $(z_1, z_2) \sim -2+i$. Оскільки дільниками одиниці в кільці $\mathbb{Z}[i]$ є елементи: $1, -1, i, -i$, то найбільшими спільними дільниками цілих гаусових чисел $z_1 = 7+24i$ і $z_2 = 22+19i$ є числа: $d_1 = -2+i$, $d_2 = (-2+i)(-1) = 2-i$, $d_3 = (-2+i)i = -1-2i$, $d_4 = (-2+i)(-i) = 1+2i$.

Найменші спільні кратні чисел z_1 і z_2 знайдемо, використовуючи формулу (III.18). Маємо:

$$[z_1, z_2] \sim \frac{z_1 z_2}{(z_1, z_2)} = \frac{(7+24i)(22+19i)}{-2+i} = \frac{-302+661i}{-2+i} = \\ = \frac{(-302+661i)(-2-i)}{(-2+i)(-2-i)} = \frac{1265-1020i}{5} = 253-204i.$$

Таким чином,

$$[z_1, z_2] \sim 253-204i,$$

тобто найменшими спільними кратними чисел z_1 і z_2 є: $m_1 = 253-204i$, $m_2 = -253+204i$, $m_3 = 204+253i$, $m_4 = -204-253i$.

Розв'язання в Maple. Один із найбільших спільних дільників двох цілих гаусових чисел a і b (а саме: той НСД d, який лежить в I чверті, тобто $\operatorname{Re} d \geqslant 0$, $\operatorname{Im} d \geqslant 0$) знайдемо за допомогою команди **GIgcd(a,b)** із пакету **GaussInt**.

```
> with(GaussInt):
  GIgcd(7+24*I,22+19*I);
```

$$1+2\,I$$

Отже, $(z_1, z_2) \sim 1+2i$. Оскільки дільниками одиниці в кільці $\mathbb{Z}[i]$ є елементи: $1, -1, i, -i$, то найбільшими спільними дільниками цілих гаусових чисел $z_1 = 7+24i$ і $z_2 = 22+19i$ є числа:

```
> (1+2*I)*1;  (1+2*I)*(-1);  (1+2*I)*I;  (1+2*I)*(-I);
```

$$1+2\,I$$
$$-1-2\,I$$
$$-2+I$$
$$2-I$$

Для відшукання НСК двох цілих гаусових чисел a, b використовується команда **GIlcm(a,b)**.

```
> GIlcm(7+24*I,22+19*I);
```

$$204+253\,I$$

Таким чином, $[z_1, z_2] \sim 204+253i$, тобто найменшими спільними кратними чисел z_1 і z_2 є:

```
> (204+253*I)*1;  (204+253*I)*(-1); (204+253*I)*I;
(204+253*I)*(-I);
```

$$204+253\,I$$
$$-204-253\,I$$
$$-253+204\,I$$

$$253 - 204\,I$$

При розв'язанні даного завдання помилки зустрічаються досить часто: це пов'язано із подекуди досить громіздкими обчисленнями. Тому доцільно у випадку виявленої помилки зробити покрокову перевірку.

I. Визначаємо, яке з чисел має більшу норму, за допомогою команди **GInorm(z)**:

```
> with(GaussInt):
  GInorm(7+24*I);
  GInorm(22+19*I);
```

$$625$$
$$845$$

II. Число з більшою нормою позначаємо через z_2, число з меншою нормою – через z_1.

```
> z2:=22+19*I;
  z1:=7+24*I;
```

$$z2 := 22 + 19\,I$$
$$z1 := 7 + 24\,I$$

III. Перевіримо, чи правильно було знайдено послідовні неповні частки q_i і остачі r_i алгоритму Евкліда. Для їх відшукання використовуються команди **GIquo** і **GIrem** відповідно:

```
> q1:=GIquo(z2,z1);
  r1:=GIrem(z2,z1);
```

$$q1 := 1 - I$$
$$r1 := -9 + 2\,I$$

```
> q2:=GIquo(z1,r1);
  r2:=GIrem(z1,r1);
```

$$q1 := -3\,I$$
$$r2 := 1 - 3\,I$$

```
> q3:=GIquo(r1,r2);
  r3:=GIrem(r1,r2);
```

$$q3 := -1 - 2\,I$$
$$r3 := -2 + I$$

```
> q4:=GIquo(r2,r3);
  r4:=GIrem(r2,r3);
```

$$q4 := -1 + I$$
$$r4 := 0$$

Остання відмінна від 0 остача алгоритму Евкліда $r_3 = -2 + i$. Отже, $(z_1, z_2) \sim -2 + i$.

Завдання 33. Знайти найбільший спільний дільник і найменше спільне кратне цілих гаусових чисел z_1 і z_2, якщо:

33.1. $z_1 = 180 + 104i$;
$z_2 = -34 + 56i$.

33.2. $z_1 = -7 - 19i$;
$z_2 = 7 + 9i$.

33.3. $z_1 = 15 + 4i$;
$z_2 = -12 - 7i$.

33.4. $z_1 = 53 - 54i$;
$z_2 = 10 + 45i$.

33.5. $z_1 = 29 - 24i$;
$z_2 = 2 + 23i$.

33.6. $z_1 = 13 + 13i$;
$z_2 = 34 - 12i$.

33.7. $z_1 = -36 + 3i$;
$z_2 = 24 + 27i$.

33.8. $z_1 = 12 + i$;
$z_2 = -61 + 36i$.

33.9. $z_1 = 11 + 23i$;
$z_2 = 17 - 19i$.

33.10. $z_1 = 9 - 19i$;
$z_2 = -13 - 13i$.

33.11. $z_1 = 18 - i$;
$z_2 = 10 - 15i$.

33.12. $z_1 = 153 + 155i$;
$z_2 = -16 + 22i$.

33.13. $z_1 = -7 - 24i$;
$z_2 = -46 + 3i$.

33.14. $z_1 = 58 + 4i$;
$z_2 = 23 - 15i$.

33.15. $z_1 = -10 + 3i$;
$z_2 = 16 + 5i$.

33.16. $z_1 = 33 - 4i$;
$z_2 = 5 + 12i$.

33.17. $z_1 = 13 + 18i$;
$z_2 = 31 - 24i$.

33.18. $z_1 = 31 + 33i$;
$z_2 = -19 + 18i$.

33.19. $z_1 = -17 + i$;
$z_2 = 18 + 16i$.

33.20. $z_1 = 14 + 52i$;
$z_2 = 17 + 31i$.

33.21. $z_1 = -43 - i$;
$z_2 = 185 + 37i$.

33.22. $z_1 = -104 + 93i$;
$z_2 = 221 + 60i$.

33.23. $z_1 = 19 + 17i$;
$z_2 = 47 - 25i$.

33.24. $z_1 = 7 + 4i$;
$z_2 = 9 - 4i$.

33.25. $z_1 = 22 - 7i$;
$z_2 = -2 - 23i$.

Розділ IV

Многочлени від однієї змінної

1. Відношення подільності в кільці многочленів. Ділення з остачею

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай K – комутативне кільце з одиницею без дільників нуля (область цілісності), $K[x]$ – кільце многочленів від змінної x над кільцем K. Многочлен $f(x) \in K[x]$ ділиться на $g(x) \in K[x]$ (пишуть $f(x) \vdots g(x)$), якщо існує многочлен $s(x) \in K[x]$ такий, що $f(x) = g(x) \cdot s(x)$. При цьому також кажуть, що $g(x)$ є дільником $f(x)$ (пишуть $g(x) | f(x)$). Якщо такого многочлена $s(x) \in K[x]$ не існує, то $f(x)$ не ділиться на $g(x)$ в $K[x]$ (пишуть $f(x) \,\overline{\vdots}\, g(x)$) або $g(x)$ не є дільником $f(x)$ (пишуть $g(x) \nmid f(x)$).

Відношення подільності многочленів над областю цілісності K має наступні **властивості**.

Нехай $f(x), \varphi(x), g(x)$ – довільні многочлени із $K[x]$. Тоді:

1°. якщо $f(x) \vdots \varphi(x)$, $\varphi(x) \vdots g(x)$, то $f(x) \vdots g(x)$;

2°. якщо $f(x) \vdots g(x)$, $\varphi(x) \vdots g(x)$, то $(f(x) \pm \varphi(x) \vdots g(x)$;

3°. якщо $f(x) \vdots g(x)$, то $f(x) \cdot \varphi(x) \vdots g(x)$;

4°. $\varphi(x) \vdots c$, де $0 \neq c \in K$;

5°. якщо $f(x) \vdots g(x)$, то $f(x) \vdots cg(x)$, де $0 \neq c \in K$;

6°. якщо $f(x) \vdots g(x)$ і $g(x) \vdots f(x)$ то $f(x) = c \cdot g(x)$, де $c \in K$.

Нехай P – поле. Говорять, що многочлен $f(x) \in P[x]$ ділиться з остачею на многочлен $g(x) \neq 0$ з кільця $P[x]$, якщо в $P[x]$ існують многочлени $s(x)$ і $r(x)$ такі, що:

1) $f(x) = g(x) \cdot s(x) + r(x)$;
2) $r(x) = 0$ або $\deg r < \deg g$.

При цьому $f(x)$ називають діленим, $g(x)$ – дільником, $s(x)$ – неповною часткою, $r(x)$ – остачею.

Розділити многочлен $f(x)$ на многочлен $g(x)$ з остачею означає записати його у вигляді $f(x) = g(x) \cdot s(x) + r(x)$, де $s(x)$ – неповна частка, $r(x)$ – остача.

Теорема (про ділення з остачею)**.** *Для будь-яких многочленів* $f(x)$ *і* $g(x) \neq 0$ *над полем* P *завжди існує, причому єдина, пара многочленів* $s(x)$ *і* $r(x)$ *із* $P[x]$ *така, що* $f(x) = g(x) \cdot s(x) + r(x)$*, де* $r(x) = 0$ *або* $\deg r < \deg g$*.*

Кільце $P[x]$ многочленів над полем P є евклідовим, а значить, і кільцем головних ідеалів.

Для знаходження частки і остачі від ділення многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ на многочлен $g(x) = b_m x^n + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ над полем P (а при певних умовах і над областю цілісності K) застосовують різні методи: метод ділення „кутом" (або „стовпчиком"), метод невизначених коефіцієнтів.

I. Метод ділення многочлена на многочлен „кутом" (або „стовпчиком"). В загальному випадку при діленні многочлена $f(x)$ на многочлен $g(x)$ $(m \leqslant n)$ „кутом" многочлени $f(x)$ і $g(x)$ записують в стандартному вигляді. Потім старший член $a_n x^n$ многочлена $f(x)$ ділять на старший член $b_m x^m$ многочлена $g(x)$ і отримують старший член $\frac{a_n}{b_m}x^{n-m}$ частки $s(x)$. Потім дільник $g(x)$ множать на $\frac{a_n}{b_m}x^{n-m}$ і отриманий многочлен $\frac{a_n}{b_m}x^{n-m} \cdot g(x)$ віднімають від многочлена $f(x)$. В результаті віднімання отримується деякий многочлен $f_1(x)$, степінь якого меньший за n: $\deg f_1 = n_1 < n$.

Якщо $n_1 < m$, то процес ділення закінчено, при цьому $f_1(x) = r(x)$ – остача. Якщо $n_1 \geqslant m$, то описаний процес ділення повторюється для многочлена $f_1(x)$ і т.д. Процес продовжується доти, поки степінь отриманого на k-му кроці многочлена $f_k(x)$ не стане менший за степінь дільника $g(x)$, тобто менший за m, або $f_k = 0$. При цьому многочлен $f_k(x) = r(x)$ – остача.

II. Метод невизначених коефіцієнтів. В силу теореми про ділення з остачею, для многочленів $f(x)$ і $g(x)$ існує єдина пара многочленів $s(x)$ і $r(x)$ така, що $f(x) = g(x) \cdot s(x) + r(x)$, і, крім того, стандартний вигляд кожного із многочленів – єдина. Тому для знаходження $s(x)$ і $r(x)$ можна використати метод невизначених коефіцієнтів.

При цьому неповну частку шукають у вигляді

$$s(x) = \frac{a_n}{b_m}x^{n-m} + c_{n-2}x^{n-2} + \ldots + c_1 x + c_0, \tag{IV.1}$$

а остачу

$$r(x) = d_{m-1}x^{m-1} + d_{m-2}x^{m-2} + \ldots + d_1 x + d_0, \tag{IV.2}$$

де коефіцієнти $c_{n-2}, \ldots, c_1, c_0$ і $d_{m-1}, d_{m-2}, \ldots, d_1, d_0$ – невизначені, зокрема, деякі або всі із коефіцієнтів $d_{m-1}, d_{m-2}, \ldots, d_1, d_0$ можуть бути рівні нулю.

Записують тотожну рівність

$$a_n x^n + \ldots + a_1 x + a_0 = (b_m x^n + \ldots + b_1 x + b_0)\left(\frac{a_n}{b_m}x^{n-m} + \ldots + c_1 x + c_0\right) + \\ + d_{m-1}x^{m-1} + \ldots + d_1 x + d_0. \tag{IV.3}$$

Перемножуючи многочлени $g(x)$ і $s(x)$ і зводячи подібні члени в правій частині рівності (IV.3), записують многочлен n-го степеня в стандартному вигляді. Прирівнюючи коефіцієнти при однакових степенях змінної x цього многочлена і многочлена $f(x)$, отримують систему n рівнянь, розв'язуючи яку, знаходять коефіцієнти $c_{n-2}, \ldots, c_1, c_0, d_{m-1}, \ldots, d_1, d_0$.

Рівняння для знаходження даних коефіцієнтів можна також одержати, надаючи певних значень змінній x.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 34.1. Виконати ділення з остачею многочлена

$$f(x) = 3x^6 - 2x^3 + 7x^2 - 4$$

на многочлен

$$g(x) = 2x^3 - x + 7$$

в кільці $\mathbb{Q}[x]$: а) методом ділення „кутом”;
б) методом невизначених коефіцієнтів.

Розв'язання. а) Виконаємо ділення „кутом”.

$$\begin{array}{rl|l}
f(x) = & 3x^6 - 2x^3 + 7x^2 - 4 & 2x^3 - x + 7 = g(x) \\
\cline{3-3}
& \underline{3x^6 - \frac{3}{2}x^4 + \frac{21}{2}x^3} & \frac{3}{2}x^3 + \frac{3}{4}x - \frac{25}{4} = s(x) \\
& \frac{3}{2}x^4 - \frac{25}{2}x^3 + 7x^2 - 4 & \\
& \underline{\frac{3}{2}x^4 - \frac{3}{4}x^2 + \frac{21}{4}x} & \\
& -\frac{25}{2}x^3 + \frac{31}{4}x^2 - \frac{21}{4}x - 4 & \\
& \underline{-\frac{25}{2}x^3 + \frac{25}{4}x - \frac{175}{4}} & \\
& \frac{31}{4}x^2 - \frac{23}{2}x + \frac{159}{4} = r(x) &
\end{array}$$

Таким чином, $f(x) = g(x)\left(\frac{3}{2}x^3 + \frac{3}{4}x - \frac{25}{4}\right) + \frac{31}{4}x^2 - \frac{23}{2}x + \frac{159}{4}$.

б) Використаємо метод невизначених коефіцієнтів. Оскільки $\mathbb{Q}$ – поле, $\deg f = 6$, $\deg g = 3$, то $\deg s = \deg f - \deg g = 3$, $\deg r \leqslant 2$ або $r(x) = 0$.

Нехай $s(x) = \frac{3}{2}x^3 + c_2x^2 + c_1x + c_0$, $r(x) = d_2x^2 + d_1x + d_0$. Отримуємо тотожність

$$3x^6 - 2x^3 + 7x^2 - 4 = \\ = \left(2x^3 - x + 7\right)\left(\frac{3}{2}x^3 + c_2x^2 + c_1x + c_0\right) + d_2x^2 + d_1x + d_0.$$

Розкриваючи дужки і зводячи подібні доданки в правій частині останньої рівності, отримуємо:

$$3x^6 - 2x^3 + 7x^2 - 4 = 3x^6 + 2c_2x^5 + \left(2c_1 - \frac{3}{2}\right)x^4 + \left(2c_0 - c_2 + \frac{21}{2}\right)x^3 + \\ + \left(7c_2 - c_1 + d_2\right)x^2 + \left(7c_1 - c_0 + d_1\right)x + 7c_0 + d_0.$$

Прирівнюємо коефіцієнти при однакових степенях змінної x:

$$\begin{array}{c|rl} x^5 & 0 = & 2c_2, \\ x^4 & 0 = & 2c_1 - \frac{3}{2}, \\ x^3 & -2 = & 2c_0 - c_2 + \frac{21}{2}, \\ x^2 & 7 = & 7c_2 - c_1 + d_2, \\ x & 0 = & 7c_1 - c_0 + d_1, \\ x^0 & -4 = & 7c_0 + d_0. \end{array}$$

Розв'язавши дану систему рівнянь, маємо: $c_2 = 0$, $c_1 = \frac{3}{4}$, $c_0 = -\frac{25}{4}$, $d_2 = \frac{31}{4}$, $d_1 = -\frac{23}{2}$, $d_0 = \frac{159}{4}$. Таким чином, $s(x) = \frac{3}{2}x^3 + \frac{3}{4}x - \frac{25}{4}$, $r(x) = \frac{31}{4}x^2 - \frac{23}{2}x + \frac{159}{4}$, тобто

$$f(x) = g(x)\left(\tfrac{3}{2}x^3 + \tfrac{3}{4}x - \tfrac{25}{4}\right) + \tfrac{31}{4}x^2 - \tfrac{23}{2}x + \tfrac{159}{4}.$$

Розробка процедур. Створимо процедури, які дадуть змогу покроково перевірити розв'язання методом невизначених коефіцієнтів. Одна із таких процедур – **generatePoly(n,c)**, яка генеруватиме многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ з невизначеними коефіцієнтами.

На початку циклу покладемо $f = 0$. В ході виконання циклу змінна f поступово набуває значень a_0, $a_0 + a_1 x$, $a_0 + a_1 x + a_2 x^2$,..., $a_0 + a_1 x + a_2 x^2 + .. + a_n x^n$:

```
generatePoly:=proc(n,c)
local f,i;
   f:=0;
   for i from 0 to n do f:=f+c[i]*x^i;
      end do;
end proc:
```

Наприклад, щоб задати многочлен $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, достатньо буде викликати:

```
> f:=generatePoly(3,a);
```

$$f := a_0 + a_1\,x + a_2\,x^2 + a_3\,x^3$$

Тепер створимо процедуру **mUndefCoeff(lp,rp)**, за допомогою якої можна буде знайти невизначені коефіцієнти в рівності $lp = rp$.

В даній процедурі використовуються наступні команди:

degree(f,x) – степінь многочлена $f(x)$;

coeff(f,x,k) – коефіцієнт a_k многочлена f при x^k.

В ході процедури: розкриваємо дужки і зводимо подібні доданки в заданих лівій **lp** і правій **rp** частинах рівності

```
> elp:=expand(lp);
  erp:=expand(rp);
```

далі прирівнюємо коефіцієнти при відповідних степенях змінної x, отримуємо рівняння **eq[i]**;

```
> eq[i]:=coeff(elp,x,i)=coeff(erp,x,i)
```

розв'язуємо отриману систему рівнянь:

```
> solve({seq(eq[i],i=0..n)});
```

Код процедури наступний:

```
mUndefCoeff:=proc(lp,rp)
local i,n,elp,erp,eq;
   n:=max(degree(lp),degree(rp));
   elp:=expand(lp);
   erp:=expand(rp);
   for i from 0 to n do eq[i]:=coeff(elp,x,i)=coeff(erp,x,i) end do;
   solve({seq(eq[i],i=0..n)});
end proc:
```

Розв'язання в Maple. а) Для знаходження неповної частки і остачі від ділення многочлена $f(x)$ на многочлен $g(x)$ над числовим полем (полями $\mathbb{Q}$, $\mathbb{R}, \mathbb{C}$) застосовують команди **quo(f, g, x)** і **rem(f, g, x)** відповідно.

```
> quo(3*x^6-2*x^3+7*x^2-4,2*x^3-x+7,x);
```

$$\frac{3}{2}x^3 + \frac{3}{4}x - \frac{25}{4}$$

```
> rem(3*x^6-2*x^3+7*x^2-4,2*x^3-x+7,x);
```

$$\frac{159}{4} + \frac{31}{4}x^2 - \frac{23}{2}x$$

Отже, неповна частка від ділення многочлена $f(x)$ на многочлен $g(x)$ дорівнює $s(x) = \frac{3}{2}x^3 + \frac{3}{4}x - \frac{25}{4}$, а остача – $r(x) = \frac{31}{4}x^2 - \frac{23}{2}x + \frac{159}{4}$.

б) Задаємо многочлени $f(x)$ і $g(x)$. Знаходимо їхні степені:

```
> f:=3*x^6-2*x^3+7*x^2-4:
  g:=2*x^3-x+7:
  n:=degree(f,x);
  m:=degree(g,x);
```

$$n := 6$$

$$m := 3$$

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

і генеруємо многочлени $s(x)$ і $r(x)$:

```
> s:=generatePoly(n-m,c);
```

$$s := c_0 + c_1\,x + c_2\,x^2 + c_3\,x^3$$

```
> r:=generatePoly(m-1,d);
```

$$r := d_0 + d_1\,x + d_2\,x^2$$

Метод невизначених коефіцієнтів будемо застосовувати до рівності $f(x) = g(x) \cdot s(x) + r(x)$. Окремо ліву, окремо праву частини даної рівності заносимо аргументами процедури **mUndefCoeff**:

```
> mUndefCoeff(f,g*s+r);
```

$$\{c_0 = \frac{-25}{4},\ c_1 = \frac{3}{4},\ c_2 = 0,\ c_3 = \frac{3}{2},\ d_0 = \frac{159}{4},\ d_1 = \frac{-23}{2},\ d_2 = \frac{31}{4}\}$$

Отже, $s(x) = -\frac{25}{4} + \frac{3}{4}x + \frac{3}{2}x^3$, $r(x) = \frac{159}{4} - \frac{-23}{2}x + \frac{31}{4}$.

Приклад 34.2. Виконати ділення з остачею многочлена

$$f(x) = (2i+3)x^4 - (2+i)x^2 + 5x - 4 + i$$

на многочлен $g(x) = (1+3i)x^2 + i$ в кільці $\mathbb{C}[x]$.

Розв'язання. а) Виконуємо ділення „кутом".

$$\begin{array}{l|l}
f(x) = (2i+3)x^4 - (2+i)x^2 + 5x - 4 + i & (1+3i)x^2 + i \quad = g(x) \\
\hline
\underline{(2i+3)x^4 + \left(\frac{7}{10} + \frac{9}{10}i\right)x^2} & \left(\frac{9}{10} - \frac{7}{10}i\right)x^2 + \left(-\frac{21}{25} + \frac{31}{50}i\right) = s(x) \\
\left(-\frac{27}{10} - \frac{19}{10}i\right)x^2 + 5x - 4 + i & \\
\underline{\left(-\frac{27}{10} - \frac{19}{10}i\right)x^2 + \left(-\frac{31}{50} - \frac{21}{25}i\right)} & \\
5x + \left(-\frac{169}{50} + \frac{46}{25}i\right) &
\end{array}$$

Таким чином, $f(x) = g(x)\left(\left(\frac{9}{10} - \frac{7}{10}i\right)x^2 + \left(-\frac{21}{25} + \frac{31}{50}i\right)\right) + 5x + \left(-\frac{169}{50} + \frac{46}{25}i\right)$.

б) Використаємо метод невизначених коефіцієнтів. Оскільки $\mathbb{C}$ – поле, $\deg f = 4$, $\deg g = 2$, то $\deg s = \deg f - \deg g = 2$, $\deg r \leqslant 1$ або $r(x) = 0$.

Нехай $s(x) = \left(\frac{9}{10} - \frac{7}{10}i\right)x^2 + c_1x + c_0$, $r(x) = d_1x + d_0$. Отримуємо рівність

$$(2i+3)x^4 - (2+i)x^2 + 5x - 4 + i = \\ = \left((1+3i)x^2 + i\right)\left(\frac{9}{10} - \frac{7}{10}i\right)x^2 + c_1x + c_0 + d_1x + d_0.$$

Розкривши дужки і звівши подібні доданки в правій частині останньої рівності, отримуємо:

$$(2i+3)x^4 - (2+i)x^2 + 5x - 4 + i = (c_2 + 3ic_2)x^4 + (c_1 + 3ic_1)x^3 + \\ + (c_0 + 3ic_0 + c_2i)x^2 + (c_1i + d_1)x + (c_0i + d_0).$$

Прирівнюємо коефіцієнти при однакових степенях змінної x:

$$\begin{array}{c|rl} x^4 & 2i+3 = & c_2+3ic_2, \\ x^3 & 0 = & c_1+3ic_1, \\ x^2 & -(2+i) = & c_0+3ic_0+c_2i, \\ x & 5 = & c_1i+d_1, \\ x^0 & -4+i = & c_0i+d_0. \end{array}$$

Розв'язавши дану систему рівнянь, маємо: $c_2 = \frac{9}{10} - \frac{7}{10}i$, $c_1 = 0$, $c_0 = -\frac{21}{25} + \frac{31}{50}i$, $d_1 = 5$, $d_0 = -\frac{169}{50} + \frac{46}{25}i$. Таким чином, $s(x) = \left(\frac{9}{10} - \frac{7}{10}i\right)x^2 + \left(-\frac{21}{25} + \frac{31}{50}i\right)$, $r(x) = 5x + \left(-\frac{169}{50} + \frac{46}{25}i\right)$.

Розв'язання в Maple. Задаємо многочлени $f(x)$ і $g(x)$:

```
> f:=(2*I+3)*x^4-(2+I)*x^2+5*x-4+I:
  g:=(1+3*I)*x^2+I:
```

і знаходимо неповну частку і остачу:

```
> quo(f,g,x);
```

$$-\frac{21}{25} + \frac{31}{50}\,I + \left(\frac{9}{10} - \frac{7}{10}\,I\right)x^2$$

```
> rem(f,g,x);
```

$$-\frac{169}{50} + \frac{46}{25}\,I + 5\,x$$

Перевірку розв'язання пункту б) здійснюємо також за алгоритмом із Прикладу 34.1.

```
> f:=(2*I+3)*x^4-(2+I)*x^2+5*x-4+I:
  g:=(1+3*I)*x^2+I:
  n:=degree(f,x):
  m:=degree(g,x):
> s:=generatePoly(n-m,c);
```

$$s := c_0 + c_1\,x + c_2\,x^2$$

```
> r:=generatePoly(m-1,d);
```

$$r := d_0 + d_1\,x$$

```
> mUndefCoeff(f,g*s+r);
```

$$\left\{c_0 = \frac{-21}{25} + \frac{31}{50}\,I,\ c_1 = 0,\ c_2 = \frac{9}{10} - \frac{7}{10}\,I,\ d_0 = \frac{-169}{50} + \frac{46}{25}\,I,\ d_1 = 5\right\}$$

Приклад 34.3. Виконати ділення з остачею многочлена

$$f(x) = \overline{7}x^5 + \overline{5}x^2 - \overline{3}x + \overline{4}$$

на многочлен

$$g(x) = \overline{3}x^2 - \overline{2}x + \overline{1}$$

в кільці $\mathbb{Z}_{11}[x]$: а) методом ділення „кутом”;
б) методом невизначених коефіцієнтів.

Розв'язання. а) Використаємо метод ділення „кутом”. Зауважимо, що коефіцієнти неповної частки $s(x)$ можна шукати двома способами. Наприклад, щоб знайти старший коефіцієнт многочлена $s(x)$ можна:

I: підібрати коефіцієнт, який би в добутку із старшим коефіцієнтом $b_2 = \overline{3}$ многочлена $g(x)$ давав би старший коефіцієнт $a_5 = \overline{7}$ многочлена $f(x)$. Таким елементом є $\overline{6}$, оскільки $\overline{6} \cdot \overline{3} = \overline{7}$;

II: знайти елемент b_2^{-1}, обернений до старшого коефіцієнта $b_2 = \overline{3}$ многочлена $g(x)$ в $\mathbb{Z}_{11}$: $b_2^{-1} = \overline{3}^{-1} = \overline{4}$, тоді старший коефіцієнт многочлена $s(x)$ дорівнює добутку $a_5 b_2^{-1} = \overline{7} \cdot \overline{4} = \overline{6}$.

Решта коефіцієнтів многочлена $s(x)$ шукаються аналогічно:
$c_2 = \overline{1} \cdot b_2^{-1} = \overline{4}$; $c_1 = \overline{2} \cdot b_2^{-1} = \overline{2} \cdot \overline{4} = \overline{8}$; $c_0 = \overline{6} \cdot b_2^{-1} = \overline{6} \cdot \overline{4} = \overline{2}$.

$$
\begin{array}{rl|l}
f(x) = \overline{7}x^5 + 5x^2 - \overline{3}x + \overline{4} & & \overline{3}x^2 - \overline{2}x + \overline{1} = g(x) \\
\cline{3-3}
\overline{7}x^5 - x^4 + \overline{6}x^3 & & \overline{6}x^3 + \overline{4}x^2 + \overline{8}x + \overline{2} = s(x) \\
\cline{1-1}
x^4 - \overline{6}x^3 + \overline{5}x^2 - \overline{3}x + \overline{4} & & \\
x^4 - \overline{8}x^3 + \overline{4}x^2 & & \\
\cline{1-1}
\overline{2}x^3 + x^2 - \overline{3}x + \overline{4} & & \\
\overline{2}x^3 - \overline{5}x^2 + \overline{8}x & & \\
\cline{1-1}
\overline{6}x^2 + \overline{4} & & \\
\overline{6}x^2 - \overline{4}x + \overline{2} & & \\
\cline{1-1}
\overline{4}x + \overline{2} = r(x) & &
\end{array}
$$

Оскільки $\deg r < \deg g$, то $r(x)$ – остача.

Таким чином, при діленні многочлена $f(x)$ на многочлен $g(x)$ одержали неповну частку $s(x) = \overline{6}x^3 + \overline{4}x^2 + \overline{8}x + \overline{2}$ і остачу $r(x) = \overline{4}x + \overline{2}$. Отже, $f(x) = g(x) \cdot (\overline{6}x^3 + \overline{4}x^2 + \overline{8}x + \overline{2}) + \overline{4}x + \overline{2}$.

б) Використаємо метод невизначених коефіцієнтів. Оскільки $\mathbb{Z}_{11}$ – поле, $\deg f = 5$, $\deg g = 2$, то $\deg s = 3$, $\deg r \leqslant 1$ або $r(x) = 0$. Нехай $s(x) = c_3x^3 + c_2x^2 + c_1x + c_0$, $r(x) = d_1x + d_0$. Отримуємо тотожність

$$\overline{7}x^5 + \overline{5}x^2 - \overline{3}x + \overline{4} = \left(\overline{3}x^2 - \overline{2}x + \overline{1}\right)\left(c_3x^3 + c_2x^2 + c_1x + c_0\right) + d_1x + d_0.$$

Розкривши дужки і звівши подібні доданки в правій частині останньої рівності, отримуємо:

$$\overline{7}x^5+\overline{5}x^2-\overline{3}x+\overline{4}=\overline{3}c_3x^5+\left(\overline{3}c_2-\overline{2}c_3\right)x^4+\left(\overline{3}c_1-\overline{2}c_2+c_3\right)x^3+$$
$$+\left(\overline{3}c_0-\overline{2}c_1+c_2\right)x^2+\left(c_1-\overline{2}c_0+d_1\right)x+c_0+d_0.$$

Прирівнюємо коефіцієнти при однакових степенях змінної x:

$$\begin{array}{c|rl} x^5 & \overline{7}= & \overline{3}c_3,\\ x^4 & \overline{0}= & \overline{3}c_2-\overline{2}c_3,\\ x^3 & \overline{0}= & \overline{3}c_1-\overline{2}c_2+c_3,\\ x^2 & \overline{5}= & \overline{3}c_0-\overline{2}c_1+c_2,\\ x & -\overline{3}= & c_1-\overline{2}c_0+d_1,\\ x^0 & \overline{4}= & c_0+d_0. \end{array}$$

Розв'язавши отриману систему рівнянь, маємо: $c_3=\overline{6}$, $c_2=\overline{4}$, $c_1=\overline{8}$, $c_0=\overline{2}$, $d_1=\overline{4}$, $d_0=\overline{2}$. Таким чином, $s(x)=\overline{6}x^3+\overline{4}x^2+\overline{8}x+\overline{2}$, $r(x)=\overline{4}x+\overline{2}$, тобто

$$f(x)=g(x)\left(\overline{6}x^3+\overline{4}x^2+\overline{8}x+\overline{2}\right)+\overline{4}x+\overline{2}.$$

Розв'язання в Maple. Для знаходження неповної частки і остачі від ділення многочлена $f(x)$ на многочлен $g(x)$ над скінченним полем $\mathbb{Z}_p$, p – просте, застосовують команди **Quo(f, g, x)** і **Rem(f, g, x)** відповідно, додаючи оператор **mod p**.

```
> Quo(7*x^5+5*x^2-3*x+4,3*x^2-2*x+1,x) mod 11;
```
$$6\,x^3+4\,x^2+8\,x+2$$
```
> Rem(7*x^5+5*x^2-3*x+4,3*x^2-2*x+1,x) mod 11;
```
$$4\,x+2$$

Завдання 34. Виконати ділення з остачею многочлена $f(x)$ на многочлен $g(x)$: а) методом ділення „кутом";
б) методом невизначених коефіцієнтів.

34.1. $f(x)=3x^7-7x^6-6x^5+10x^4-6x^3+6x^2+x$ на $g(x)=3x^2-x+1$ в кільці $\mathbb{Q}[x]$.

34.2. $f(x)=x^5+2x^4+ix^3+(1+i)x^2+2x$ на $g(x)=x^2+i$ в кільці $\mathbb{C}[x]$.

34.3. $f(x) = \overline{4}x^6 + \overline{3}x^5 - x^4 - \overline{2}x^3 - \overline{2}x^2 + x - \overline{1}$ на
$g(x) = x^2 + \overline{1}$ в кільці $\mathbb{Z}_5[x]$.

34.4. $f(x) = 8x^6 - 22x^5 + 16x^4 - 13x^3 - 2x^2 - 3x - 3$ на
$g(x) = 2x^2 - 4x - 1$ в кільці $\mathbb{Z}[x]$.

34.5. $f(x) = x^7 + \overline{2}x^6 + x^5 - \overline{4}x^3 + \overline{3}x^2 - \overline{4}x$ на
$g(x) = x^2 + \overline{4}x + \overline{2}$ в кільці $\mathbb{Z}_7[x]$.

34.6. $f(x) = x^4 + (2+i)x^3 - (1-i)x - 1$ на
$g(x) = x^3 - 1 + i$ в кільці $\mathbb{C}[x]$.

34.7. $f(x) = x^5 + \frac{8}{3}x^4 + x^3 + \frac{11}{2}x^2 + \frac{1}{3}x + 1$ на
$g(x) = x^2 - \frac{1}{3}x + 2$ в кільці $\mathbb{Q}[x]$.

34.8. $f(x) = x^5 + ix^4 + 2x^3 + 2$ на
$g(x) = x^3 + ix^2 + 1$ в кільці $\mathbb{C}[x]$.

34.9. $f(x) = x^7 - x^6 + x^4 - x^2 + \overline{2}$ на
$g(x) = \overline{4}x^2 - x + \overline{3}$ в кільці $\mathbb{Z}_5[x]$.

34.10. $f(x) = 4x^7 - 16x^6 - 12x^5 + 38x^4 + 8x^3 - 10x^2 + 2x - 3$ на
$g(x) = 2x^2 - 4$ в кільці $\mathbb{Q}[x]$.

34.11. $f(x) = \overline{2}x^6 + \overline{4}x^5 - x^4 - \overline{3}x^3 - x^2 + x + \overline{6}$ на
$g(x) = \overline{5}x^2 + x + \overline{6}$ в кільці $\mathbb{Z}_7[x]$.

34.12. $f(x) = x^4 - 2x^3 + (1+2i)x^2 + (3-4i)x + i$ на
$g(x) = x^2 + 2i$ в кільці $\mathbb{C}[x]$.

34.13. $f(x) = 4x^5 - 13x^3 + 14x^2 - 2x$ на
$g(x) = 2x^2 - 3x + 1$ в кільці $\mathbb{Z}[x]$.

34.14. $f(x) = x^7 - \overline{2}x^5 + \overline{3}x^4 - \overline{2}x^3 + x^2 - \overline{2}x$ на
$g(x) = \overline{4}x^2 + x + \overline{2}$ в кільці $\mathbb{Z}_5[x]$.

34.15. $f(x) = 2x^7 - 5x^6 + 5x^5 + 2x^4 - 6x^3 + 7x$ на
$g(x) = 2x^2 - 3x + 2$ в кільці $\mathbb{Z}[x]$.

34.16. $f(x) = x^5 - x^4 - x^2 + x - \overline{4}$ на
$g(x) = \overline{4}x^2 + \overline{1}$ в кільці $\mathbb{Z}_5[x]$.

34.17. $f(x) = \overline{2}x^7 + x^5 - \overline{3}x^4 + \overline{5}x^2 + x - 2$ на
$g(x) = \overline{6}x^2 - x + \overline{2}$ в кільці $\mathbb{Z}_7[x]$.

34.18. $f(x) = 12x^6 - 10x^5 - 15x^4 + 9x^3 - 11x^2 + 3x + 12$ на
$g(x) = 3x^2 - x - 5$ в кільці $\mathbb{Z}[x]$.

34.19. $f(x) = \overline{3}x^7 - x^6 + x^5 + x^4 - x^3 + \overline{4}x^2 + x - \overline{4}$ на
$g(x) = \overline{4}x^2 - \overline{2}x + \overline{1}$ в кільці $\mathbb{Z}_5[x]$.

34.20. $f(x) = x^4 - x^3 + 2ix^2 - ix + 2 - i$ на
$g(x) = x^2 + i$ в кільці $\mathbb{C}[x]$.

34.21. $f(x) = 4x^7 - 24x^6 - 21x^5 + 8x^4 - 7x^3 - 11x^2 + 7x + 2$ на
$g(x) = x^2 - 6x + 5$ в кільці $\mathbb{Z}[x]$.

34.22. $f(x) = x^4 + \overline{5}x^3 + \overline{2}$ на
$g(x) = \overline{6}x^2 - x - \overline{1}$ в кільці $\mathbb{Z}_7[x]$.

34.23. $f(x) = x^5 + 2ix^3 + 2 - i$ на
$g(x) = x^3 - i$ в кільці $\mathbb{C}[x]$.

34.24. $f(x) = x^5 + \frac{35}{6}x^4 + \frac{1}{2}x^3 + 8x^2 + \frac{1}{2}x - 1$ на
$g(x) = 2x^2 - \frac{1}{3}x + 3$ в кільці $\mathbb{Q}[x]$.

34.25. $f(x) = \overline{2}x^7 + \overline{2}x^6 - \overline{2}x^5 + \overline{2}x^4 + x^3$ на
$g(x) = \overline{2}x^2 - \overline{3}x + \overline{2}$ в кільці $\mathbb{Z}_7[x]$.

Приклад 35. Знайти остачу від ділення многочлена $f(x) = x^{2006} + x + 1$ на многочлен $g(x) = x^2 - (1+i)x + i$ в кільці $\mathbb{C}[x]$.

Розв'язання. За теоремою про ділення з остачею в кільці $\mathbb{C}[x]$ існують такі многочлени $s(x)$ і $r(x)$, що

$$x^{2006} + x + 1 = \big(x^2 - (1+i)x + i\big)\, s(x) + r(x), \qquad \text{(IV.4)}$$

причому або степінь многочлена $r(x)$ менше 2, або $r(x) = 0$. Це означає, що многочлен $r(x)$ можна записати у вигляді

$$r(x) = ax + b,$$

де a, b – невідомі коефіцієнти із $\mathbb{C}$. Підставляючи цей вираз у рівність (IV.4), отримуємо:

$$x^{2006} + x + 1 = \left(x^2 - (1+i)x + i\right) s(x) + ax + b. \qquad \text{(IV.5)}$$

Коренями многочлена $g(x)$ є числа $x = 1$ і $x = i$. Підставляючи ці значення в рівність (IV.5), маємо:

$$\begin{cases} 3 = a + b, \\ i = ai + b \end{cases} \quad \text{звідки} \quad \begin{cases} a = 2 + i, \\ b = 1 - i. \end{cases}$$

Отже, остача $r(x) = (2+i)x + 1 - i$.

Розв'язання в Maple. Для відшукання остачі використовуємо, як і в Прикладі 34.1, команду **rem** (в потрібному форматі в залежності від поля, над яким задано многочлени):

```
> f:=x^(2006)+x+1:
  g:=x^2-(1+I)*x+I:
> rem(f,g,x);
```

$$1 - I + (2 + I)\, x$$

Завдання 35. Знайти остачу від ділення:

35.1. $f(x) = x^{2008} - 9x^{2006} + x^{1004} - 9x^{1002} + 3x^2 - 2x + 4$ на $g(x) = x^2 - 4x + 3$ в кільці $\mathbb{R}[x]$.

35.2. $f(x) = x^{10} + x^8 + x^4 + x^2 + 1$ на $g(x) = x^2 + 1$ в кільці $\mathbb{C}[x]$.

35.3. $f(x) = (x-2)^{999} + (x-1)^{99} + 1$ на $g(x) = x^2 - 3x + 2$ в кільці $\mathbb{R}[x]$.

35.4. $f(x) = x^{40} + \overline{2}x^{37} - \overline{4}x^{18} + x^3 - \overline{2}$ на $g(x) = (x + \overline{3})(x + \overline{1})$ в кільці $\mathbb{Z}_5[x]$.

35.5. $f(x) = 2x^{99} - 3x^{24} + 4x^2 - 1$ на $g(x) = x^2 - 1$ в кільці $\mathbb{R}[x]$.

35.6. $f(x) = x^{10} - x^8 - 12x^6 + x^5 + 4x^3 + 3x - 1$ на $g(x) = x^2 - 4$ в кільці $\mathbb{Z}[x]$.

35.7. $f(x) = x^{2001} + x^{201} + x^{21} + x + 1$ на $g(x) = x^2 + 1$ в кільці $\mathbb{C}[x]$.

35.8. $f(x) = (x+2)^{777} + (x+1)^{77} + 1$ на
$g(x) = x^2 + 3x + 2$ в кільці $\mathbb{R}[x]$.

35.9. $f(x) = x^{15} + \overline{5}x^{14} + x^{13} - \overline{2}x^{12} + x + \overline{6}$ на
$g(x) = x^2 - x + \overline{5}$ в кільці $\mathbb{Z}_7[x]$.

35.10. $f(x) = x^{2007} - 9x^{2005} + x^{1003} - 9x^{1001} + x^2 - 3x + 4$ на
$g(x) = x^2 - 4x + 3$ в кільці $\mathbb{R}[x]$.

35.11. $f(x) = x^{2009} - 2x^{2008} + x^{91} - 4x^{89} + x^2 - x$ на
$g(x) = x^2 - x - 2$ в кільці $\mathbb{R}[x]$.

35.12. $f(x) = x^{81} + x^{27} + x^9 + x^3 + x + 1$ на
$g(x) = x^2 + 1$ в кільці $\mathbb{C}[x]$.

35.13. $f(x) = x^{2008} + x^{2007} + 1$ на
$g(x) = x^2 - 1$ в кільці $\mathbb{Z}[x]$.

35.14. $f(x) = x^{504} - 9x^{502} + x^2 - x - 1$ на
$g(x) = x^2 - 2x - 3$ в кільці $\mathbb{R}[x]$.

35.15. $f(x) = x^5 - 2x^3 + x^2 - 3x + 2$ на
$g(x) = x^2 - 4$ в кільці $\mathbb{Q}[x]$.

35.16. $f(x) = x^{100} - 16x^{98} + x^{50} - 4x^{49} + x^2 - 3x + 4$ на
$g(x) = x^2 - 5x + 4$ в кільці $\mathbb{R}[x]$.

35.17. $f(x) = x^{15} + \overline{2}x^{14} + x^{13} - \overline{4}x^{11} - \overline{2}x^2 - \overline{2}x + \overline{2}$ на
$g(x) = x^2 + x - \overline{2}$ в кільці $\mathbb{Z}_7[x]$.

35.18. $f(x) = x^{1999} - 2x^{1998} + x^{499} - 2x^{498} + x^{237} - 4x^{235} + x^{106} - 4x^{104} + x$ на
$g(x) = x^2 - x - 2$ в кільці $\mathbb{R}[x]$.

35.19. $f(x) = 2x^{64} - 5x^{36} - 3x^{27} + 7x^{15} + 2x^6 - 3x^4 + 8$ на
$g(x) = x^3 - x$ в кільці $\mathbb{R}[x]$.

35.20. $f(x) = x^{2007} + 5x^{2006} + x^{2005} + 5x^{2004} + x + 6$ на
$g(x) = x^2 + 6x + 5$ в кільці $\mathbb{R}[x]$.

35.21. $f(x) = x^{12} + x^{11} + x^{10} - \overline{4}x^9 + \overline{3}x^2 - \overline{2}x - \overline{2}$ на
$g(x) = x^2 - \overline{4}$ в кільці $\mathbb{Z}_5[x]$.

35.22. $f(x) = x^{2008} - 6x^{2007} + x^{2006} - 6x^{2005} + x - 3$ на
$g(x) = x^2 - 7x + 6$ в кільці $\mathbb{R}[x]$.

35.23. $f(x) = x^{19} - \overline{2}x^{18} + x^{11} + \overline{5}x^{10} + x^9 + \overline{3}x^7 + x^6 - \overline{4}x^4 + x$ на $g(x) = x^2 - x - \overline{2}$ в кільці $\mathbb{Z}_7[x]$.

35.24. $f(x) = -x^{2007} + 6x^{2006} - x^{1003} + 6x^{1002} + x - 6$ на $g(x) = x^2 - 5x - 6$ в кільці $\mathbb{R}[x]$.

35.25. $f(x) = x^{10} - x^8 + x^6 + x^5 + x^2 - \overline{3}x + \overline{4}$ на $g(x) = x^2 + \overline{4}$ в кільці $\mathbb{Z}_5[x]$.

2. Ділення многочлена на двочлен $x - a$. Розклад многочлена за степенями двочлена $x - a$

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x) \in P[x]$, P – поле.

Теорема (Безу)**.** *Для будь-якого $c \in P$ остача від ділення многочлена $f(x)$ на двочлен $x - c$ дорівнює $f(c)$. Зокрема, многочлен $f(x)$ ділиться на двочлен $x - c$ тоді і тільки тоді, коли $f(c) = 0$.*

Якщо $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, то коефіцієнти частки $q(x) = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$ і остачу r від ділення $f(x)$ на $x - c$ можна знайти за схемою Горнера:

	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
c	$\underbrace{a_n}$	$\underbrace{b_{n-1}c + a_{n-1}}$	$\underbrace{b_{n-2}c + a_{n-2}}$	$\ldots$	$\underbrace{b_1 c + a_1}$	$\underbrace{b_0 c + a_0}$
	b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	r

тобто $b_{n-1} = a_n$,

$$b_i = b_{i+1}c + a_{i+1} \qquad \text{для всіх } i = 0, 1, ..., n-2. \tag{IV.6}$$

$$r = b_0 c + a_0. \tag{IV.7}$$

Запис многочлена $f(x)$ у вигляді

$$f(x) = d_n(x-c)^n + d_{n-1}(x-c)^{n-1} + \ldots + d_1(x-c) + d_0,$$

де $d_n, d_{n-1}, \ldots, d_1, d_0 \in P$, називається розкладом многочлена $f(x)$ за степенями двочлена $x - c$. Коефіцієнти $d_n, d_{n-1}, \ldots, d_1, d_0$ розкладу можна знайти в результаті послідовного ділення $f(x)$ на $x - c$, потім здобутої першої частки на $x - c$ і т.д.

	a_n	a_{n-1}	$\ldots$	a_2	a_1	a_0
c	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\boxed{d_0}$
c	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\boxed{d_1}$	
c	$\ldots$	$\ldots$	$\ldots$	$\boxed{d_2}$		
$\ldots$	$\ldots$	$\ldots$	$\ldots$			
c	$\boxed{d_n}$					

ПРИКЛАДИ І ЗАДАЧІ

Приклад 36. Остачі від ділення многочлена $f(x)$ з кільця $\mathbb{Q}[x]$ на $g_1(x) = x - 2$ і $g_2(x) = x - 3$ дорівнюють відповідно $r_1 = 1$ і $r_2 = 2$. Знайти остачу від ділення многочлена $f(x)$ на многочлен $g(x) = (x - 2)(x - 3)$.
Розв'язання. За теоремою Безу

$$f(2) = r_1, \quad f(3) = r_2. \tag{IV.8}$$

При діленні многочлена $f(x)$ на многочлен $g(x) = x^2 - 5x + 6$ отримаємо деяку неповну частку $s(x)$ і остачу $r(x)$, причому $\deg r < \deg g$ або $r(x) = 0$, тобто $r(x) = ax + b$, де $a, b \in \mathbb{Q}$. Отже,

$$f(x) = \left(x^2 - 5x + 6\right) s(x) + ax + b. \tag{IV.9}$$

Підставимо в рівність (IV.9) значення $x = 2$ і $x = 3$ (корені многочлена $g(x)$). Маємо:

$$\begin{cases} f(2) = 2a + b, \\ f(3) = 3a + b; \end{cases} \quad \text{або, з огляду на (IV.8),} \quad \begin{cases} 1 = 2a + b, \\ 2 = 3a + b, \end{cases}$$

звідки $\begin{cases} a = 1, \\ b = -1. \end{cases}$ Тоді шукана остача від ділення многочлена $f(x)$ на многочлен $g(x)$ дорівнює $r(x) = x - 1$.

Розв'язання в Maple. Розв'язання задачі зводиться до системи лінійних рівнянь $\begin{cases} r_1 = ac_1 + b, \\ r_2 = ac_2 + b; \end{cases}$, де c_1, c_2 – корені многочлена $f(x)$, яку розв'язуємо в Maple:

```
> r1:=1: r2:=2: c1:=2: c2:=3:
  solve({r1=a*c1+b,r2=a*c2+b},{a,b});
```

$$\{a = 1,\ b = -1\}$$

Отже, $r(x) = x - 1$.

Завдання 36. Остачі від ділення многочлена $f(x)$ з кільця $\mathbb{Q}[x]$ на $g_1(x) = x - c_1$ і $g_2(x) = x - c_2$ дорівнюють відповідно r_1 і r_2. Знайти остачу від ділення многочлена $f(x)$ на многочлен $g(x) = (x - c_1)(x - c_2)$, якщо:

	c_1	c_2	r_1	r_2
36.1.	-5	3	-9	7
36.2.	-3	1	2	3
36.3.	-4	-5	0	2
36.4.	-2	5	1	3
36.5.	-2	2	1	2
36.6.	3	-1	1	0
36.7.	2	1	2	3
36.8.	1	-3	1	2
36.9.	-3	-1	1	3
36.10.	-1	2	0	1
36.11.	3	-5	0	1
36.12.	4	1	1	2
36.13.	-1	-3	3	1

	c_1	c_2	r_1	r_2
36.14.	-1	-2	0	2
36.15.	-2	-3	2	1
36.16.	2	-2	1	2
36.17.	-3	3	1	2
36.18.	-1	1	2	3
36.19.	-4	3	2	3
36.20.	-3	2	3	1
36.21.	-4	-3	3	1
36.22.	-3	-4	1	3
36.23.	3	-2	1	3
36.24.	1	3	2	4
36.25.	4	-3	1	2

Приклад 37.1. Розділити многочлен на двочлен, використовуючи схему Горнера:

а) $f(x) = x^4 - 2x^3 + x - 1$ на $x - 3$ в кільці $\mathbb{Q}[x]$;

б) $f(x) = \overline{2}x^8 + \overline{3}x^7 + x^4 + \overline{2}x^2 + \overline{2}$ на $x - \overline{3}$ в кільці $\mathbb{Z}_7[x]$;

в) $f(x) = 3x^4 - 5ix^3 + 7x^2 + ix - 21$ на $x - 2i$ в кільці $\mathbb{C}[x]$.

Розв'язання. а) Маємо: $a_4 = 1$, $a_3 = -2$, $a_2 = 0$, $a_1 = 1$, $a_0 = -1$. Складемо таблицю:

	1	-2	0	1	-1
3	$\underbrace{1}_{b_3 = 1}$	$\underbrace{1 \cdot 3 - 2}_{b_2 = 1}$	$\underbrace{1 \cdot 3 + 0}_{b_1 = 3}$	$\underbrace{3 \cdot 3 + 1}_{b_0 = 10}$	$\underbrace{3 \cdot 10 - 1}_{r = 29}$

Таким чином, неповна частка $q(x) = x^3 + x^2 + 3x + 10$, а остача $r = 29$.

б) Маємо: $a_8 = \overline{2}$, $a_7 = \overline{3}$, $a_6 = \overline{0}$, $a_5 = \overline{0}$, $a_4 = \overline{1}$, $a_3 = \overline{0}$, $a_2 = \overline{2}$, $a_1 = \overline{0}$, $a_0 = \overline{2}$. Складемо таблицю:

	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$b_7 = \overline{2}$	$b_6 = \overline{2}$	$b_5 = \overline{6}$	$b_4 = \overline{4}$	$b_3 = \overline{6}$	$b_2 = \overline{4}$	$b_1 = \overline{0}$	$b_0 = \overline{0}$	$r = \overline{2}$

Отже, $q(x) = \overline{2}x^7 + \overline{2}x^6 + \overline{6}x^5 + \overline{4}x^4 + \overline{6}x^3 + \overline{4}x^2$, а остача $r = \overline{2}$.

в) Маємо: $a_4 = 3$, $a_3 = -5i$, $a_2 = 7$, $a_1 = i$, $a_0 = -2$. Складемо таблицю:

	1	-2	0	1	-1
$2i$	$b_3 = 3$	$b_2 = i$	$b_1 = 5$	$b_0 = 11i$	$r = -24$

Таким чином, неповна частка s і остача r від ділення f на $x-3$ дорівнюють відповідно $s = 3x^3 + ix^2 + 5x + 11i$, $r = -24$.

Розв'язання в Maple. а) Нехай $x - c$ – двочлен, на який потрібно розділити з остачею многочлен $f(x)$. Задаємо многочлен $f(x)$ і елемент c.

```
> f:=x^4-2*x^3+x-1:          c:=3:
```

Нехай n – степінь многочлена $f(x)$:

```
> n:=degree(f,x):
```

Старший коефіцієнт неповної частки $s(x)$ від ділення $f(x)$ на $x - 3$ дорівнює старшому коефіцієнту многочлена $f(x)$:

```
> b[n-1]:=coeff(f,x,n);
```

$$b_3 := 1$$

решту коефіцієнтів b_i многочлена $s(x)$ знаходимо за формулою (IV.6):

```
> for i from n-2 by -1 to 0 do
     b[i]:=b[i+1]*c+coeff(f,x,i+1);
  end do;
```

$$b_2 := 1$$
$$b_1 := 3$$
$$b_0 := 10$$

Многочлен-остачу r знаходимо за формулою (IV.7):

```
> r:=b[0]*c+coeff(f,x,0);
```

$$r := 29$$

Таким чином, неповна частка $s(x)$ і остача r від ділення $f(x)$ на $x - 3$ дорівнюють відповідно $s(x) = x^3 + x^2 + 3x + 10$, $r = 29$.

б) Над скінченним полем змінюється формат введення многочлена $f(x)$, і при пошуку коефіцієнтів b_i додаємо оператор mod :

```
> f:=2*x^8+3*x^7-6*x^4+2*x^2-5 mod 7; c:=3;
```

$$f := 2\,x^8 + 3\,x^7 + x^4 + 2\,x^2 + 2$$
$$c := 3$$

```
> n:=degree(f,x);
```

$$n := 8$$

```
> b[n-1]:=coeff(f,x,n);
  for i from n-2 by -1 to 0 do
     b[i]:=b[i+1]*c+coeff(f,x,i+1) mod 7;
  end do;
  r:=b[0]*c+coeff(f,x,0) mod 7;
```

$$b_7 := 2$$
$$b_6 := 2$$
$$b_5 := 6$$
$$b_4 := 4$$
$$b_3 := 6$$
$$b_2 := 4$$
$$b_1 := 0$$
$$b_0 := 0$$
$$r := 2$$

Таким чином, неповна частка $s(x)$ і остача r від ділення $f(x)$ на $x - \overline{3}$ дорівнюють відповідно $s = \overline{2}x^7 + \overline{2}x^6 + \overline{6}x^5 + \overline{4}x^4 + \overline{6}x^3 + \overline{4}x^2$, $r = \overline{2}$.

в) Для многочленів з комплексними коефіцієнтами розв'язання аналогічне п.а):

```
> f:=3*x^4-5*I*x^3+7*x^2+I*x-2:
  c:=2*I:

> n:=degree(f,x):

> b[n-1]:=coeff(f,x,n);
  for i from n-2 by -1 to 0 do
      b[i]:=b[i+1]*c+coeff(f,x,i+1);
  end do;
```

$$b_3 := 3$$
$$b_2 := I$$
$$b_1 := 5$$
$$b_0 := 11\,I$$

```
> r:=b[0]*c+coeff(f,x,0);
```

$$r := -24$$

Таким чином, неповна частка $s(x)$ і остача r від ділення $f(x)$ на $x - 3$ дорівнюють відповідно $s(x) = 3x^3 + ix^2 + 5x + 11i$, $r = -24$.

Приклад 37.2. Використовуючи схему Горнера, обчислити $f(-2)$ і розкласти многочлен $f(x) = x^4 - 2x^3 + 4x^2 - 6x + 8$ за степенями двочлена $x + 2$.

Розв'язання. За теоремою Безу остача від ділення многочлена $f(x)$ на двочлен $x-c$ дорівнює $f(c)$. Знайдемо цю остачу, використовуючи схему Горнера:

	1	-2	4	-6	8
-2	1	-4	12	-30	$\boxed{68}$

Отже, $f(-2)=68$.

Щоб знайти коефіцієнти розкладу многочлена $f(x)$ за степенями $x+2$, треба за схемою Горнера спочатку розділити з остачею на $x+2$ многочлен $f(x)$, потім першу неповну частку, другу неповну частку і т.д. Одержані при цьому остачі і є шуканими коефіцієнтами. Продовжимо таблицю:

	1	-2	4	-6	8
-2	1	-4	12	-30	$\boxed{68}$
-2	1	-6	24	$\boxed{-78}$	
-2	1	-8	$\boxed{40}$		
-2	1	$\boxed{-10}$			
-2	$\boxed{1}$				

Шуканий розклад многочлена $f(x)$ має вигляд:

$$f(x)=(x+2)^4-10(x+2)^3+40(x+2)^2-78(x+2)+68.$$

Розробка процедур. Створимо процедуру **HornerScheme** для реалізації схеми Горнера. Задаємо таблицю T, що має $n+2$ рядки і $n+2$ стовпчики,ж де $n=\deg f$:

```
> T:= Array(1..n+2,1..n+2):
```

Клітинку $T[1,1]$ залишаємо порожньою:

```
> T[1,1]:=‘‘:
```

В клітинках $T[1,2]$, $T[1,3]$, ..., $T[1,n+2]$ записуємо коефіцієнти многочлена:

```
> for j from 2 to n+2 do T[1,j]:=coeff(f,x,n-j+2): end do:
```

Тепер заповнюємо другий рядок таблиці. В клітинку $T[2,1]$ вміщуємо елемент c:

```
> T[2,1]:=c:
```

в клітинку $T[2,2]$ зносимо старший коефіцієнт многочлена:

```
> T[2,2]:=T[1,2]:
```

Решту клітинок другого рядка заповнюємо за формулами (IV.6) і (IV.7):

```
> for j from 3 to n+2 do T[2,j]:=T[2,j-1]*c+T[1,j]; end do:
```

Третій рядок таблиці заповнюємо аналогічно з єдиною відмінністю: останню клітинку слід залишити порожньою. Отже, в клітинку $T[3,1]$ вміщуємо елемент c, в клітинку $T[3,2]$ зносимо старший коефіцієнт многочлена, клітинки $T[3,3], T[3,4], ..., T[3,n+1]$ заповнюємо:

```
> T[3,1]:=c:
  T[3,2]:=T[1,2]:

> for j from 3 to n+2 do T[3,j]:=T[3,j-1]*c+T[2,j]; end do:
```

клітинка $T[3,n+2]$ – порожня:

```
> T[3,n+2]:=‘‘:
```

і т.д. аналогічно.

Таким чином, в кожному рядку i ($i \in \overline{2,n+2}$) перша клітинка $T[i,1]$ заповнюється елементом c, а друга клітинка $T[i,2]$ – старшим коефіцієнтом многочлена $f(x)$:

```
> T[i,1]:=c; T[i,2]:=T[1,2];
```

З 3-го і до $(n+4-i)$-го стовпчика клітинки заповнюємо (використовуючи клітинки попереднього рядка):

```
> for j from 3 to n+4-i do T[i,j]:=T[i,j-1]*c+T[i-1,j]; end do;
```

а стовпчики з $(n+5-i)$-го до $(n+2)$-го залишаємо порожніми:

```
> for j from n+5-i to n+2 do T[i,j]:=‘‘; end do:
```

Маємо наступну процедуру:

```
HornerScheme:=proc(f,c)
local n,T,j,i:
   n:=degree(f,x):
   T:= Array(1..n+2,1..n+2): T[1,1]:=‘‘:
   for j from 2 to n+2 do T[1,j]:=coeff(f,x,n-j+2): end do:
   for i from 2 to n+2 do
      T[i,1]:=c; T[i,2]:=T[1,2];
      for j from 3 to n+4-i do T[i,j]:=T[i,j-1]*c+T[i-1,j]; end do;
      for j from n+5-i to n+2 do T[i,j]:=‘‘; end do:
   end do;
   return(T);
end proc:
```

Розв'язання в Maple. Для розкладу многочлена $f(x)$ за степенями $x-c$ в Maple зручно використовувати вбудовану команду **taylor(f, x=c)**, при

цьому її бажано вводити у форматі **taylor(f, x=c, k)**, де $k = n+1$ – число, що на одиницю більше за степінь многочлена.

```
> f:=x^4-2*x^3+4*x^2-6*x+8:
> taylor(f, x=-2,5);
```

$$68 - 78\,(x+2) + 40\,(x+2)^2 - 10\,(x+2)^3 + (x+2)^4$$

Можна просто знайти коефіцієнти b_k розкладу многочлена $f(x)$ за степенями $x - c$ (за допомогою команди **coeftayl(f, x=c, k)**).

```
> coeftayl(f, x=-2, 0);
```

$$68$$

```
> coeftayl(f, x=-2, 1);
```

$$-78$$

```
> coeftayl(f, x=-2, 2);
```

$$40$$

```
> coeftayl(f, x=-2, 3);
```

$$-10$$

```
> coeftayl(f, x=-2, 4);
```

$$1$$

і самостійно записати многочлен $f(x)$.

Для перевірки проміжних обчислень використовуємо розроблену процедуру:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> HornerScheme(x^4-2*x^3+4*x^2-6*x+8,-2);
```

$$\begin{bmatrix} & 1 & -2 & 4 & -6 & 8 \\ -2 & 1 & -4 & 12 & -30 & 68 \\ -2 & 1 & -6 & 24 & -78 & \\ -2 & 1 & -8 & 40 & & \\ -2 & 1 & -10 & & & \\ -2 & 1 & & & & \end{bmatrix}$$

Приклад 37.3. Використовуючи схему Горнера, обчислити $f(-2i)$ і розкласти многочлен $f(x) = x^4 + (2+i)x^3 - 2ix - (1+i)$ із кільця $\mathbb{C}[x]$ за степенями двочлена $x + 2i$.

Розв'язання. Використовуємо схему Горнера:

	1	$2+i$	$-2i$	0	$-(1+i)$
$-2i$	1	$2-i$	$-2-4i$	$-8+2i$	3+15i
$-2i$	1	$2-3i$	$-8-8i$	$-24+18i$	
$-2i$	1	$2-5i$	-18-12i		
$-2i$	1	$2-7i$			
$-2i$	1				

Шуканий розклад многочлена $f(x)$ має вигляд:

$$f(x) = (x+2i)^4+(2-7i)(x+2i)^3+(-18-12i)(x+2i)^2+(-24+18i)(x+2i)+3+15i.$$

Розв'язання в Maple. Спочатку обчислюємо значення $f(-2i)$. Маємо:

```
> f:=x^4+(2+I)*x^3-2*I*x-(1+I):
  coeftayl(f, x=-2*I, 0);
```

$$3 + 15\,I$$

Таким чином, $f(-2i) = 3 + 15i$. Тепер за допомогою команди **taylor** розкладаємо за степенями $x + 2i$:

```
> taylor(f, x=-2*I);
```

$$3 + 15\,I + (-24 + 18\,I)\,(x + 2\,I) + (-18 - 12\,I)\,(x + 2\,I)^2 + (2 - 7\,I)\,(x + 2\,I)^3 + (x + 2\,I)^4$$

Далі застосовуємо процедуру **HornerScheme**:

```
> HornerScheme(x^4+(2+I)*x^3-2*I*x-(1+I),-2*I);
```

$$\begin{bmatrix} & 1 & 2+I & 0 & -2\,I & -1-I \\ -2\,I & 1 & 2-I & -2-4\,I & -8+2\,I & 3+15\,I \\ -2\,I & 1 & 2-3\,I & -8-8\,I & -24+18\,I & \\ -2\,I & 1 & 2-5\,I & -18-12\,I & & \\ -2\,I & 1 & 2-7\,I & & & \\ -2\,I & 1 & & & & \end{bmatrix}$$

Приклад 37.4. Використовуючи схему Горнера, обчислити $f(\overline{4})$ і розкласти многочлен $f(x) = x^4+\overline{3}x^3-\overline{4}x-\overline{5}$ із кільця $\mathbb{Z}_7[x]$ за степенями двочлена $x - \overline{4}$.

Розв'язання. Використовуємо схему Горнера:

	$\overline{1}$	$\overline{3}$	$\overline{0}$	$-\overline{4}$	$-\overline{5}$
$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{3}$	$\boxed{\overline{0}}$
$\overline{4}$	$\overline{1}$	$\overline{4}$	$\overline{2}$	$\boxed{\overline{4}}$	
$\overline{4}$	$\overline{1}$	$\overline{1}$	$\boxed{\overline{6}}$		
$\overline{4}$	$\overline{1}$	$\boxed{\overline{5}}$			
$\overline{4}$	$\boxed{\overline{1}}$				

Шуканий розклад многочлена $f(x)$ має вигляд:

$$f(x) = (x-\overline{4})^4 + \overline{5}(x-\overline{4})^3 + \overline{6}(x-\overline{4})^2 + \overline{4}(x-\overline{4}).$$

Розробка процедур. Для побудови схеми Горнера для многочленів, заданих над скінченними полями $\mathbb{Z}_m$, дещо модифікуємо процедуру **HornerScheme**, а саме, додамо параметр m:

```
HornerSchemeMod:=proc(f,c,m)
local n,T,j,i:
   n:=degree(f,x):
   T:= Array(1..n+2,1..n+2):
   T[1,1]:=‘‘:
   for j from 2 to n+2 do T[1,j]:=coeff(f,x,n-j+2): end do:
   for i from 2 to n+2 do
      T[i,1]:=c;
      T[i,2]:=T[1,2];
      for j from 3 to n+4-i do
         T[i,j]:=T[i,j-1]*c+T[i-1,j] mod m;
      end do;
      for j from n+5-i to n+2 do T[i,j]:=‘‘; end do:
   end do;
   return(T);
end proc:
```

Розв'язання в Maple. Отриманий результат перевіряємо аналогічно до попередніх прикладів 37.2-37.3, додаючи оператор **mod m**.

```
> f:=x^4+3*x^3-4*x-5:
  coeftayl(f, x=4, 0) mod 7;
```

$$0$$

```
> taylor(f,x=4) mod 7;
```

$$4\,(x-4) + 6\,(x-4)^2 + 5\,(x-4)^3 + (x-4)^4$$

Отже, $f(\overline{4}) = \overline{0}$, розклад $f(x)$ за степенями двочлена $x - \overline{4}$ має вигляд:

$$f = (x - \overline{4})^4 + \overline{5}(x - \overline{4})^3 + \overline{6}(x - \overline{4})^2 + \overline{4}(x - \overline{4}).$$

Для перевірки проміжних обчислень використовуємо процедуру **HornerSchemeMod**. Підключаємо бібліотеку atchlib:

```
> read('e:/atchlib.m'); with(atchlib):
```

Для заданого многочлена $f(x)$, значень $c = \overline{4}$ і $m = 7$ матимемо:

```
> HornerSchemeMod(x^4+3*x^3-4*x-5,4,7);
```

$$\begin{bmatrix} & 1 & 3 & 0 & -4 & -5 \\ 4 & 1 & 0 & 0 & 3 & 0 \\ 4 & 1 & 4 & 2 & 4 & \\ 4 & 1 & 1 & 6 & & \\ 4 & 1 & 5 & & & \\ 4 & 1 & & & & \end{bmatrix}$$

Завдання 37. Використовуючи схему Горнера, обчислити $f(a)$ і розкласти многочлен $f(x)$ за степенями $x - a$:

37.1. $f(x) = x^4 - 4ix^3 - 7x^2 + 6ix + 2, \quad a = i \quad$ в $\mathbb{C}[x]$.

37.2. $f(x) = x^4 + x^3 - 5x^2 - 10x - 7, \quad a = -1 \quad$ в $\mathbb{Q}[x]$.

37.3. $f(x) = \overline{4}x^4 + \overline{4}x^2 - \overline{3}x + \overline{3}, \quad a = \overline{2} \quad$ в $\mathbb{Z}_5[x]$.

37.4. $f(x) = -2x^5 - 20x^4 - 80x^3 - 163x^2 - 173x - 75, \quad a = -2 \quad$ в $\mathbb{Q}[x]$.

37.5. $f(x) = x^4 - 8ix^3 - 25x^2 + (36i + 1)x + 24 - 2i, \quad a = 2i \quad$ в $\mathbb{C}[x]$.

37.6. $f(x) = x^5 - 5x^4 + 9x^3 - 7x^2 + 4x - 4, \quad a = 1 \quad$ в $\mathbb{Q}[x]$.

37.7. $f(x) = \overline{4}x^4 - x^3 + \overline{3}x^2 - \overline{1}, \quad a = \overline{4} \quad$ в $\mathbb{Z}_7[x]$.

37.8. $f(x) = x^4 + 8x^2 + 12ix - 1, \quad a = -i$ в $\mathbb{C}[x]$.

37.9. $f(x) = -x^5 - \overline{3}x^4 - x^3 + \overline{2}x + \overline{4}, \quad a = \overline{5} \quad$ в $\mathbb{Z}_7[x]$.

37.10. $f(x) = x^3 - (1 - 3i)x^2 - (4 + 2i)x + 7 - 2i, \quad a = 1 - i \quad$ в $\mathbb{C}[x]$.

37.11. $f(x) = x^4 + 8x^3 + 24x^2 + 29x + 12, \quad a = -2 \quad$ в $\mathbb{Q}[x]$.

37.12. $f(x) = x^5 - \overline{4}x^4 + \overline{2}x^2 - x^2 + x - \overline{4}, \quad a = \overline{2} \quad$ в $\mathbb{Z}_5[x]$.

37.13. $f(x) = \overline{2}x^5 - x^4 + x^3 - x^2 + x - \overline{4}, \quad a = \overline{4} \quad$ в $\mathbb{Z}_5[x]$.

37.14. $f(x) = 2x^4 - 10x^2 - 12x, \quad a = -1 \quad$ в $\mathbb{Z}[x]$.

37.15. $f(x) = 2x^4 + 8ix^3 - 14x^2 - 12ix + 4 + i, \quad a = -i \quad$ в $\mathbb{C}[x]$.

37.16. $f(x) = x^5 + x - 5, \quad a = -1 \quad$ в $\mathbb{Q}[x]$.

37.17. $f(x) = \overline{2}x^4 - x^3 + x^2, \quad a = \overline{2} \quad$ в $\mathbb{Z}_3[x]$.

37.18. $f(x) = -x^4 + \overline{3}x^3 - \overline{4}x^2 - x + \overline{6}, \quad a = \overline{6} \quad$ в $\mathbb{Z}_7[x]$.

37.19. $f(x) = x^5 + 5x^4 + 10x^3 + 9x^2 + 4x - 2, \quad a = -1 \quad$ в $\mathbb{Q}[x]$.

37.20. $f(x) = x^3 + (5 + 3i)x^2 + (10i + 4)x + 7i - 2, \quad a = -1 - i \quad$ в $\mathbb{C}[x]$.

37.21. $f(x) = x^5 - 4x^4 + 7x^3 - 8x^2 + 12x - 1, \quad a = 1 \quad$ в $\mathbb{Q}[x]$.

37.22. $f(x) = \overline{2}x^{11} - 3x^3 + \overline{3}x^2 - \overline{3}x + \overline{8}, \quad a = \overline{1} \quad$ в $\mathbb{Z}_5[x]$.

37.23. $f(x) = \overline{6}x^5 + \overline{4}x^4 - x^3 + \overline{2}x + \overline{4}, \quad a = \overline{5} \quad$ в $\mathbb{Z}_7[x]$.

37.24. $f(x) = -x^5 - 5x^4 + 8x^2 + x + 1, \quad a = -1 \quad$ в $\mathbb{Q}[x]$.

37.25. $f(x) = x^5 + 11x^3 + 33x, \quad a = i \quad$ в $\mathbb{C}[x]$.

3. Незвідні множники над полем. Розклад многочленів на незвідні множники

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x) \in P[x]$, P – поле. Многочлен $f(x)$ називається незвідним в $P[x]$ (або над полем P), якщо він не є константою і не має в $P[x]$ інших дільників, крім констант і многочленів виду $cf(x)$, де $c \in P\backslash\{0\}$.

Многочлен $f(x)$ називається звідним в $P[x]$ (над полем P), якщо $\deg f \geqslant 1$ і в кільці $P[x]$ існують такі многочлени $g(x), s(x)$, що $f(x) = g(x)s(x)$, $\deg g \geqslant 1$ і $\deg s \geqslant 1$.

Теорема. *Будь-який многочлен ненульового степеня над полем P можна подати у вигляді добутку незвідних многочленів $p_k(x)$, $1 \leqslant k \leqslant l$, над полем P:*

$$f(x) = p_1(x)p_2(x)\dots p_l(x).$$

Такий розклад є єдиним з точністю до сталих множників і порядку нумерації многочленів $p_k(x)$.

Теорема. *Многочлен першого степеня – незвідний над будь-яким полем.*

Запис многочлена $f(x)$ з кільця $P[x]$ у вигляді добутку

$$f(x) = [p_1(x)]^{k_1} [p_2(x)]^{k_2} \dots [p_m(x)]^{k_m},$$

де $p_1(x), p_2(x), ..., p_m(x)$ – попарно взаємно прості і незвідні над полем P многочлени, називають канонічним розкладом многочлена $f(x)$ над полем P.

Теорема. *Канонічний розклад для будь-якого многочлена $f(x)$ ненульового степеня над полем P завжди існує і єдиний з точністю до сталих множників та порядку нумерації множників.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 38.1. Розкласти на незвідні в кільцях $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ множники многочлени: а) $f(x) = x^3 - 3x - 2$; б) $g(x) = x^4 - x^2 - 2$.

Розв'язання. а) Оскільки

$$f(x) = x^3 - 3x - 2 = (x^3 + 1) + (-3x - 3) = (x+1)(x^2 - x + 1) - 3(x+1) = \\ = (x+1)(x^2 - x - 2) = (x+1)(x-2)(x+1) = (x-2)(x+1)^2,$$

то многочлен має два *різні* незвідні множники: $f_1(x) = x - 2$ кратності 1 і $f_2(x) = x + 1$ кратності 2. Цей же розклад многочлен $f(x)$ матиме і в кільцях $\mathbb{R}[x]$, і $\mathbb{C}[x]$, оскільки многочлени $f_1(x)$ і $f_2(x)$ першого степеня, і тому незвідні.

б) Розглянемо многочлен

$$g(x) = x^4 - x^2 - 2 = x^4 - x^2 + \frac{1}{4} - \frac{9}{4} = \left(x^2 - \frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 = (x^2 - 2)(x^2 + 1).$$

Цей розклад є розкладом $g(x)$ на незвідні множники в кільці $\mathbb{Q}[x]$.

Дійсно, припустимо, що многочлен $g_1(x) = x^2 - 2$ є звідним в $\mathbb{Q}[x]$. Тоді

$$x^2 - 2 = (ax + b)(cx + d),$$

де $a, b, c, d \in \mathbb{Q}$, причому $a \neq 0$, $c \neq 0$. Покладемо $x = -\frac{b}{a}$, тоді $\left(-\frac{b}{a}\right)^2 - 2 = 0$, тобто $\left(\frac{b}{a}\right)^2 = 2$, що неможливо при $\frac{b}{a} \in \mathbb{Q}$. Аналогічно якщо припустимо, що многочлен $g_2(x) = x^2 + 1$ є звідним в кільці $\mathbb{Q}[x]$, то отримаємо розклад

$$x^2 + 1 = (ax + b)(cx + d),$$

де $a, b, c, d \in \mathbb{Q}$, причому $a \neq 0$, $c \neq 0$. Звідки, поклавши $x = -\frac{b}{a}$, маємо: $\left(-\frac{b}{a}\right)^2 + 1 = 0$, тобто $b^2 + a^2 = 0$. Але тоді $a = b = 0$, що суперечить вибору a.

В кільці $\mathbb{R}[x]$ многочлен $g_1(x) = x^2 - 2$ є звідним, а тому маємо інший розклад $g(x)$ на незвідні множники:

$$g(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 1).$$

В свою чергу, в кільці $\mathbb{C}[x]$ многочлен $g_2(x) = x^2 + 1 = (x + i)(x - i)$, тому

$$g(x) = (x - \sqrt{2})(x + \sqrt{2})(x + i)(x - i).$$

Розв'язання в Maple. Для розкладу многочлена $f(x) \in P[x]$ на незвідні над P множники використовується команда **factor(f,P)**. Параметр **P** – необов'язковий, за замовчуванням (відсутності параметра) здійснюється розклад над полем $\mathbb{Q}$. Для розкладу над полем $\mathbb{R}$ замість **P** слід зазначити **real**, для розкладу над полем $\mathbb{C}$ – **complex**.

а) Розкладаємо многочлен $f(x)$ послідовно над полями $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

```
> factor(x^3-3*x-2);
```

$$(x - 2)\,(x + 1)^2$$

```
> factor(x^3-3*x-2,real);
```

$$(x + 1.)^2\,(x - 2.)$$

```
> factor(x^3-3*x-2,complex);
```

$$(x + 1.)^2\,(x - 2.)$$

б) Для многочлена $g(x)$ аналогічно:

```
> factor(x^4-x^2-2);
```

$$(x^2 - 2)\,(x^2 + 1)$$

```
> factor(x^4-x^2-2,real);
```

$$(x + 1.414213562)\,(x - 1.414213562)\,(x^2 + 1.)$$

```
> factor(x^4-x^2-2,complex);
```

$$(x + 1.414213562)\,(x + 1.\,I)\,(x - 1.\,I)\,(x - 1.414213562)$$

Щоб одержати запис ірраціонального числа $\sqrt{2} = 1.414213562...$ в розкладі над полем дійсних чисел у вигляді $\sqrt{2}$ можна вказати поле P, над яким необхідно розкласти многочлен, як поле $\mathbb{Q}[\sqrt{2}]$ (при цьому зазначаємо лише радикал $\sqrt{2}$):

```
> factor(x^4-x^2-2,sqrt(2));
```

$$-(x^2 + 1)\,(x + \sqrt{2})\,(-x + \sqrt{2})$$

Щоб визначити, чи є многочлен незвідним над деяким полем, можна використати команду **irreduc(f,P)**. Результатом цієї команди є: *true* – якщо многочлен f – незвідний над P; *false* – якщо многочлен f – звідний над P.

В процесі розв'язання було доведено, що многочлени $g_1(x) = x^2 - 2$ і $g_2(x) = x^2 + 1$ є незвідними в кільці $\mathbb{Q}[x]$. Дійсно,

```
> g1:=x^2-2: irreduc(g1);
```

$$true$$

```
> g2:=x^2+1: irreduc(g2);
```

$$true$$

Далі над полем $\mathbb{R}$ многочлен $g_1(x)$ – звідний, а $g_2(x)$ – незвідний:

```
> irreduc(g1,real); irreduc(g2,real);
```

$$false$$

$$true$$

а над полем $\mathbb{C}$ обидва многочлени – звідні:

```
> irreduc(g1,complex); irreduc(g2,complex);
```

$$false$$

$$false$$

Зауваження. Часто необхідно розкласти многочлен на множники 1-го степеня. Такий розклад існує для будь-якого многочлена степеня $\geqslant 1$ в його полі розкладу. Відомо також, що поле $\mathbb{C}$ містить поле розкладу довільного многочлена степеня $\geqslant 1$ з числовими коефіцієнтами, тому над полем $\mathbb{C}$ кожний із многочленів степеня $\geqslant 1$ можна розкласти на множники 1-го степеня. Це означає, що розклад на множники в кільці $\mathbb{C}[x]$ заданих многочленів можна знаходити за допомогою команди **Split(f, x)** із пакету **PolynomialTools**, результатом якої є розклад многочлена $f(x)$ в добуток множників 1-го степеня:

```
> with(PolynomialTools):
  f:=x^4-x^2-2:
  f1:=Split(f, x);
```

$$f1 := (\mathrm{RootOf}(\_Z^2 - 2) + x)\,(x - \mathrm{RootOf}(\_Z^2 + 1))\,(\mathrm{RootOf}(\_Z^2 + 1) + x)\,(x - \mathrm{RootOf}(\_Z^2 - 2))$$

Запис RootOf(_Z$^2 - 2$) використовується для позначення числа, яке є одним із розв'язків рівняння $z^2 - 2 = 0$ (тобто для числа $\sqrt{2}$). Аналогічно запис RootOf(_Z$^2 + 1$) – для позначення числа i. Подамо цю відповідь у радикалах:

```
> convert(f1, radical);
```

$$(x + \sqrt{2})\,(x - I)\,(I + x)\,(x - \sqrt{2})$$

Приклад 38.2. Розкласти на незвідні в кільці $\mathbb{Z}_5[x]$ множники многочлен

$$f(x) = x^5 + x^3 + x^2 + \overline{1}.$$

Розв'язання. Для розкладу многочлена $f(x)$ на множники застосуємо спосіб групування:

$$f(x) = x^5 + x^3 + x^2 + \overline{1} = x^3(x^2 + \overline{1}) + (x^2 + \overline{1}) = (x^2 + \overline{1})(x^3 + \overline{1}).$$

Далі використовуємо формули скороченого множення:

$$x^2 + \overline{1} = x^2 - \overline{4} = (x + \overline{2})(x - \overline{2}),$$
$$x^3 + \overline{1} = (x + \overline{1})(x^2 - x + \overline{1}).$$

Таким чином,

$$f(x) = (x + \overline{2})(x - \overline{2})(x + \overline{1})(x^2 - x + \overline{1}).$$

Покажемо, що многочлен $f_1(x) = x^2 - x + \overline{1}$ – незвідний в кільці $\mathbb{Z}_5[x]$. Припустимо супротивне. Нехай $f_1(x)$ є звідним. Тоді його можна подати у вигляді

$$f_1(x) = (\overline{a}x + \overline{b})(\overline{c}x + \overline{d}),$$

де $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{Z}_5[x]$, $\overline{a} \neq \overline{0}$, $\overline{c} \neq \overline{0}$. Тоді $f_1(-\overline{a}^{\,-1}\overline{b}) = \overline{0}$, проте

$$f_1(\overline{0}) = \overline{1}, \qquad f_1(\overline{1}) = \overline{1}, \qquad f_1(\overline{2}) = \overline{3}, \qquad f_1(\overline{3}) = \overline{2}, \qquad f_1(\overline{4}) = \overline{3}.$$

Отримана суперечність показує, що припущення невірне. Отже, $f_1(x)$ є незвідним в $\mathbb{Z}_5[x]$, а шуканий розклад многочлена $f(x)$ має вигляд

$$f(x) = (x + \overline{2})(x - \overline{2})(x + \overline{1})(x^2 - x + \overline{1}).$$

Розв'язання в Maple. Для розкладу на незвідні множники над скінченними полями $\mathbb{Z}_p$ використовується команда **factor** у відповідному форматі.

Маємо:

```
> Factor(x^5+x^3+x^2+1) mod 5;
```

$$(x^2 + 4\,x + 1)\,(x + 3)\,(x + 2)\,(x + 1)$$

Оскільки в кільці $\mathbb{Z}_5[x]$ справедливі рівності: $x^2 + \overline{4}x + \overline{1} = x^2 - x + \overline{1}$, $x + \overline{3} = x - \overline{2}$, то результат збігається із аналітично отриманим розв'язком.

Зауваження. В Maple є можливість розкладати многочлен на множники не лише над основними числовими полями $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, але й над полями виду $P = \mathbb{Q}(\sqrt{d})$, де d – довільне раціональне число. В такому випадку поле P характеризується параметрами: **sqrt(d); d^ (1/2); root(d,2); surd(d,2)**. Наприклад, якщо потрібно розкласти на множники многочлен $f = x^2 - 3$ над полем $P = \mathbb{Q}(\sqrt{3})$, то матимемо:

```
> f:=x^2-3;
```

$$f := x^2 - 3$$

```
> factor(f,sqrt(3)); factor(f,3^(1/2));
  factor(f,root(3,2)); factor(f,surd(3,2));
```

$$-(-x+\sqrt{3})\,(x+\sqrt{3})$$
$$-(-x+\sqrt{3})\,(x+\sqrt{3})$$
$$-(-x+\sqrt{3})\,(x+\sqrt{3})$$
$$-(-x+\sqrt{3})\,(x+\sqrt{3})$$

Над полем $P = \mathbb{Q}(\sqrt[3]{2})$ многочлен f – незвідний:

```
> factor(f,2^(1/3)); factor(f,root(2,3)); factor(f,surd(2,3));
```

$$x^2 - 3$$
$$x^2 - 3$$
$$x^2 - 3$$

Завдання 38. Розкласти на незвідні множники многочлен:

38.1. $f(x) = x^2(x-2)^2 + 3x^2 - 15x + 18$ в кільці $\mathbb{Q}[x]$.

38.2. $f(x) = x^4 + 11x^2 + 100$ в кільці $\mathbb{R}[x]$.

38.3. $f(x) = (x+2)(x+4)(x+6)(x+8) + 7$ в кільці $\mathbb{Q}[x]$.

38.4. $f(x) = x^6 - x^2$ в кільці $\mathbb{Z}_5[x]$.

38.5. $f(x) = (x^2+3x-1)^2 + 4x(x^2+3x-1) - 12x^2$ в кільці $\mathbb{Q}[x]$.

38.6. $f(x) = x^9 - 1$ в кільці $\mathbb{Q}[x]$.

38.7. $f(x) = 2(x^2+1)^2 + 3x^4 + 3x^2$ в кільці $\mathbb{C}[x]$.

38.8. $f(x) = x^4 - 7x^2 + 81$ в кільці $\mathbb{R}[x]$.

38.9. $f(x) = (x+1)(x+3)(x+5)(x+7) - 7$ в кільці $\mathbb{Q}[x]$.

38.10. $f(x) = x^4 + \overline{4}x - \overline{7}$ в кільці $\mathbb{Z}_{11}[x]$.

38.11. $f(x) = x^4 + 16$ в кільці $\mathbb{C}[x]$.

38.12. $f(x) = x^{12} - 1$ в кільці $\mathbb{Z}_5[x]$.

38.13. $f(x) = 4(x^2+2)^2 + 3x^3 + 6x$ в кільці $\mathbb{R}[x]$.

38.14. $f(x) = 2x^4 + 11x^2 + 12$ в кільці $\mathbb{R}[x]$.

38.15. $f(x) = (x+2)(x+3)(x+4)(x+5) - 15$ в кільці $\mathbb{Q}[x]$.

38.16. $f(x) = x^6 - x^2$ в кільці $\mathbb{Z}_{17}[x]$.

38.17. $f(x) = x^9 - x$ в кільці $\mathbb{Z}_5[x]$.

38.18. $f(x) = (x^3 + 3x)^2 + 5x^4 + 15x$ в кільці $\mathbb{Q}[x]$.

38.19. $f(x) = x(x-3)(x+1)^2 + 4x^2 - 8x - 12$ в кільці $\mathbb{Q}[x]$.

38.20. $f(x) = x^4 + 8x^3 + 16x^2 - 9$ в кільці $\mathbb{R}[x]$.

38.21. $f(x) = x^4 - \overline{2}x^2 + \overline{2}$ в кільці $\mathbb{Z}_5[x]$.

38.22. $f(x) = x^4 - 6x^2 + 7$ в кільці $\mathbb{C}[x]$.

38.23. $f(x) = (2x^2 - x + 7)^2 - 6x(2x^2 - x + 7) + 5x^2$ в кільці $\mathbb{Q}[x]$.

38.24. $f(x) = (x-1)(x-2)(x-5)(x-6) - 21$ в кільці $\mathbb{R}[x]$.

38.25. $f(x) = x^4 + \overline{4}$ в кільці $\mathbb{Z}_5[x]$.

4. Найбільший спільний дільник та найменше спільне кратне многочленів

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x)$ і $g(x)$ – многочлени над полем P. Якщо $f(x)$ і $g(x)$ діляться на многочлен $d(x)$ з кільця $P[x]$, то $d(x)$ називають їхнім спільним дільником.

Найбільшим спільним дільником многочленів $f(x)$ і $g(x)$ над полем P, називається такий їхній спільний дільник, який ділиться на будь-який спільний дільник цих многочленів, і позначається символом (f, g) або НСД(f, g). Найбільший спільний дільник заданих многочленів визначається з точністю до сталого множника. Із всіх найбільших спільних дільників многочленів $f(x)$ і $g(x)$, як правило, вибирають той, у якого старший коефіцієнт рівний 1.

Теорема. *Для будь-яких двох многочленів $f(x)$ і $g(x)$ з кільця $P[x]$ (з яких хоча б один відмінний від нуля) найбільший спільний дільник існує і асоційований із останньою відмінною від 0 остачею алгоритму Евкліда.*

Теорема (про лінійне представлення найбільшого спільного дільника)**.** *Нехай $d(x) \sim (f, g)$, де $f(x), g(x) \in P[x]$, P– поле,* $\deg f = n$, $\deg g = m$, $\deg d = k$. *Тоді існує, причому єдина, пара многочленів $u(x)$ і $v(x)$ таких, що*

$$\begin{aligned} d(x) &= f(x) \cdot u(x) + g(x) \cdot v(x), \\ &\text{де} \quad \deg u \leqslant m - k - 1, \\ &\qquad \deg v \leqslant n - k - 1. \end{aligned} \tag{IV.10}$$

Многочлени $f(x)$ і $g(x)$ з кільця $P[x]$ називаються взаємно простими, якщо кожен їхній найбільший спільний дільник є многочленом нульового степеня. При цьому пишуть $(f, g) \sim 1$.

Теорема. *Многочлени $f(x)$ і $g(x)$ з кільця $P[x]$ є взаємно простими тоді і лише тоді, коли існують многочлени $u(x), v(x) \in P[x]$ такі, що*

$$1 = f(x) \cdot u(x) + g(x) \cdot v(x).$$

Спільним кратним многочленів $f(x), g(x)$ з кільця $P[x]$ називають многочлен $s(x) \in P[x]$ такий, що ділиться і на $f(x)$, і на $g(x)$.

Найменшим спільним кратним многочленів $f(x)$ і $g(x)$ називається таке їхнє спільне кратне, на яке ділиться кожне спільне кратне цих многочленів, і позначається $[f, g]$ або $\text{НСК}(f, g)$.

Теорема. *Для будь-яких відмінних від нуля многочленів $f(x), g(x) \in P[x]$ найменше спільне кратне в $P[x]$ існує, причому*

$$[f, g] \sim \frac{f(x) \cdot g(x)}{(f, g)}.$$

Теорема. *Нехай $f(x), g(x) \in P[x]$,*

$$\begin{aligned} f(x) &= [p_1(x)]^{k_1} [p_2(x)]^{k_2} \dots [p_s(x)]^{k_s}, \\ g(x) &= [p_1(x)]^{t_1} [p_2(x)]^{t_2} \dots [p_s(x)]^{t_s} \end{aligned}$$

– їхні узагальнені канонічні розклади ($k_i \geqslant 0$, $t_i \geqslant 0$, $i = 1, 2, ..., s$). Тоді:

$$\begin{aligned} &(f, g) \sim [p_1(x)]^{r_1} [p_2(x)]^{r_2} \dots [p_s(x)]^{r_s}, \text{ де } r_i = \min_{1 \leqslant i \leqslant s} (k_i, t_i), \\ &[f, g] \sim [p_1(x)]^{m_1} [p_2(x)]^{m_2} \dots [p_s(x)]^{m_s}, \text{ де } m_i = \max_{1 \leqslant i \leqslant s} (k_i, t_i). \end{aligned}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 39.1. Знайти найбільший спільний дільник многочленів:

а) $f(x) = x^4 - 2x^3 + x - 2$ і $g(x) = 2x^3 - 2x^2 - 8$ з кільця $\mathbb{Q}[x]$;

б) $f(x) = \overline{2}x^4 + x^3 + x^2 + x - \overline{1}$ і $g(x) = \overline{2}x^4 + x^3 - x^2 - \overline{1}$ з кільця $\mathbb{Z}_5[x]$.

Розв'язання. а) Оскільки найбільший спільний дільник визначається з точністю до сталого множника, то ми можемо множити ділене і дільник на довільне відмінне від 0 число, причому не лише на початку деякого із послідовних ділень, а й в процесі самого ділення. (При цьому неповні частки $s_1(x), s_2(x), \dots$ змінюються, проте вони нас не цікавлять.)

Ділимо многочлен $f(x)$ на $g(x)$, помноживши попередньо $f(x)$ на 2.

$$
\begin{array}{rrl}
f(x) = & x^4 - 2x^3 + x - 2 & \big| \; 2x^3 - 2x^2 - 8 = g(x) \\
(* \text{ на } 2) & 2x^4 - 4x^3 + 2x - 4 & \big| \; \overline{x - 1} \\
\cline{2-2}
& 2x^4 - 2x^3 - 8x & \\
\cline{2-2}
& -2x^3 + 10x - 4 & \\
& -2x^3 + 2x^2 + 8 & \\
\cline{2-2}
& -2x^2 + 10x - 12 & \\
(\div \text{ на } -2) & x^2 - 5x + 6 &
\end{array}
$$

Таким чином, $r_1(x) \sim x^2 - 5x + 6$ в $\mathbb{Q}[x]$.

Далі ділимо $g(x)$ на многочлен, асоційований до $r_1(x)$:

$$
\begin{array}{rrl}
g(x) = & 2x^3 - 2x^2 - 8 & \big| \; \overline{x^2 - 5x + 6} \sim r_1(x) \\
(\div \text{ на } 2) & x^3 - \; x^2 - \; 4 & \big| \; x + 4 \\
\cline{2-2}
& x^3 - 5x^2 + 6x & \\
\cline{2-2}
& 4x^2 - 6x - \; 4 & \\
& 4x^2 - 20x + 24 & \\
\cline{2-2}
& 14x - 28 & \\
(\div \text{ на } 14) & x - 2 &
\end{array}
$$

Отже, $r_2(x) \sim x - 2$.

Тепер ділимо многочлен, асоційований до $r_1(x)$, на многочлен, асоційований до $r_2(x)$:

$$
\begin{array}{rrl}
r_1(x) \sim & x^2 - 5x + 6 & \big| \; \overline{x - 2} \sim r_2(x) \\
& \underline{x^2 - 2x} \quad & \big| \; x - 3 \\
& -3x + 6 & \\
& \underline{-3x + 6} & \\
& 0 & \sim r_3(x)
\end{array}
$$

Останньою відмінною від 0 остачею є $r_2(x)$. Це означає, що $(f, g) \sim r_2(x)$, тобто $(f, g) \sim x - 2$.

б) Найбільший спільний дільник двох многочленів, заданих над полем P, визначається з точністю до константи (елемента, відмінного від нульового елемента θ цього поля), тому в процесі ділення дозволяється множити ділене і дільник на довільний елемент $c \in P \backslash \{\theta\}$, тобто на $c \in \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Ділимо многочлен $f(x)$ на $g(x)$:

$$\begin{array}{rl} f(x) = \overline{2}x^4 + x^3 + x^2 + x - \overline{1} & \big| \; \overline{2}x^4 + x^3 - x^2 - \overline{1} = g(x) \\ \underline{\overline{2}x^4 + x^3 - x^2 - \overline{1}} & \big| \; \overline{1} \\ \overline{2}x^2 + x = r_1(x) & \end{array}$$

Далі ділимо $g(x)$ на $r_1(x)$:

$$\begin{array}{rl} g(x) = \overline{2}x^4 + x^3 - x^2 - \overline{1} & \big| \; \overline{2}x^2 + x = r_1(x) \\ \underline{\overline{2}x^4 + x^3} & \big| \; x^2 + \overline{2} \\ -x^2 - \overline{1} & \\ \text{(замінюємо коефіцієнти)} \quad \overline{4}x^2 + \overline{4} & \\ \underline{\overline{4}x^2 + \overline{2}x} & \\ \overline{3}x + \overline{4} & \\ (\div \text{ на } \overline{3}) \quad x + \overline{3} & \end{array}$$

Отже, $r_2(x) \sim x + \overline{3}$.

Тепер ділимо многочлен $r_1(x)$ на многочлен, асоційований до $r_2(x)$:

$$\begin{array}{rl} r_1(x) = \overline{2}x^2 + x & \big| \; x + \overline{3} \sim r_2(x) \\ \underline{\overline{2}x^2 + x} & \big| \; \overline{2}x \\ \overline{0} \sim r_3(x) & \end{array}$$

Останньою відмінною від $\overline{0}$ остачею є $r_2(x)$. Це означає, що $(f, g) \sim r_2(x)$, тобто $(f, g) \sim x + \overline{3}$.

Розв'язання в Maple. а) Для знаходження НСД двох многочленів $f(x)$ і $g(x)$ над числовими полями використовується команда **gcd(f, g)**:

```
> f:=x^4-2*x^3+x-2: g:=2*x^3-2*x^2-8:
> gcd(f,g);
```

$$x - 2$$

б) У випадку скінченного поля використовуємо формат **Gcd(f, g) mod m**.

```
> f:=2*x^4+x^3+x^2+x-1 mod 5:
  g:=2*x^4+x^3-x^2-1 mod 5:
> Gcd(f,g) mod 5;
```

$$x + 3$$

Зверніть увагу: у випадку використання команди в звичайному форматі, отримуємо неправильний результат:

```
> gcd(f,g);
```

$$1$$

Приклад 39.2. Знайти найбільший спільний дільник многочленів $f(x) = x^6 - x^5 - 2x^4 - 16x^2 + 16x + 32$ і $g(x) = (x+1)^2(x^2-4)(x-2)^2$ з кільця $\mathbb{Q}[x]$.

Розв'язання. Для многочлена $g(x)$ легко знайти канонічний розклад в кільці $\mathbb{Q}[x]$:

$$g(x) = (x+1)^2(x^2-4)(x-2)^2 = (x+1)^2(x+2)(x-2)(x-2)^2 = \\ = (x-2)^3(x+1)^2(x+2).$$

Тому доцільно знайти і канонічний розклад многочлена $f(x)$ в цьому кільці. Маємо:

$$f(x) = x^6 - x^5 - 2x^4 - 16x^2 + 16x + 32 = x^4(x^2-x-2) - 16(x^2-x-2) = \\ = (x^2-x-2)(x^4-16) = (x-2)^2(x+1)(x+2)(x^2+4).$$

За теоремою про знаходження найбільшого спільного дільника многочленів, розкладених на незвідні множники, маємо:

$$(f,g) \sim (x-2)^2(x+1)(x+2).$$

Розв'язання в Maple. Знайдемо спочатку канонічні розклади многочленів $f(x)$ і $g(x)$, позначимо їх через f1 і g1 відповідно:

```
> f:=x^6-x^5-2*x^4-16*x^2+16*x+32:
  g:=(x+1)^2*(x^2-4)*(x-2)^2:
  f1:=factor(f);
  g1:=factor(g);
```

$$f1 := (x+2)\,(x+1)\,(x^2+4)\,(x-2)^2$$

$$g1 := (x+1)^2\,(x-2)^3\,(x+2)$$

Тепер знайдемо НСД многочленів f1 і f2:

```
> gcd(f1,g1);
```

$$(x+2)\,(x+1)\,(x-2)^2$$

Зауваження. Якщо команду **gcd** застосувати безпосередньо до заданих многочленів, а не до їхніх розкладів $f1$ і $f2$, то результат (НСД цих многочленів) не обов'язково буде записано в канонічному розкладі, що може викликати хибне припущення про те, що одержана відповідь не є правильною. Наприклад,

```
> gcd(f,g);
```

$$(x+1)\,(-4+x^2)\,(x-2)$$

Безпосередня перевірка (розклад на множники за допомогою команди factor) показує, що одержана відповідь правильна:

```
> factor((x+1)*(-4+x^2)*(x-2));
```

$$(x+2)\,(x+1)\,(x-2)^2$$

Завдання 39. Знайти найбільший спільний дільник многочленів $f(x)$ і $g(x)$, використовуючи: а) алгоритм Евкліда,
б) канонічний розклад многочленів $f(x)$ і $g(x)$.

39.1. а) $f(x) = x^4 - 9x^3 + 25x^2 - 24x + 16$,
$g(x) = 2x^3 - x^2 + x + 1$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = x^7 - x^3$,
$g(x) = (x + \overline{2})^2(\overline{2}x + \overline{3})$ в кільці $\mathbb{Z}_5[x]$.

39.2. а) $f(x) = x^4 - 4x^3 + 4x^2 - 5x - 2$,
$g(x) = x^2 - x + 2$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x+1)^2(x^2+1)(x^2+5x+6)^2$,
$g(x) = (x^2 + 3x - 10)(x^2 - 1)$ в кільці $\mathbb{Z}[x]$.

39.3. а) $f(x) = x^5 + 7x^4 + 13x^3 - x^2 - 7x - 13$,
$g(x) = x^4 + 8x^3 + 23x^2 + 34x + 39$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x-2)^2(x^2-1)(x^2+1)$,
$g(x) = (x+i)^2(x-1)$ в кільці $\mathbb{C}[x]$.

39.4. а) $f(x) = \overline{2}x^4 + x^3 + x^2 + x - \overline{1}$,
$g(x) = \overline{2}x^4 + x^3 - x^2 - \overline{1}$ в кільці $\mathbb{Z}_5[x]$;
б) $f(x) = (x^2 - 4x + 5)^2(x^2 - 4x + 3)^2$,
$g(x) = (x^3 - 1)^2(x^2 - 7x + 12)$ в кільці $\mathbb{Q}[x]$.

39.5. а) $f(x) = x^3 + (3+i)x^2 + (4i-1)x - i - 1$,
$g(x) = x^3 + (3+i)x^2 + (2i-1)x - i + 1$ в кільці $\mathbb{C}[x]$;
б) $f(x) = x^{15} - 1$,
$g(x) = x^9 - 1$ в кільці $\mathbb{Q}[x]$.

39.6. а) $f(x) = x^3 - x^2 + 5x - 5$,
$g(x) = x^4 + 2x^3 + 2x - 1$ в кільці $\mathbb{R}[x]$;
б) $f(x) = (x^2 + x + \overline{1})(x^3 - \overline{2})$,
$g(x) = (x + \overline{2})^3(x + \overline{1})$ в кільці $\mathbb{Z}_3[x]$.

39.7. а) $f(x) = x^4 + x^3 + 3x^2 + x + 2$,
$g(x) = x^4 + x^3 + 4x^2 + x + 3$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 - 1)(x - 2)^3(x^2 - 4x + 3)$,
$g(x) = (x^2 - 5x + 6)(x^2 + 1)$ в кільці $\mathbb{Z}[x]$.

39.8. а) $f(x) = x^5 + x^4 - 6x^3 - x^2 - x + 6$,
$g(x) = x^4 + 2x^3 - 4x^2 - 5x - 6$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + 4)^2(x^2 - 3x + 2)$,
$g(x) = (x - 2i)^2(x - i)^3$ в кільці $\mathbb{C}[x]$.

39.9. а) $f(x) = x^5 - \overline{3}x^4 + \overline{2}x^3 + \overline{4}x^2 + x + \overline{2}$,
$g(x) = \overline{2}x^4 + \overline{3}x^3 + \overline{4}x^2 + \overline{4}x + \overline{3}$ в кільці $\mathbb{Z}_5[x]$;
б) $f(x) = (x + 4)(x^3 + 1)^2(x^2 - 9)^2$,
$g(x) = (x^2 + x - 12)^2(x + 1)^2$ в кільці $\mathbb{Q}[x]$.

39.10. а) $f(x) = x^3 + (1 - 2i)x^2 + 3ix - 2$,
$g(x) = x^3 - ix^2 + 3x - 2i$ в кільці $\mathbb{C}[x]$;
б) $f(x) = x^4 - 2x^3 - 3x^2 + 8x - 4$,
$g(x) = (x - 1)(x^2 - 3x + 2)$ в кільці $\mathbb{Q}[x]$.

39.11. а) $f(x) = 3x^5 + 5x^4 - 16x^3 - 65x^2 - 5x - 6$,
$g(x) = 3x^4 - 4x^3 - x^2 - x - 2$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = x^{10} - x^7$,
$g(x) = (x^2 + x + \overline{1})^2(x^2 + \overline{1})$ в кільці $\mathbb{Z}_5[x]$.

39.12. а) $f(x) = x^4 - x^3 + x - 1$,
$g(x) = x^4 - x^3 + 3x^2 - 2x + 2$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + 4)(x^2 - 4)(x^2 - 5x + 6)^2$,
$g(x) = (x^2 - 3x + 2)(x^2 - 1)$ в кільці $\mathbb{Z}[x]$.

39.13. а) $f(x) = x^4 - 6x^3 + x^2 + 24x + 16$,
$g(x) = x^5 - 8x^4 + 16x^3 + x^2 - 8x + 16$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + x - \overline{2})(x - \overline{3})^2$,
$g(x) = x^5 - x$ в кільці $\mathbb{Z}_5[x]$.

39.14. а) $f(x) = x^5 - \overline{6}x^4 + \overline{2}x^3 + \overline{2}x^2 + x + \overline{2}$,
$g(x) = \overline{3}x^5 + \overline{4}x^4 - \overline{4}x^3 + \overline{2}x^2 + \overline{4}x + \overline{1}$ в кільці $\mathbb{Z}_7[x]$;
б) $f(x) = (x + 2)(x^3 - 1)^2(x^2 + 2x - 3)^2$,
$g(x) = (x - 1)(x^2 + 5x + 6)^2$ в кільці $\mathbb{Q}[x]$.

39.15. а) $f(x) = x^4 + ix^3 + x + 1$,
$g(x) = x^5 + (1 - i)x^4 - ix^3 - x^2 + 1$ в кільці $\mathbb{C}[x]$;
б) $f(x) = x^3 - 2x^2 - x + 2$,
$g(x) = (x^2 - 5x + 6)(x^2 - 4)$ в кільці $\mathbb{Q}[x]$.

39.16. а) $f(x) = x^5 + 3x^2 - x + 3$,
$g(x) = x^4 - x^3 + 5x^2 - x + 4$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + \overline{2})^2(x^2 + \overline{4})(\overline{2}x - \overline{1})$,
$g(x) = x^{13} - x^9$ в кільці $\mathbb{Z}_5[x]$.

39.17. а) $f(x) = 2x^3 - 3x^2 + 3x - 1$,
$g(x) = 2x^4 - x^3 + 10x^2 - 7x + 1$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + 4)^2(x^2 - 1)(x^2 - 5x + 6)^3$,
$g(x) = (x^2 - 4)^2(x^2 + 6)$ в кільці $\mathbb{C}[x]$.

39.18. а) $f(x) = 2x^3 + 3x^2 - x - 1$,
$g(x) = x^5 + x^4 + 4x^3 + 4x^2 - 6x + 1$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^3 - 8)^2(x^2 - 2x + 1)$,
$g(x) = x^4 - 3x^3 + 3x^2 - 3x + 2$ в кільці $\mathbb{Q}[x]$.

39.19. а) $f(x) = -\overline{2}x^3 + x^2 - \overline{4}x - \overline{2}$,
$g(x) = x^4 + x^2 + \overline{1}$ в кільці $\mathbb{Z}_5[x]$;
б) $f(x) = (x^2 + x + 1)(x^2 - 6x - 7)(x - 2)^3$,
$g(x) = (x^2 - 9x + 14)(x^2 - 9)$ в кільці $\mathbb{Z}[x]$.

39.20. а) $f(x) = x^3 + x^2 - ix - i$,
$g(x) = x^5 - 2ix^3 + ix^2 - x + 1$ в кільці $\mathbb{C}[x]$;
б) $f(x) = x^4 - 5x^3 + 5x^2 + 5x - 6$,
$g(x) = (x+1)^2(x^2 - 2x - 3)^2$ в кільці $\mathbb{Q}[x]$.

39.21. а) $f(x) = x^4 - 4x^3 + 4x^2 - 5x - 2$,
$g(x) = x^3 + x + 2$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + \overline{2})(x - \overline{1})^2$,
$g(x) = (x^2 + x + \overline{1})^2$ в кільці $\mathbb{Z}_3[x]$.

39.22. а) $f(x) = x^4 + 2x^2 + 1$,
$g(x) = x^5 - x^3 + 2x^2 - 2x + 2$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 + 9)^2(x^2 - 4)(x - 2)^2$,
$g(x) = (x^2 + 3x + 2)^2(x - 3i)$ в кільці $\mathbb{C}[x]$.

39.23. а) $f(x) = x^4 + 7x^3 + 19x^2 + 23x + 10$,
$g(x) = x^4 + 7x^3 + 18x^2 + 22x + 12$ в кільці $\mathbb{Q}[x]$;
б) $f(x) = (x^2 - 9)(x^2 - x + 1)(x^2 - 2x - 3)^2$,
$g(x) = (x^2 - 7x + 10)^2(x^2 + x + 1)$ в кільці $\mathbb{Z}[x]$.

39.24. а) $f(x) = x^4 - \overline{3}x^3 - x - \overline{4}$,
$g(x) = x^4 + \overline{2}x^3 + \overline{5}x^2 - \overline{5}x - \overline{3}$ в кільці $\mathbb{Z}_7[x]$;
б) $f(x) = (x^2 - 5x + 6)^2(x^2 - 4)$,
$g(x) = (x^2 - 4x + 6)^2(x^2 - 9)$ в кільці $\mathbb{Q}[x]$.

39.25. а) $f(x) = 4x^4 + 5x^2 + 1$,
$g(x) = 16x^3 + 22ix^2 - 5x + i$ в кільці $\mathbb{C}[x]$;
б) $f(x) = x^{16} - 1$,
$g(x) = (x^7 - 1)^2$ в кільці $\mathbb{Q}[x]$.

Приклад 40.1 Знайти лінійне представлення нормованого найбільшого спільного дільника $d(x)$ многочленів

$$f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9 \quad \text{і} \quad g(x) = 2x^3 - x^2 - 5x + 4$$

над полем $\mathbb{Q}$ двома способами:

1) використовуючи алгоритм Евкліда;

2) методом невизначених коефіцієнтів.

Розв'язання. Знайти лінійне представлення найбільшого спільного дільника $d(x)$ многочленів $f(x)$ і $g(x)$ над полем P означає знайти такі многочлени $u(x)$ і $v(x)$ із $P[x]$, щоб виконувалась рівність

$$d(x) = f(x) \cdot u(x) + g(x) \cdot v(x). \tag{IV.11}$$

1) Застосуємо алгоритм Евкліда до многочленів $f(x)$ і $g(x)$. Зауважимо, що тепер вже не можна змінювати ділене і дільник (як в прикладі 39.1), оскільки неповні частки $s_1(x), s_2(x), \ldots$ використовуються при відшуканні $u(x)$ і $v(x)$. Поділимо многочлен $f(x)$ на $g(x)$:

$$\begin{array}{rl|l} f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9 & 2x^3 - x^2 - 5x + 4 & = g(x) \\ \cline{1-2} 4x^4 - 2x^3 - 10x^2 + 8x & 2x = s_1(x) & \\ \cline{1-1} -6x^2 - 3x + 9 = r_1(x) & & \end{array}$$

Далі ділимо $g(x)$ на $r_1(x)$:

$$\begin{array}{rl|l} g(x) = 2x^3 - x^2 - 5x + 4 & -6x^2 - 3x + 9 & = r_1(x) \\ \cline{1-2} 2x^3 + x^2 - 3x & -\frac{1}{3}x + \frac{1}{3} = s_2(x) & \\ \cline{1-1} -2x^2 - 2x + 4 & & \\ -2x^2 - x + 3 & & \\ \cline{1-1} -x + 1 = r_2(x) \neq 0 & & \end{array}$$

Тепер ділимо $r_1(x)$ на $r_2(x)$:

$$\begin{array}{rl|l} r_1(x) = -6x^2 - 3x + 9 & -x + 1 & = r_2(x) \\ \cline{1-2} -6x^2 + 6x & 6x + 9 = s_3(x) & \\ \cline{1-1} -9x + 9 & & \\ -9x + 9 & & \\ \cline{1-1} 0 = r_3(x) & & \end{array}$$

Отже, остання відмінна від нуля остача $r_1(x) = -x + 1$. За найбільший спільний дільник приймемо нормований многочлен $d(x) = -r_2(x) = x - 1$.

Знайдемо представлення $d(x)$ через $f(x)$ і $g(x)$. Маємо систему рівностей:

$$\begin{cases} f(x) = g(x) \cdot s_1(x) + r_1(x), \\ g(x) = r_1(x)s_2(x) + r_2(x). \end{cases}$$

Тоді

$$r_1(x) = f(x) - g(x) \cdot s_1(x), \tag{IV.12}$$
$$r_2(x) = g(x) - r_1(x) \cdot s_2(x). \tag{IV.13}$$

$$r_2(x) \overset{\text{з (IV.15)}}{=} g(x) - r_1(x)s_2(x) \overset{\text{з (IV.14)}}{=}$$
$$= g(x) - (f(x) - g(x) \cdot s_1(x))\, s_2(x) = f(x)\cdot(-s_2(x)) + g(x)\,(1 + s_1(x)s_2(x)) =$$
$$= f(x)\left(\frac{1}{3}x - \frac{1}{3}\right) + g(x)\left(1 + 2x\left(-\frac{1}{3}x + \frac{1}{3}\right)\right) =$$
$$= f(x)\left(\frac{1}{3}x - \frac{1}{3}\right) + g(x)\left(1 - \frac{2}{3}x^2 + \frac{2}{3}x\right).$$

А значить, $d(x) = -r_2(x) = f(x)\underbrace{\left(-\frac{1}{3}x + \frac{1}{3}\right)}_{u(x)} + g(x)\underbrace{\left(\frac{2}{3}x^2 - \frac{2}{3}x - 1\right)}_{v(x)}$.

2) Поділимо кожний із многочленів $f(x)$ і $g(x)$ на їхній найбільший спільний дільник $d(x) = x-1$ (див. п.1). Знайдені частки дорівнюють відповідно: $f_1(x) = 4x^3 + 2x^2 - 14x - 9$ і $g_1(x) = 2x^2 + x - 4$, причому $(f_1, g_1) \sim 1$. Для многочленів $f_1(x)$ і $g_1(x)$ використаємо теорему про лінійне представлення найбільшого спільного дільника. В нашому випадку $n = 3$, $m = 2$, $k = 0$. Отже, для многочленів $f_1(x)$ і $g_1(x)$ існують многочлени $u(x)$ і $v(x)$ із $\mathbb{Q}[x]$ такі, що:

$$f_1(x) \cdot u(x) + g_1(x) \cdot v(x) = 1,$$

де

$$\begin{cases} \deg u \leqslant 1, \\ \deg v \leqslant 2. \end{cases}$$

Нехай $\begin{cases} u(x) = ax + b, \\ v(x) = cx^2 + dx + m. \end{cases}$

Тоді лінійне представлення (f_1, g_1) матиме вигляд

$$(4x^3 + 2x^2 - 14x - 9)(ax + b) + (2x^2 + x - 4)(cx^2 + dx + m) = 1$$

або

$$(4a + 2c)x^4 + (4b + 2a + 2d + c)x^3 + (2b - 14a + 2m + d - 4c)x^2 +$$
$$+ (-9a - 14b + m - 4d)x + (-9b - 4m) = 1.$$

Прирівнявши в останній рівності коефіцієнти при однакових степенях змінної x, маємо:

$$\begin{cases} 4a + 2c = 0, \\ 4b + 2a + 2d + c = 0, \\ 2b - 14a + 2m + d - 4c = 0, \\ -9a - 14b + m - 4d = 0, \\ -9b - 4m = 1. \end{cases}$$

Розв'язавши дану систему, отримуємо: $a = -\frac{1}{3}$, $b = \frac{1}{3}$, $c = \frac{2}{3}$, $d = -\frac{2}{3}$, $m = -1$. Отже, $u(x) = -\frac{1}{3}x + \frac{1}{3}$, $v(x) = \frac{2}{3}x^2 - \frac{2}{3}x - 1$. Таким чином,

$$1 = f_1(x)\left(-\frac{1}{3}x + \frac{1}{3}\right) + g_1(x)\left(\frac{2}{3}x^2 - \frac{2}{3}x - 1\right).$$

Тоді

$$(f, g) = f(x)\left(-\frac{1}{3}x + \frac{1}{3}\right) + g(x)\left(\frac{2}{3}x^2 - \frac{2}{3}x - 1\right).$$

Розв'язання в Maple. Для знаходження лінійного представлення НСД двох многочленів $f(x)$ і $g(x)$ використовується розширена команда **gcdex(f, g, x 'u','v')**.

```
> f:=4*x^4-2*x^3-16*x^2+5*x+9:
  g:=2*x^3-x^2-5*x+4:
  gcdex(f,g,x,'u','v');
```

$$-1 + x$$

Отже, $(f, g) \sim x - 1$. Побачити многочлени $u(x)$ і $v(x)$ можна, викликавши їх:

```
> u;
```

$$\frac{1}{3} - \frac{x}{3}$$

```
> v;
```

$$-1 + \frac{2}{3}x^2 - \frac{2}{3}x$$

Для покрокової перевірки способу 2 розв'язання використаємо процедуру **mUndefCoeff** із Прикладу 34.1.

Задаємо многочлени $f(x)$ і $g(x)$:

```
> f:=4*x^4-2*x^3-16*x^2+5*x+9:
  g:=2*x^3-x^2-5*x+4;
```

Знаходимо найбільший спільний дільник цих многочленів:

```
> d:=gcd(f,g);
```

$$d := x - 1$$

Далі знаходимо многочлени $f_1(x)$ і $g_1(x)$ та їхні степені:

```
> f1:=simplify(f/d); g1:=simplify(g/d);
```

$$f1 := 4\,x^3 + 2\,x^2 - 14\,x - 9$$

$$g1 := 2\,x^2 + x - 4$$

```
> n:=degree(f1,x); m:=degree(g1,x);
```

$$n := 3$$

$$m := 2$$

Генеруємо многочлени $u(x)$ та $v(x)$ (див. Приклад 34.1):

```
> read(‘e:/atchlib.m‘);  with(atchlib):
> u:=generatePoly(m-1,a);
  v:=generatePoly(n-1,b);
```

$$u := a_0 + a_1\,x$$

$$v := b_0 + b_1\,x + b_2\,x^2$$

Застосовуємо метод невизначених коефіцієнтів до рівності $f_1u+g_1v=1$:

```
> mUndefCoeff(f1*u+g1*v,1);
```

$$\{a_0 = \frac{1}{3},\ a_1 = \frac{-1}{3},\ b_0 = -1,\ b_1 = \frac{-2}{3},\ b_2 = \frac{2}{3}\}$$

Отже, $u(x) = \frac{1}{3} - \frac{1}{3}x$, $v(x) = -1 - \frac{2}{3}x + \frac{2}{3}x^2$.

Приклад 40.2 Знайти лінійне представлення найбільшого спільного дільника $d(x)$ многочленів

$$f(x) = \overline{2}x^4 + x^3 + x^2 + x - \overline{1} \quad \text{і} \quad g(x) = \overline{2}x^4 + x^3 - x^2 - \overline{1}$$

з кільця $\mathbb{Z}_5[x]$ двома способами:

1) використовуючи алгоритм Евкліда;

2) методом невизначених коефіцієнтів.

Розв'язання. 1) Під час застосування алгоритму Евкліда до многочленів $f(x)$ і $g(x)$ в Прикладі 39.1 ділені і дільники не змінювались, випишемо рівності:

$$\begin{cases} f(x) = g(x)\cdot s_1(x) + r_1(x), \\ g(x) = r_1(x)s_2(x) + r_2(x). \end{cases}$$

лише замість остачі $r_2(x) = -\overline{2}x + \overline{4}$ було взято асоційований нормований многочлен $d(x) = x + \overline{3} = \overline{2}r_2(x)$. Знайдемо представлення $d(x)$ через $f(x)$ і $g(x)$. Маємо систему рівностей:

$$\begin{cases} f(x) = g(x) \cdot s_1(x) + r_1(x), \\ g(x) = r_1(x)s_2(x) + r_2(x). \end{cases}$$

Тоді

$$r_1(x) = f(x) - g(x) \cdot s_1(x), \tag{IV.14}$$
$$r_2(x) = g(x) - r_1(x) \cdot s_2(x). \tag{IV.15}$$

звідки

$$r_2(x) \overset{\text{з (IV.15)}}{=} g(x) - r_1(x)s_2(x) \overset{\text{з (IV.14)}}{=}$$
$$= g(x) - (f(x) - g(x) \cdot s_1(x))\, s_2(x) = f(x) \cdot (-s_2(x)) + g(x)\,(1 + s_1(x)s_2(x)) =$$
$$= f(x)\left(-x^2 - \overline{2}\right) + g(x)(\overline{1} + \overline{1} \cdot (x^2 + \overline{2}) =$$
$$= f(x)\left(\overline{4}x^2 - \overline{2}\right) + g(x)(x^2 + \overline{3}).$$

А значить,

$$d(x) = \overline{2}r_2(x) = f(x)\left(\overline{3}x^2 - \overline{4}\right) + g(x)(\overline{2}x^2 + \overline{1}) =$$
$$= f(x)\underbrace{\left(\overline{3}x^2 + \overline{1}\right)}_{u(x)} + g(x)\underbrace{\left(\overline{2}x^2 + \overline{1}\right)}_{v(x)}.$$

2) Ділимо кожний із многочленів $f(x)$ і $g(x)$ на їхній найбільший спільний дільник $d(x) = x + \overline{3}$. Знайдені частки дорівнюють відповідно: $f_1(x) = \overline{2}x^3 + x + \overline{3}$ і $g_1(x) = \overline{2}x^3 + \overline{4}x + \overline{3}$, причому $(f_1, g_1) \sim \overline{1}$. Для многочленів $f_1(x)$ і $g_1(x)$ використаємо теорему про лінійне представлення найбільшого спільного дільника. В даному випадку $n = 3$, $m = 3$, $k = 0$. Отже, для многочленів $f_1(x)$ і $g_1(x)$ існують многочлени $u(x)$ і $v(x)$ із $\mathbb{Q}[x]$ такі, що:

$$f_1(x) \cdot u(x) + g_1(x) \cdot v(x) = 1,$$

де

$$\begin{cases} \deg u \leqslant 2, \\ \deg v \leqslant 2. \end{cases}$$

Нехай $\begin{cases} u(x) = ax^2 + bx + c, \\ v(x) = mx^2 + nx + p. \end{cases}$

Тоді лінійне представлення (f_1, g_1) матиме вигляд

$$(\overline{2}x^3 + x + \overline{3})(ax^2 + bx + c) + (\overline{2}x^3 + \overline{4}x + \overline{3})(mx^2 + nx + p) = \overline{1}$$

або

$$(\overline{2}m + \overline{2}a)x^5 + (\overline{2}n + \overline{2}b)x^4 + (\overline{2}p + \overline{4}m + \overline{2}c + a)x^3 + (\overline{3}m + \overline{3}a + \overline{4}n + b)x^2 + \\ + (\overline{4}p + \overline{3}n + c + \overline{3}b)x + (\overline{3}p + \overline{3}c) = \overline{1}.$$

Прирівнюючи в останній рівності коефіцієнти при однакових степенях змінної x, маємо:

$$\begin{cases} \overline{2}m + \overline{2}a = \overline{0}, \\ \overline{2}n + \overline{2}b = \overline{0}, \\ \overline{2}p + \overline{4}m + \overline{2}c + a = \overline{0}, \\ \overline{3}m + \overline{3}a + \overline{4}n + b = \overline{0}, \\ \overline{4}p + \overline{3}n + c + \overline{3}b = \overline{0}. \\ \overline{3}p + \overline{3}c = \overline{1}. \end{cases}$$

Розв'язавши дану систему, отримаємо: $a = \overline{3}$, $b = \overline{0}$, $c = \overline{1}$, $m = \overline{2}$, $n = \overline{0}$, $p = \overline{1}$. Отже, $u(x) = \overline{3}x^2 + \overline{1}$, $v(x) = \overline{2}x^2 + \overline{1}$. Таким чином,

$$1 = f_1(x)\left(\overline{3}x^2 + \overline{1}\right) + g_1(x)\left(\overline{2}x^2 + \overline{1}\right).$$

Тоді і

$$(f, g) = f(x)\left(\overline{3}x^2 + \overline{1}\right) + g(x)\left(\overline{2}x^2 + \overline{1}\right).$$

Розв'язання в Maple. Для пошуку лінійного представлення НСД многочленів $f(x)$ і $g(x)$, заданих над полем $\mathbb{Z}_m$, використовується аналогічна команда **Gcdex(f, g, x 'u','v') mod m**.

```
> f:=2*x^4+x^3+x^2+x-1 mod 5:
  g:=2*x^4+x^3-x^2-1 mod 5:
  Gcdex(f,g,x,'u','v') mod 5;
```

$$x + 3$$

```
> u;v;
```

$$3\,x^2 + 1$$
$$2\,x^2 + 1$$

Завдання 40. Знайти лінійне представлення найбільшого спільного дільника многочленів $f(x)$ і $g(x)$ двома способами:

1) використовуючи алгоритм Евкліда;

2) методом невизначених коефіцієнтів, якщо:

40.1. $f(x) = x^5 - \overline{2}x^3 + \overline{2}x^2 - \overline{2}x + \overline{2}$,
$g(x) = x^3 - \overline{3}x + \overline{2}$ в кільці $\mathbb{Z}_5[x]$.

40.2. $f(x) = x^3 - 4x^2 - 4x - 5$,
$g(x) = x^3 - 6x^2 - 6x - 7$ в кільці $\mathbb{Q}[x]$.

40.3. $f(x) = 3x^5 - 2x^4 - 2x^3 + 4x^2 - x - 2$,
$g(x) = x^4 - x^3 + x - 12$ в кільці $\mathbb{Q}[x]$.

40.4. $f(x) = x^5 + (2i - 4)x^4 - 8ix^3 + x + 2i$,
$g(x) = x^4 + (2i - 3)x^3 - 6ix^2 + x + 2i$ в кільці $\mathbb{C}[x]$.

40.5. $f(x) = x^5 - \overline{2}x^3 + \overline{2}x^2 - \overline{2}x + \overline{2}$,
$g(x) = x^3 - \overline{3}x + \overline{2}$ в кільці $\mathbb{Z}_7[x]$.

40.6. $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$,
$g(x) = x^4 - 3x^3 + 4x^2 - 3x + 3$ в кільці $\mathbb{Q}[x]$.

40.7. $f(x) = 3x^5 - 2x^4 - 13x^3 + 8x^2 + 7x + 1$,
$g(x) = 3x^3 - 2x^2 + 2x + 1$ в кільці $\mathbb{Q}[x]$.

40.8. $f(x) = \overline{2}x^5 - \overline{3}x^2 - \overline{3}x + \overline{2}$,
$g(x) = \overline{2}x^4 + \overline{3}x^3 - \overline{2}x - \overline{1}$ в кільці $\mathbb{Z}_5[x]$.

40.9. $f(x) = 6x^4 - (3i + 4)x^3 + (2i + 2)x^2 + (4 - i)x - 2i$,
$g(x) = 2x^3 - (i + 2)x^2 + (2 + i)x - i$ в кільці $\mathbb{C}[x]$.

40.10. $f(x) = x^3 + x + 1$,
$g(x) = x^4 - x^3 + x - 3$ в кільці $\mathbb{Q}[x]$.

40.11. $f(x) = x^3 - 2x^2 + 2x - 1$,
$g(x) = x^3 - 8x^2 + 8x - 7$ в кільці $\mathbb{Q}[x]$.

40.12. $f(x) = 3x^5 + x^4 + 2x^3 + x^2 + 3x + 2$,
$g(x) = x^4 + x^2 + 1$ в кільці $\mathbb{Q}[x]$.

40.13. $f(x) = \overline{2}x^2 + \overline{3}$,
$g(x) = x^4 + \overline{2}x^3 - \overline{3}x^2 + x + 1$ в кільці $\mathbb{Z}_5[x]$.

40.14. $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$,
$g(x) = 2x^3 + 4x^2 + 6x$ в кільці $\mathbb{R}[x]$.

40.15. $f(x) = x^6 - 6x^5 + 7x^4 + 18x^3 - 43x^2 + 19x + 6$,
$g(x) = x^4 - 6x^3 + 12x^2 - 11x + 6$ в кільці $\mathbb{Q}[x]$.

40.16. $f(x) = x^5 - (i+1)x^4 + ix^3 + x^2 - (i+3)x + 3i$,
$g(x) = x^4 - ix^3 + x^2 + (1-i)x - i$ в кільці $\mathbb{C}[x]$.

40.17. $f(x) = 3x^5 - 2x^4 + 7x^3 - 2x^2 + 2x + 4$,
$g(x) = x^4 - x^3 + 3x^2 - 2x + 2$ в кільці $\mathbb{Q}[x]$.

40.18. $f(x) = \overline{3}x^6 + \overline{3}x^4 - \overline{2}x^3 + \overline{3}x^2 - x + \overline{3}$,
$g(x) = \overline{3}x^5 + \overline{2}x^4 + \overline{3}x - \overline{3}$ в кільці $\mathbb{Z}_5[x]$.

40.19. $f(x) = x^4 - ix^3 + x^2 - (i-1)x - i$,
$g(x) = 2x^4 + x^3 + (6i+2)x^2 + 3ix + 6i$ в кільці $\mathbb{C}[x]$.

40.20. $f(x) = x^6 - 3x^5 - 3x^4 - 4x^3 + x^2 + x + 1$,
$g(x) = x^5 - 2x^4 - 2x^3 - 2x^2 + x + 1$ в кільці $\mathbb{Q}[x]$.

40.21. $f(x) = x^4 + (i-1)x^3 + (2-i)x^2 - (i-1)x + 1$,
$g(x) = x^4 + (i+3)x^3 + (3i+3)x^2 + (3+2i)x + 2$ в кільці $\mathbb{C}[x]$.

40.22. $f(x) = x^4 - 6x^3 + 9x^2 + 4x - 12$,
$g(x) = x^4 - 2x^3 - 7x^2 + 8x + 12$ в кільці $\mathbb{Q}[x]$.

40.23. $f(x) = \overline{4}x^5 - x^4 + x^3 - \overline{2}x^2 + x - \overline{2}$,
$g(x) = \overline{4}x^4 + \overline{2}x^2 - x + \overline{1}$ в кільці $\mathbb{Z}_5[x]$.

40.24. $f(x) = x^3 - 5x^2 + x - 5$,
$g(x) = x^3 + x^2 + x + 1$ в кільці $\mathbb{Q}[x]$.

40.25. $f(x) = x^3 - 2x^2 + 2x - 1$,
$g(x) = x^4 - 4x^3 + 7x^2 - 6x + 3$ в кільці $\mathbb{R}[x]$.

Приклад 41.1. Знайти найменше спільне кратне многочленів:
а) $f(x) = x^4 - 2x^3 + x - 2$ і $g(x) = 2x^3 - 2x^2 - 8$ з кільця $\mathbb{Q}[x]$;
б) $f(x) = \overline{2}x^4 + x^3 + x^2 + x - \overline{1}$ і $g(x) = \overline{2}x^4 + x^3 - x^2 - \overline{1}$ з кільця $\mathbb{Z}_5[x]$.

Розв'язання. Для відшукання найменшого спільного кратного даних многочленів використаємо формулу:

$$[f, g] \sim \frac{f(x) \cdot g(x)}{(f, g)}.$$

а) В прикладі 39.1 було показано, що $(f, g) \sim d(x)$, де $d(x) = x - 2$, тому

$$[f, g] \sim \frac{(x^4 - 2x^3 + x - 2)(2x^3 - 2x^2 - 8)}{x - 2} = \frac{(x - 2)(x^3 + 1)(2x^3 - 2x^2 - 8)}{x - 2} =$$
$$= (x^3 + 1)(2x^3 - 2x^2 - 8) = 2x^6 - 2x^5 - 6x^3 - 2x^2 - 8.$$

Відповідним нормованим НСК многочленів $f(x)$ і $g(x)$ є многочлен

$$m(x) = x^6 - x^5 - x^3 - x^2 - 4.$$

б) НСД многочленів $f(x)$ і $g(x)$ було знайдено в Прикладі 39.1: $(f, g) \sim x + \overline{3}$, тому

$$[f, g] \sim \frac{(\overline{2}x^4 + x^3 + x^2 + x - \overline{1})(\overline{2}x^4 + x^3 - x^2 - \overline{1})}{x + \overline{3}} =$$

$$= \frac{(x + \overline{3})(\overline{2}x^3 + x + \overline{3})(\overline{2}x^4 + x^3 - x^2 - \overline{1})}{x + \overline{3}} = (\overline{2}x^3 + x + \overline{3})(\overline{2}x^4 + x^3 - x^2 - \overline{1}) =$$
$$= \overline{4}x^7 + \overline{2}x^6 + \overline{2}x^4 + \overline{2}x^2 + \overline{4}x + \overline{2}.$$

Нормованим НСК многочленів $f(x)$ і $g(x)$ є многочлен

$$m(x) = x^7 + \overline{2} \cdot \overline{4}^{-1} x^6 + \overline{2} \cdot \overline{4}^{-1} x^4 + \overline{2} \cdot \overline{4}^{-1} x^2 + x + \overline{2} \cdot \overline{4}^{-1} = x^7 + \overline{3}x^6 + \overline{3}x^4 + \overline{3}x^2 + x + \overline{3}.$$

Розв'язання в Maple. Для знаходження НСК двох многочленів $f(x)$ і $g(x)$ використовується команда **lcm(f,g)** або (у випадку скінченного поля) **Lcm(f, g) mod m**.

а) Маємо:

```
> f:=x^4-2*x^3+x-2:g:=2*x^3-2*x^2-8:
  lcm(f,g);
```

$$(x^3+1)\,(2\,x^3-2\,x^2-8)$$

Знайдемо стандартний вигляд одержаного многочлена, розкривши дужки в останній рівності:

```
> expand(%);
```

$$2\,x^6-2\,x^5-6\,x^3-2\,x^2-8$$

Отже, $[f,g]\sim 2x^6-2x^5-6x^3-2x^2-8$.

б)

```
> f:=2*x^4+x^3+x^2+x-1 mod 5:
  g:=2*x^4+x^3-x^2-1 mod 5:
> Lcm(f,g) mod 5;
```

$$\overline{3}+x+\overline{3}\,x^2+\overline{3}\,x^4+\overline{3}\,x^6+x^7$$

Отже, $[f,g]\sim x^7+\overline{3}x^6+\overline{3}x^4+\overline{3}x^2+x+\overline{3}$.

Приклад 41.2. Знайти найменше спільне кратне многочленів

$$f(x)=x^6-x^5-2x^4-16x^2+16x+32$$

і

$$g(x)=(x+1)^2(x^2-4)(x-2)^2$$

з кільця $\mathbb{Q}[x]$.

Розв'язання. Як було показано при розв'язанні Прикладу 39.2, многочлени $f(x)$ і $g(x)$ в кільці $\mathbb{Q}[x]$ мають канонічні розклади:

$$\begin{aligned} f(x) &= (x-2)^2(x+1)(x+2)(x^2+4),\\ g(x) &= (x-2)^3(x+1)^2(x+2). \end{aligned}$$

За теоремою про знаходження найменшого спільного кратного многочленів, розкладених на незвідні множники, маємо:

$$[f,g]\sim (x-2)^3(x+1)^2(x+2)(x^2+4).$$

Розв'язання в Maple. Застосуємо той самий підхід, що й при розв'язуванні Прикладу 39.2.

```
> f:=x^6-x^5-2*x^4-16*x^2+16*x+32;
```

$$f:=x^6-x^5-2\,x^4-16\,x^2+16\,x+32$$

```
> g:=(x+1)^2*(x^2-4)*(x-2)^2;
```

$$g:=(x+1)^2\,(x^2-4)\,(x-2)^2$$

```
> f1:=factor(f); g1:=factor(g);
```

$$f1 := (x+2)\,(x+1)\,(x^2+4)\,(x-2)^2$$

$$g1 := (x+1)^2\,(x-2)^3\,(x+2)$$

```
> lcm(f1,g1);
```

$$(x^2+4)\,(x+1)^2\,(x-2)^3\,(x+2)$$

Завдання 41. Знайти найменше спільне кратне многочленів $f(x)$ і $g(x)$ із завдання 39.

5. Формальна алгебраїчна похідна многочлена. Кратні корені. Відокремлення кратних множників многочлена

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ – деякий многочлен над полем P.

Похідною многочлена $f(x)$ називають многочлен

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1.$$

Вважають, що похідна многочлена нульового степеня і нуль-многочлена дорівнює нулю (нульовому многочлену). Якщо поле P має характеристику 0, то для кожного многочлена $f(x)$ з кільця $P[x]$ такого, що $\deg f \geqslant 1$, виконується рівність $\deg f' = \deg f - 1$.

Елемент a поля P називають коренем многочлена $f(x)$ з кільця $P[x]$, якщо $f(a) = 0$.

Теорема. *Для того, щоб елемент a поля P був коренем многочлена $f(x)$ з кільця $P[x]$ необхідно і достатньо, щоб $f(x)$ ділився на $x - a$.*

Розглядають також другу, третю, ..., k-у похідні від многочлена $f(x)$, відповідно позначаючи їх $f''(x), f'''(x), \ldots, f^{(k)}(x)$; при цьому $f^{(k)}(x)$ визначають як похідну від $f^{(k-1)}(x)$.

Елемент a називається коренем k-ї кратності многочлена $f(x)$ з кільця $P[x]$, якщо $f(x)$ ділиться на $(x-a)^k$ і не ділиться на $(x-a)^{k+1}$. Корені кратності 1 називають простими, а корені, кратність яких більша 1, – кратними.

Теорема (критерій кореня k-ї кратності)**.** *Для того, щоб елемент a поля P характеристики 0 був коренем кратності k для многочлена $f(x)$ з кільця $P[x]$, необхідно і достатньо, щоб*

$$f(a) = f'(a) = \ldots = f^{(k-1)}(a) = 0 \text{ і } f^{(k)}(a) \neq 0,$$

де $f^{(i)}(x)$ – i-а похідна многочлена $f(x)$.

Теорема (про степінь незвідного множника в канонічному розкладі многочлена)**.** *Якщо незвідний над полем P характеристики 0 множник $p(x)$ входить до канонічного розкладу многочлена $f(x)$ в степені $k \geqslant 2$, то він входить до канонічного розкладу похідної $f'(x)$ в степені $k-1$. Якщо незвідний множник $p(x)$ входить до канонічного розкладу многочлена $f(x)$ в 1-му степені, то він не входить до канонічного розкладу похідної $f'(x)$.*

Наслідок. *Многочлен $f(x)$ не має кратних множників тоді і лише тоді, коли $(f, f') = 1$.*

Позначимо через $\varphi_1(x)$ добуток всіх незвідних множників першої кратності многочлена $f(x)$, через $\varphi_2(x)$ – добуток всіх незвідних множників 2-ої кратності і т.д. Тоді

$$f(x) = \varphi_1(x)[\varphi_2(x)]^2 \dots [\varphi_m(x)]^m$$

або

$$f(x) = \varphi_1\varphi_2^2\varphi_3^3 \dots \varphi_m^m. \tag{IV.16}$$

Якщо многочлен не має множників кратності $k < m$, то вважають, що $\varphi_k = 1$. Запис многочлена у вигляді (IV.16) називається відокремленням кратних множників.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 42.1. Знайти кратність кореня $c = -1$ многочлена

$$f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$$

з кільця $\mathbb{Q}[x]$ двома способами:

1) за схемою Горнера;

2) використовуючи критерій кратності кореня.

Розв'язання. 1) Поділимо $f(x)$ послідовно на $x+1$, використовуючи схему Горнера (приклади 37.1, 37.2).

	1	**0**	**−6**	**−4**	**9**	**12**	**4**
−1	1	−1	−5	1	8	4	$\boxed{0}$
−1	1	−2	−3	4	4	$\boxed{0}$	
−1	1	−3	0	4	$\boxed{0}$		
−1	1	−4	4	$\boxed{0}$			
−1	1	−5	$\boxed{9}$				

Як бачимо, многочлен $f(x)$ ділиться на $(x+1)^4$, але не ділиться на $(x+1)^5$. Отже, кратність кореня $c = -1$ дорівнює 4.

2) Перевіримо, чи є $c = -1$ коренем многочлена $f(x)$. Оскільки $f(-1) = 0$, то $c = -1$ є коренем.

Знайдемо послідовно похідні многочлена $f(x)$ і їхні значення при $x = -1$ (перше відмінне від нуля із знайдених значень вказуватиме на кратність кореня):

$$\begin{array}{ll} f'(x) = 6x^5 - 24x^3 - 12x^2 + 18x + 12, & f'(-1) = 0; \\ f''(x) = 30x^4 - 72x^2 - 24x + 18, & f''(-1) = 0; \\ f'''(x) = 120x^3 - 144x - 24, & f'''(-1) = 0; \\ f^{IV}(x) = 360x^2 - 144, & f^{IV}(-1) = 216 \neq 0. \end{array}$$

Отже, $c = -1$ – корінь многочлена $f(x)$ кратності 4.

Зауваження. Вимога "P – поле характеристики 0" в умові критерію кореня k-ої кратності є суттєвою. Для полів P скінченної характеристики p критерій можна без застережень застосовувати лише до многочленів, степінь яких $< p$.

Розробка процедур. Створимо процедуру **rootMult(f,c)** для відшукання кратності заданого кореня c многочлена $f(x)$ з числовими коефіцієнтами, алгоритм якої базуватиметься на означенні кратного кореня. В ході процедури знаходимо максимальний показник степеня k такий, що многочлен $f(x)$ ділиться на $(x - c)^k$ (для цього ділимо многочлен $f(x)$ на $(x - c)^k$, $k = 0, 1, 2, ...$, доки це можливо, тобто доти, доки остача дорівнюватиме нулю: `rem(f,(x-c)^k,x)=0`):

```
rootMult:=proc(f,c)
local k;
   k:=0;
   while rem(f,(x-c)^k,x)=0 do k:=k+1; end do;
   return(k-1);
end proc:
```

Зокрема, якщо в результаті отримуємо 0, то це означає, що c не є коренем многочлена $f(x)$.

Розв'язання в Maple. Спосіб I. Застосуємо створену процедуру **rootMult** до заданого многочлена:

```
> read('e:/atchlib.m'); with(atchlib):
> f:=x^6-6*x^4-4*x^3+9*x^2+12*x+4:
  rootMult(f,-1);
```

4

Отже, число -1 є коренем кратності 4 многочлена $f(x)$.

Спосіб II.Найпростіший метод знаходження кратності кореня в Maple – використання команди **roots**. Дана команда для алгебраїчних полів має формат **roots(f,x,P)**, де **f(x)** – заданий многочлен, **P** (необов'язковий параметр) – поле, в якому шукають корені многочлена $f(x)$. В результаті застосування команди отримуємо набір [[c1, k1], ..., [cn, kn]] пар виду [ci, ki], де ci – корінь кратності ki многочлена $f(x)$. За відсутності параметра **P** здійснюється пошук коренів в полі, до якого належать коефіцієнти многочлена. Наприклад, якщо всі коефіцієнти є раціональними числами, то виводяться лише раціональні корені.

Маємо:

```
> f:=x^6-6*x^4-4*x^3+9*x^2+12*x+4:
> roots(f);
```

$$[[2,\ 2],\ [-1,\ 4]]$$

Заданий многочлен має корені: $c_1 = 2$ кратності 2 і $c_2 = -1$ кратності 4.

Приклад 42.2. Знайти кратність кореня $c = \overline{6}$ многочлена

$$f(x) = x^6 - \overline{6}x^4 - \overline{4}x^3 + \overline{2}x^2 + \overline{5}x + \overline{4}$$

з кільця $\mathbb{Z}_7[x]$.

Розв'язання. Ділимо $f(x)$ послідовно на $x - \overline{6}$, використовуючи схему Горнера.

	$\overline{1}$	$\overline{0}$	$-\overline{6}$	$-\overline{4}$	$\overline{2}$	$\overline{5}$	$\overline{4}$
$\overline{\mathbf{6}}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{1}$	$\overline{1}$	$\overline{4}$	$\boxed{\overline{0}}$
$\overline{\mathbf{6}}$	$\overline{1}$	$\overline{5}$	$\overline{4}$	$\overline{4}$	$\overline{4}$	$\boxed{\overline{0}}$	
$\overline{\mathbf{6}}$	$\overline{1}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\boxed{\overline{0}}$		
$\overline{\mathbf{6}}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\boxed{\overline{0}}$			
$\overline{\mathbf{6}}$	$\overline{1}$	$\overline{2}$	$\boxed{\overline{2}}$				

Як бачимо, многочлен $f(x)$ ділиться на $(x - \overline{6})^4$, але не ділиться на $(x - \overline{6})^5$. Отже, кратність кореня $c = \overline{6}$ дорівнює 4.

Розробка процедур. Трохи модифікуємо процедуру **rootmult**, створену при розв'язуванні попереднього прикладу, замінивши команду **rem** на її модулярний аналог **Rem**. Нова процедура **RootMult** вже буде мати 3 параметри.

```
RootMult:=proc(f,c,m)
local k;
   k:=0;
   while Rem(f,(x-c)^k,x) mod m =0 do k:=k+1; end do;
   return(k-1);
end proc:
```

Розв'язання в Maple. Застосовуємо створену процедуру:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> f:=x^6-6*x^4-4*x^3+2*x^2+5*x+4 mod 7:
> RootMult(f,6,7);
```

4

Або в інший спосіб: використовуємо команду **roots** у форматі **Roots(f, P) mod m**.

```
> f:=x^6-6*x^4-4*x^3+2*x^2+5*x+4 mod 7:
> Roots(f) mod 7;
```

[[2, 2], [6, 4]]

Кратність кореня $c = \overline{6}$ многочлена $f(x)$ дорівнює 4.

Завдання 42. Знайти кратність кореня c многочлена $f(x)$ двома способами (якщо це можливо, див. зауваження на С.318):

1) за схемою Горнера;

2) використовуючи критерій кратності кореня, якщо:

42.1. $f(x) = x^5 - x^4 - 25x^3 + 94x^2 - 124x + 56$ з кільця $\mathbb{Q}[x]$, $c = 2$.

42.2. $f(x) = x^7 - 4x^6 + 8x^5 - 11x^4 + 9x^3 - 2x^2 - 2x + 1$ з кільця $\mathbb{Q}[x]$, $c = 1$.

42.3. $f(x) = x^4 + (i-3)x^3 + (3-3i)x^2 + (3i-1)x - i$ з кільця $\mathbb{C}[x]$, $c = -i$.

42.4. $f(x) = x^5 - \overline{2}x^4 + \overline{3}x^2 + \overline{3}x + \overline{3}$ з кільця $\mathbb{Z}_5[x]$, $c = \overline{3}$.

42.5. $f(x) = x^5 - 11x^4 + 42x^3 - 54x^2 - 27x + 81$ з кільця $\mathbb{Q}[x]$, $c = 3$.

42.6. $f(x) = -x^4 + 9x^3 - 23x^2 + 8x + 16$ з кільця $\mathbb{Q}[x]$, $c = 4$.

42.7. $f(x) = x^7 + \overline{4}x^5 + x^3 + \overline{4}x^2 + x + \overline{1}$ з кільця $\mathbb{Z}_7[x]$,
$c = \overline{6}$.

42.8. $f(x) = x^4 - (4+2i)x^3 + (5+6i)x^2 - (2+6i)x + 2i$ з кільця $\mathbb{C}[x]$,
$c = 1+i$.

42.9. $f(x) = x^5 + 2x^4 + 2x^3 + 3x^2 + 3x + 1$ з кільця $\mathbb{Q}[x]$,
$c = -1$.

42.10. $f(x) = x^5 - 9x^4 + 32x^3 - 56x^2 + 48x - 16$ з кільця $\mathbb{Q}[x]$,
$c = 2$.

42.11. $f(x) = x^7 + x^6 + \overline{2}x^5 + x^4 + \overline{2}x^3 + \overline{2}x^2 + x + \overline{2}$ з кільця $\mathbb{Z}_5[x]$,
$c = \overline{2}$.

42.12. $f(x) = x^4 - (4i+2)x^3 + (6i-5)x^2 + (6+2i)x - 2i$ з кільця $\mathbb{C}[x]$,
$c = i$.

42.13. $f(x) = x^5 + 9x^4 + 32x^3 + 56x^2 + 48x + 16$ з кільця $\mathbb{Q}[x]$,
$c = -2$.

42.14. $f(x) = -x^5 - 2x^4 - x^3 + x^2 + 2x + 1$ з кільця $\mathbb{Q}[x]$,
$c = -1$.

42.15. $f(x) = x^6 - 6ix^5 - 15x^4 + 20ix^3 + 15x^2 - 6ix - 1$ з кільця $\mathbb{C}[x]$,
$c = i$.

42.16. $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + \overline{1}$ з кільця $\mathbb{Z}_3[x]$,
$c = \overline{1}$.

42.17. $f(x) = x^4 + 3x^3 + 2x^2 + x + 2$ з кільця $\mathbb{Q}[x]$,
$c = -2$.

42.18. $f(x) = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$ з кільця $\mathbb{Q}[x]$,
$c = -1$.

42.19. $f(x) = x^5 - \overline{3}$ з кільця $\mathbb{Z}_5[x]$,
$c = \overline{3}$.

42.20. $f(x) = x^5 - ix^4 + 2x^3 - 2ix^2 + x - i$ з кільця $\mathbb{C}[x]$,
$c = i$.

42.21. $f(x) = x^7 + \overline{2}x^6 + x^5 + \overline{2}x^2 + \overline{4}x + \overline{2}$ з кільця $\mathbb{Z}_5[x]$,
$c = \overline{4}$.

42.22. $f(x) = x^5 + 7x^4 + 15x^3 + 10x^2 + 6x + 9$ з кільця $\mathbb{Q}[x]$, $c = -3$.

42.23. $f(x) = x^5 - 2x^4 + 2x^3 - 3x^2 + 3x - 1$ з кільця $\mathbb{Q}[x]$, $c = 1$.

42.24. $f(x) = x^4 - (4i + 2)x^3 + (6i - 5)x^2 + (6 + 2i)x - 2i$ з кільця $\mathbb{C}[x]$, $c = 1 + i$.

42.25. $f(x) = x^4 - 2x^3 + 2x - 1$ з кільця $\mathbb{Q}[x]$, $c = -1$.

Приклад 43.1 Відокремити кратні множники многочлена

$$f(x) = x^5 + 2ix^4 + 2x^3 + 8ix^2 - 7x - 2i.$$

Розв'язання. Відокремити кратні множники многочлена $f(x)$ означає подати його у вигляді

$$f(x) = at_1t_2^2t_3^3 \dots t_m^m, \tag{IV.17}$$

де t_i – добуток всіх незвідних множників i-ї кратності в канонічному розкладі над полем $\mathbb{C}$ при всіх i, $1 \leqslant i \leqslant m$, a – старший коефіцієнт многочлена $f(x)$.

Схематично відшукання множників можна подати наступним чином:

I етап	II етап	III етап
f	$q_1 = \frac{f}{d_1}$	
$d_1 \sim (f, f')$	$q_2 = \frac{d_1}{d_2}$	$t_1 = \frac{q_1}{q_2}$
$d_2 \sim (d_1, d_1')$	$q_3 = \frac{d_2}{d_3}$	$t_2 = \frac{q_2}{q_3}$
$d_3 \sim (d_2, d_2')$	$\dots$	$\dots$
$\dots$		
$d_{m-2} \sim (d_{m-3}, d_{m-3}')$	$q_{m-1} = \frac{d_{m-2}}{d_{m-1}}$	$t_{m-1} = \frac{q_{m-1}}{q_m}$
$d_{m-1} \sim (d_{m-2}, d_{m-2}')$	$q_m = \frac{d_{m-1}}{d_m}$	$t_m = q_m$
$d_m \sim (d_{m-1}, d_{m-1}') \sim 1$		

I. Знайдемо спочатку многочлени $d_i(x)$:

$d_1 \sim (f, f')$ – це найбільший спільний дільник многочленів $f(x)$ і $f'(x)$. Застосуємо алгоритм Евкліда (як у прикладі 39.1).

$$
\begin{array}{rl}
f(x) = & x^5 + 2ix^4 + 2x^3 + 8ix^2 - 7x - 2i \;\big|\; 5x^4 + 8ix^3 + 6x^2 + 16ix - 7 = f'(x) \\
(* \text{ на } 5) & 5x^5 + 10ix^4 + 10x^3 + 40ix^2 - 35x - 10i \;\big|\; x + 2i \\
\hline
& 5x^5 + 8ix^4 + 6x^3 + 16ix^2 - 7x \\
\hline
& 2ix^4 + 4x^3 + 24ix^2 - 28x - 10i \\
(* \text{ на } 5) & 10ix^4 + 20x^3 + 120ix^2 - 140x - 50i \\
\hline
& 10ix^4 - 16x^3 + 12ix^2 - 32x - 14i \\
\hline
& 36x^3 + 108ix^2 - 108x - 36i \\
(\div \text{ на } 36) & x^3 + 3ix^2 - 3x - i \sim r_1(x)
\end{array}
$$

$$
\begin{array}{rl}
f'(x) = 5x^4 + 8ix^3 + 6x^2 + 16ix - 7 & \big| \; x^3 + 3ix^2 - 3x - i \sim r_1(x) \\
\hline
5x^4 + 15ix^3 - 15x^2 - 5ix & \big| \; 5x - 7i \\
\hline
-7ix^3 + 21x^2 + 21ix - 7 & \\
\hline
-7ix^3 + 21x^2 + 21ix - 7 & \\
\hline
0 \sim r_2(x) &
\end{array}
$$

Таким чином, $d_1 = x^3 + 3ix^2 - 3x - i = (x + i)^3$,

$d_1' = 3x^2 + 6ix - 3 = 3(x + i)^2$.

Далі $d_2 \sim (d_1, d_1')$, тобто $d_2 = (x + i)^2$,

$d_2' = 2(x + i)$.

$d_3 \sim (d_2, d_2')$, наприклад, $d_3 = (x + i)$,

$d_3' = 1$,

тому $d_4 \sim (d_3, d_3')$, звідки $d_4 = 1$.

II. Знаходимо многочлени $q_i(x)$:

$$
\begin{aligned}
q_1 &= \frac{f}{d_1} = \frac{x^5 + 2ix^4 + 2x^3 + 8ix^2 - 7x - 2i}{x^3 + 3ix^2 - 3x - i} = x^2 - ix + 2, \\
q_2 &= \frac{d_1}{d_2} = \frac{x^3 + 3ix^2 - 3x - i}{(x + i)^2} = \frac{(x + i)^3}{(x + i)^2} = x + i, \\
q_3 &= \frac{d_2}{d_3} = \frac{(x + i)^2}{x + i} = x + i, \\
q_4 &= \frac{d_3}{d_4} = x + i.
\end{aligned}
$$

III. Тепер знаходимо множники $t_i(x)$:

$$\begin{aligned} t_1 &= \frac{q_1}{q_2} = \frac{x^2 - ix + 2}{x + i} = x - 2i, \\ t_2 &= \frac{q_2}{q_3} = \frac{x + i}{x + i} = 1, \\ t_3 &= \frac{q_3}{q_4} = \frac{x + i}{x + i} = 1, \\ t_4 &= q_4 = x + i. \end{aligned}$$

Отже, $f(x) = t_1 t_2^2 t_3^3 t_4^4 = (x - 2i)(x + i)^4$.

Розробка процедур. Для перевірки проміжних обчислень створимо процедуру **isolFactors**.

В ході процедури спочатку знаходимо многочлени $d_i(x)$ $(i = 1, 2, ..., m)$:

```
> d[1]:=gcd(f,diff(f,x));
  m:=1;
  while d[m]<>1 do
     d[m+1]:=gcd(d[m],diff(d[m],x));
     m:=m+1;
  end do;
```

В результаті виконання циклу отримуємо значення числа m (максимальної кратності множника многочлена $f(x)$.

Далі знаходимо многочлени $q_i(x)$: $q_1(x) = \frac{f(x)}{d_1(x)}$, $q_i(x) = \frac{d_{i-1}(x)}{d_i(x)}$, $i = 2, ..., m$.

```
> q[1]:=quo(f,d[1],x);
  for i from 2 to m do q[i]:=quo(d[i-1],d[i],x); end do;
```

Нарешті знаходимо множники t_i:

```
> for i from 1 to m-1 do t[i]:=quo(q[i],q[i+1],x); end do;
  t[m]:=q[m];
```

Факторизацію многочлена формуємо за допомогою циклу (при цьому необхідно ввести локальну змінну $f1$):

```
> f1:=1;
  for i from 1 to m-1 do f1:=f1*t[i]^i; end do;
```

Результати всіх проміжних дій (знайдені многочлени $d_i(x), q_i(x), t_i(x)$) виводимо на екран командою **print**. Процедура матиме наступний код:

```
isolFactors:=proc(f)
local d,m,q,i,t,f1;
   d[1]:=gcd(f,diff(f,x));
   m:=1;
   while d[m]<>1 do d[m+1]:=gcd(d[m],diff(d[m],x)); m:=m+1; end do;
   print(seq(d[i],i=1..m));
   print('m'=m);
   q[1]:=quo(f,d[1],x);
   for i from 2 to m do q[i]:=quo(d[i-1],d[i],x); end do;
   print(seq(q[i],i=1..m));
   for i from 1 to m-1 do t[i]:=quo(q[i],q[i+1],x); end do;
   t[m]:=q[m];
   print(seq(t[i],i=1..m));
   f1:=lcoeff(f);
   for i from 1 to m do f1:=f1*t[i]^i: end do:
   print(f1);
end proc:
```

Розв'язання в Maple. Для перевірки лише остаточного результату можна використати команду **sqrfree(f)**, де f – заданий многочлен. Результат [a,[[t[i],k[i],[t[j],k[j],...,[t[l],k[l]]] слід інтерпретувати як $f(x) = at_i^{k_i}t_j^{k_j}...t_l^{k_l}$ (тобто Maple ігнорує множники $t_i(x) = 1$ запису (IV.17)).

```
> f:=x^5+2*I*x^4+2*x^3+8*I*x^2-7*x-2*I:
> sqrfree(f);
```

$$[1,\ [[x - 2\,I,\ 1],\ [I + x,\ 4]]]$$

Це означає, що $f(x) = t_1t_4^4 = (x - 2i)(x + i)^4$.

Для покрокової перевірки використовуємо розроблену процедуру **isolFactors**. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);  with(atchlib):
```

Маємо:

```
> isolFactors(x^5+2*I*x^4+2*x^3+8*I*x^2-7*x-2*I);
```

$$x^3 + 3\,I\,x^2 - 3\,x - I,\ x^2 + 2\,I\,x - 1,\ x + I,\ 1$$
$$m = 4$$
$$2 + x^2 - x\,I,\ x + I,\ x + I,\ x + I$$
$$-2\,I + x,\ 1,\ 1,\ x + I$$
$$(-2\,I + x)\,(x + I)^4$$

Перший рядок отриманого результату містить послідовність многочленів $d_i(x)$, максимальна кратність множника $m = 4$, в третьому рядку наведено послідовність многочленів $q_i(x)$, а в четвертому – послідовність мно-

гочленів $t_i(x)$. В останньому рядку – результат: відокремлення кратних множників многочлена $f(x)$.

Приклад 43.2. Відокремити кратні множники многочлена: $f(x) := x^6 - x^5 - x^4 + 5x^3 - 7x^2 + 5x - 2$.

Розв'язання.

I. Знаходимо спочатку многочлени $d_i(x)$. Маємо: $d_1 \sim (f, f')$, де $f'(x) = 6x^5 - 5x^4 - x^4 + 15x^2 - 14x + 5$. За допомогою алгоритму Евкліда послідовно знаходимо: $d_1 = x^2 - x + 1$. Далі $d_1' = 2x - 1$, тоді $d_2 = 1$. Таким чином, заданий многочлен має множники лише кратності не вище $m = 2$.

II. Знаходимо многочлени $q_i(x)$:

$$\begin{aligned} q_1 &= \frac{f}{d_1} = \frac{x^6 - x^5 - x^4 + 5x^3 - 7x^2 + 5x - 2}{x^2 - x + 1} = x^4 - 2x^2 + 3x - 2, \\ q_2 &= \frac{d_1}{d_2} = \frac{x^2 - x + 1}{1} = x^2 - x + 1. \end{aligned}$$

III. Тепер знаходимо множники $t_i(x)$:

$$\begin{aligned} t_1 &= \frac{q_1}{q_2} = \frac{x^4 - 2x^2 + 3x - 2}{x^2 - x + 1} = x^2 + x - 2, \\ t_2 &= q_2 = x^2 - x + 1. \end{aligned}$$

Отже, $f(x) = t_1 t_2^2 = (x^2 + x - 2)(x^2 - x + 1)^2$.

Розв'язання в Maple. Перевірка остаточного результату:

```
> f:=x^6-x^5-x^4+5*x^3-7*x^2+5*x-2:
> sqrfree(f);
```

$$[1,\ [[x^2 + x - 2,\ 1],\ [x^2 - x + 1,\ 2]]]$$

Перевірка проміжних обчислень:

```
> isolFactors(x^6-x^5-x^4+5*x^3-7*x^2+5*x-2);
```

$$x^2 - x + 1,\ 1$$
$$m = 2$$
$$x^4 - 2\,x^2 + 3\,x - 2,\ x^2 - x + 1$$
$$x^2 + x - 2,\ x^2 - x + 1$$
$$(x^2 + x - 2)\,(x^2 - x + 1)^2$$

Завдання 43. Відокремити кратні множники многочлена

43.1. $f(x) = x^5 + 3ix^4 + 6x^3 + 10ix^2 + 21x - 9i.$

43.2. $f(x) = x^5 - x^4 - 5x^3 + x^2 + 8x + 4.$

43.3. $f(x) = x^5 + 3x^4 + 5x^3 + 5x^2 + 3x + 1.$

43.4. $f(x) = x^4 - 4(2+i)x^3 + 6(3+4i)x^2 - (8+44)ix - 7 + 24i.$

43.5. $f(x) = x^6 + 14x^5 + 80x^4 + 238x^3 + 387x^2 + 324x + 108.$

43.6. $f(x) = x^5 + 3x^4 + 7x^3 + 9x^2 + 8x + 4.$

43.7. $f(x) = x^5 - 5x^4 + (6-i)x^3 + (4+6i)x^2 - (8+12i)x + 8i.$

43.8. $f(x) = x^6 + 14ix^5 - 80x^4 - 238ix^3 + 387x^2 + 324ix - 108.$

43.9. $f(x) = x^5 - 4ix^4 - x^3 - 10ix^2 - 4x - 8i.$

43.10. $f(x) = x^6 - x^5 - x^4 + 5x^3 - 7x^2 + 5x - 2.$

43.11. $f(x) = x^6 - 14x^5 + 80x^4 - 238x^3 + 387x^2 - 324x + 108.$

43.12. $f(x) = x^5 - 4ix^4 - x^3 - 10ix^2 - 4x - 8i.$

43.13. $f(x) = x^5 + (i+2)x^4 + (3+4i)x^3 + 5ix^2 + (4i-2)x - 2.$

43.14. $f(x) = x^4 + 5x^3 + 9x^2 + 8x + 4.$

43.15. $f(x) = x^6 + (1+i)x^5 + (5+i)x^4 + (5+i)x^3 + (8+i)x^2 + 4(2-i)x - 4i.$

43.16. $f(x) = x^6 + 10x^5 + 41x^4 + 88x^3 + 104x^2 + 64x + 16.$

43.17. $f(x) = x^6 + 9x^5 + (32-i)x^4 + (56-8i)x^3 + 24(2-i)x^2 + 16(1-2i)x - 16i.$

43.18. $f(x) = x^5 - 7x^4 + 20x^3 - 32x^2 + 32x - 16.$

43.19. $f(x) = x^5 - ix^4 + 5x^3 - ix^2 + 8x + 4i.$

43.20. $f(x) = x^6 - 14ix^5 - 80x^4 + 238ix^3 + 387x^2 - 324ix - 108.$

43.21. $f(x) = x^5 - (2-9i)x^4 - (26+18i)x^3 + (54-18i)x^2 - 27(1-2i)x - 27i.$

43.22. $f(x) = x^5 - 3x^4 + 5x^3 - 5x^2 + 3x - 1.$

43.23. $f(x) = x^5 + 4x^4 + x^3 - 10x^2 - 4x + 8.$

43.24. $f(x) = x^5 + ix^4 + 2x^3 + 2ix^2 + x + i.$

43.25. $f(x) = x^4 - 3x^3 + (3-i)x^2 + (2i-1)x - i.$

Розділ V

Многочлени від багатьох змінних

1. Симетричні многочлени

ТЕОРЕТИЧНІ ВІДОМОСТІ

Многочлен $f(x_1, x_2, \ldots, x_n)$ з кільця $P[x_1, x_2, \ldots, x_n]$ називають симетричним відносно змінних $x_1, x_2, \ldots, x_n$, якщо при будь-якій підстановці змінних $x_1, x_2, \ldots, x_n$ отримуємо той самий многочлен. Симетричні многочлени

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \ldots + x_n, \\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
\sigma_n &= x_1x_2 \ldots x_n
\end{aligned}$$

називають елементарними симетричними многочленами.

Теорема. *Будь-який симетричний многочлен $f(x_1, x_2, \ldots, x_n)$ від n змінних над полем P можна подати (причому єдиним чином) у вигляді многочлена від елементарних симетричних многочленів $\sigma_1, \sigma_2, \ldots, \sigma_n$ цих змінних, коефіцієнти якого належать тому самому полю P.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 44. Виразити через елементарні симетричні многочлени многочлен

$$\begin{aligned}
f(x_1, x_2, x_3) = {} & x_1x_2(2x_1^2 - x_1x_2 + 2x_2^2) + x_1x_3(2x_1^2 - x_1x_3 + 2x_3^2) + \\
& + x_2x_3(2x_2^2 - x_2x_3 + 2x_3^2) + 5x_1^2 + 5x_2^2 + 5x_3^2 - x_1 - x_2 - x_3.
\end{aligned}$$

Розв'язання. Розкриємо дужки і запишемо даний многочлен як суму однорідних многочленів: $f(x_1, x_2, x_3) = h_4(x_1, x_2, x_3) + 5h_2(x_1, x_2, x_3) - \sigma_1$, де

$$h_4(x_1, x_2, x_3) = 2x_1^3x_2 - x_1^2x_2^2 + 2x_1x_2^3 + 2x_1^3x_3 - x_1^2x_3^2 + 2x_1x_3^3 + 2x_2^3x_3 - x_2^2x_3^2 + 2x_2x_3^3,$$

$h_2(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$
четвертого і другого степенів відповідно. Розв'яжемо дану задачу для кожного однорідного симетричного многочлена окремо.

Щоб виразити многочлен $h_4(x_1, x_2, x_3)$ через елементарні симетричні многочлени, використаємо метод невизначених коефіцієнтів. Вищим членом многочлена $h_4(x_1, x_2, x_3)$ є $2x_1^3x_2$. Складемо таблицю:

Система показників вищого члена			Вищий член	Відповідний добуток елементарних симетричних многочленів
x_1	x_2	x_3		
3	1	0	$2x_1^3x_2$	$2\sigma_1^{3-1}\sigma_2^{1-0}\sigma_3^0 = 2\sigma_1^2\sigma_2$
2	2	0	$ax_1^2x_2^2$	$a\sigma_1^{2-2}\sigma_2^{1-0}\sigma_3^0 = a\sigma_2^2$
2	1	1	$bx_1^2x_2x_3$	$b\sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^1 = b\sigma_1\sigma_3$

Отже, справедливе представлення

$$h_4(x_1, x_2, x_3) = 2\sigma_1^2\sigma_2 + a\sigma_2^2 + b\sigma_1\sigma_3,$$

де a, b – невизначені коефіцієнти. Для відшукання коефіцієнтів a і b достатньо надати змінним x_1, x_2, x_3 деяких конкретних значень. Надамо спочатку значень $x_1 = x_2 = 1$, $x_3 = 0$, а потім $x_1 = x_2 = 1$, $x_3 = -1$ і заповнимо наступну таблицю:

x_1	x_2	x_3	σ_1 $= x_1 + x_2 + x_3$	σ_2 $= x_1x_2 + x_1x_3 + x_2x_3$	σ_3 $= x_1x_2x_3$	$h_4(x_1, x_2, x_3)$ $= 2\sigma_1^2\sigma_2 + a\sigma_2^2 + b\sigma_1\sigma_3$
1	1	0	2	1	0	$3 = 8 + a$
1	1	-1	1	-1	-1	$-7 = -2 + a - b$

Маємо систему рівнянь: $\begin{cases} 3 = 8 + a, \\ -7 = -2 + a - b, \end{cases}$ розв'язками якої є $\begin{cases} a = -5, \\ b = 0. \end{cases}$ Отже, $h_4(x_1, x_2, x_3) = 2\sigma_1^2\sigma_2 - 5\sigma_2^2$.

Щоб виразити многочлен $h_2(x_1, x_2, x_3)$ через елементарні симетричні многочлени, використаємо формули скороченого множення. Оскільки

$$(x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2(x_1x_2 + x_1x_3 + x_2x_3),$$

то

$$\varphi_2(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 2\sigma_2.$$

Отже,

$$f(x_1, x_2, x_3) = h_4(x_1, x_2, x_3) + 5h_2(x_1, x_2, x_3) - \sigma_1 =$$
$$= 2\sigma_1^2\sigma_2 - 5\sigma_2^2 + 5(\sigma_1^2 - 2\sigma_2) - \sigma_1 = 2\sigma_1^2\sigma_2 + 5\sigma_1^2 - 5\sigma_2^2 - \sigma_1 - 10\sigma_2.$$

Розробка процедур. Створимо процедуру **asHomogenSum**, за допомогою якої знаходитимемо однорідні компоненти многочлена $f(x)$. В ході процедури отримуємо:

1) множину M всіх членів многочлена $f(x)$:

```
> M:={op(f)};
```

2) множину N_j всіх членів степеня j, $j \in \overline{0,n}$, де $n = \deg f$;

```
> N[j]:={}:
  for i from 1 to nops(M) do
     if degree(M[i])=j then N[j]:=N[j] union {M[i]}; end if;
  end do;
```

3) многочлен $h_j(x)$ (однорідну компоненту степеня j) як суму всіх членів степеня j.

```
> h[j]:=sum(N[j][k],k=1..nops(N[j]));
```

Код процедури наступний:

```
asHomogenSum:=proc(f)
local n,i,j,M,N;
global h;
   M:={op(f)};
   n:=degree(f);
   for j from 0 to n do
      N[j]:={}:
      for i from 1 to nops(M) do
         if degree(M[i])=j then N[j]:=N[j] union {M[i]}; end if;
      end do;
      h[j]:=sum(N[j][k],k=1..nops(N[j]));
      print(h[j],odnoridna_komponenta_stepenya=j);
   end do;
end proc:
```

Тепер створимо процедуру для пошуку представлення однорідного симетричного многочлена $f(x)$ через елементарні симетричні многочлени. Зауважимо, що обмежимось лише випадком 3-х змінних (щоб не ускладнювати викладки).

Перш за все знаходимо вищий член многочлена $f(x)$. Для цього впорядкуємо члени многочлена $f(x)$ лексикографічно:

```
> f1:=sort(f, order=plex(x1,x2,x3), descending):
```

Член, який стоїть першим зліва, є вищим членом lterm:

```
> lterm:=op(1,f1);
```

Знаходимо систему показників вищого члена $(m_!, m_2, m_3)$: m_1 – це показник степеня змінних x_1 вищого члена lterm:

```
> m1:=degree(lterm,x1):
```

Аналогічно

```
> m2:=degree(lterm,x2): m3:=degree(lterm,x3):
```

Шукаємо всі можливі набори показників (i, j, k). Для таких наборів повинні виконуватись умови:

1) показники i, j, k утворюють незростаючу послідовність: $i \geqslant j \geqslant k$;

2) сума показників однакова і дорівнює степеню многочлена $f(x)$: $i + j + k = n$;

3) важливо, що вищий член многочлена $f(x)$ (якому відповідає набір (m_1, m_2, m_3)), має бути вищим за будь-який інший знайдений вищий член, який відповідає набору (i, j, k), тобто якщо вищий член має набір показників $(m1, m2, m3)$, то для набору показників `(i,j,k)` вищого члена многочлена g (відповідного добутку елементарних симетричних многочленів) має бути справедливо: або $m_1 > i$, або $m_1 = i$, $m_2 > j$, або $m_1 = i$, $m_2 = j$, $m_3 \geqslant k$.

Використовуючи ці факти, знаходимо всі можливі системи показників. Для цього перебираємо всі набори (i, j, k), $i \in \overline{0, m_1}$, $j \in \overline{0, i}$, $k \in \overline{0, j}$, і вибираємо серед них ті, для яких виконуються умови 2) і 3). Ввівши лічильник s для кількості таких наборів, отримуємо:

```
> s:=0;
  for i from 0 to m1 do
     for j from 0 to i do
       for k from 0 to j do
         if i+j+k=degree(f) and
         (m1>i or (m1=i and m2>j) or (m1=i and m2=j and m3>=k))
         then
           s:=s+1; sp[s]:=[i,j,k]; print(sp[s]);
         end if;
       end do;
     end do;
  end do;
```

Тепер кожному набору sp[i] співставимо добуток елементарних симетричних многочленів:

```
> for i from 1 to s do
     k1:=sp[i][1]; k2:=sp[i][2]; k3:=sp[i][3];
     dob[i]:=sigma1^(k1-k2)*sigma2^(k2-k3)*sigma3^k3;
  end do;
```

Тоді $f(x)$ можна подати у вигляді суми:

```
> suma:=tcoeff(lterm)*dob[1];
  for i from 2 to s do suma:=suma+a[i-1]*dob[i]; end do;
  print(suma);
```

Далі будуємо таблицю. Невизначених коефіцієнтів $s-1$, тому рядків в таблиці s. А стовпців 7 (для значень змінних x_1, x_2, x_3, значень елементарних симетричних многочленів $\sigma_1, \sigma_2, \sigma_3$ і стовпець для рівнянь):

```
> M:=Matrix(s,7);
```

Поступово заповнюємо клітинки таблиці. Перший рядок:

```
> M[1,1]:=x1: M[1,2]:=x2: M[1,3]:=x3:
  M[1,4]:=sigma1: M[1,5]:=sigma2: M[1,6]:=sigma3: M[1,7]:=eq:
```

Тепер заповнюватимемо рядки з 2-го по s-ий. За алгоритмом необхідно надати довільних значень c_1, c_2, c_3 змінним x_1, x_2, x_3. Щоб уникнути при цьому в останньому стовпці рівняння виду $0 = 0$ (яке може утворитись у випадку, коли в кожному доданку суми suma є симетричний многочлен σ_i, значення якого дорівнює 0), надамо фіксованих значень змінним x_1, x_2, x_3 так, щоб всі σ_i були відмінні від 0. А саме:

нехай в 2-му рядку $c_1 = 1$, $c_2 = 1$, $c_3 = 1$;

в 3-му рядку $c_1 = 2$, $c_2 = 1$, $c_3 = 1$;

в i-му рядку $c_1 = i-1$, $c_2 = 1$, $c_3 = 1$;

в s-му рядку $c_1 = s-1$, $c_2 = 1$, $c_3 = 1$.

Тоді i-ий рядок буде заповнено наступним чином: $c_1 = i-1$, $c_2 = 1$, $c_3 = 1$, $\sigma_1 = i+1$, $\sigma_2 = 2i-1$, $\sigma_3 = i-1$. В останній стовпець заносимо результат підстановки даних значень в рівність f=suma. Маємо:

```
> for i from 2 to s do
     M[i,1]:=i-1: M[i,2]:=1: M[i,3]:=1:
     M[i,4]:=i+1: M[i,5]:=2*i-1: M[i,6]:=i-1:
     M[i,7]:=subs({x1=M[i,1],x2=M[i,2],x3=M[i,3]},f)=
       subs({sigma1=M[i,4],sigma2=M[i,5],sigma3=M[i,6]},suma);
  end do;
```

Виводимо таблицю на екран:

```
> print(M):
```

Далі розв'язуємо систему рівнянь із останнього рядка таблиці. Щоб потім можна було використовувати значення коефіцієнтів $a_1, a_2, ...$, додаємо команду **assign** (див. §6 розд.I):

```
> assign(solve({seq(M[i,7],i=2..s)}));
```

Знаючи коефіцієнти $a_1, a_2, ...$, знаходимо представлення многочлена $f(x)$ через елементарні симетричні многочлени (на жаль, просто підставити знайдені значення у вираз suma не вдається):

```
> decomp:=tcoeff(lterm)*dob[s];
  for i from s-1 by -1 to 1 do
     decomp:=decomp+a[i]*dob[i];
  end do;
  print(decomp);
```

Таким чином, маємо наступний код процедури:

```
ElSymDecomp:=proc(f)
local i,f1,lterm,m1,m2,m3,s,j,k,sp,k1,k2,k3,dob,suma,a,decomp,M;
   f1:=sort(f, order=plex(x1,x2,x3), descending):
   lterm:=op(1,f1);
   m1:=degree(lterm,x1): m2:=degree(lterm,x2): m3:=degree(lterm,x3):
   s:=0;
   for i from 0 to m1 do
      for j from 0 to i do
         for k from 0 to j do
            if i+j+k=degree(f) and
               (m1>i or (m1=i and m2>j) or (m1=i and m2=j and m3>=k))
               then s:=s+1; sp[s]:=[i,j,k]; print(sp[s]);
            end if;
         end do;
      end do;
   end do;
   for i from 1 to s do
      k1:=sp[i][1]; k2:=sp[i][2]; k3:=sp[i][3];
      dob[i]:=sigma1^(k1-k2)*sigma2^(k2-k3)*sigma3^k3;
   end do;
   suma:=tcoeff(lterm)*dob[s];
   for i from s-1 by -1 to 1 do suma:=suma+a[i]*dob[i]; end do;
   print(suma);
   M:=Matrix(s,7);
   M[1,1]:=x1: M[1,2]:=x2: M[1,3]:=x3:
   M[1,4]:=sigma1: M[1,5]:=sigma2: M[1,6]:=sigma3: M[1,7]:=eq:
   for i from 2 to s do
      M[i,1]:=i-1: M[i,2]:=1: M[i,3]:=1:
      M[i,4]:=i+1: M[i,5]:=2*i-1: M[i,6]:=i-1:
      M[i,7]:=subs({x1=M[i,1],x2=M[i,2],x3=M[i,3]},f)=
         subs( {sigma1=M[i,4],sigma2=M[i,5],sigma3=M[i,6]},suma);
   end do;
   print(M):
   assign(solve({seq(M[i,7],i=2..s)}));
   decomp:=tcoeff(lterm)*dob[s];
   for i from s-1 by -1 to 1 do decomp:=decomp+a[i]*dob[i]; end do;
   print(decomp);
end proc:
```

Розв'язання в Maple. Задаємо многочлен $f(x)$:

```
> f:=x1*x2*(2*x1^2-x1*x2+2*x2^2)+x1*x3*(2*x1^2-x1*x3+2*x3^2)+x2
  *x3*(2*x2^2-x2*x3+2*x3^2)+5*x1^2+5*x2^2+5*x3^2-x1-x2-x3:
```

Запишемо многочлен $f(x)$ в стандартному вигляді:

```
> f1:=expand(f);
```

$$f1 := 2\,x1^3\,x2 - x1^2\,x2^2 + 2\,x1\,x2^3 + 2\,x1^3\,x3 - x1^2\,x3^2 + 2\,x1\,x3^3 + 2\,x2^3\,x3 - x2^2\,x3^2 + 2\,x2\,x3^3 + 5\,x1^2 + 5\,x2^2 + 5\,x3^2 - x1 - x2 - x3$$

Знайдемо однорідні компоненти многочлена $f(x)$:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> asHomogenSum(f1);
```

$$0,\ odnoridna\_komponenta\_stepenya = 0$$
$$-x1 - x2 - x3,\ odnoridna\_komponenta\_stepenya = 1$$
$$5\,x1^2 + 5\,x2^2 + 5\,x3^2,\ odnoridna\_komponenta\_stepenya = 2$$
$$0,\ odnoridna\_komponenta\_stepenya = 3$$

$$2\,x1\,x2^3 + 2\,x1\,x3^3 - x1^2\,x2^2 - x1^2\,x3^2 + 2\,x1^3\,x2 + 2\,x1^3\,x3 + 2\,x2\,x3^3 - x2^2\,x3^2 + 2\,x2^3\,x3,\ odnoridna\_komponenta\_stepenya = 4$$

Таким чином, $f(x)$ можна розкласти в суму однорідних многочленів степенів 4, 2 і 1. Кожний із цих многочленів виразимо через елементарні симетричні многочлени окремо.

Для однорідної компоненти 4-го степеня матимемо:

```
> ElSymDecomp(2*x1*x2^3+2*x1*x3^3-x1^2*x2^2-x1^2*x3^2+2*x1^3*x2+2*x1^3*
  x3+2*x2*x3^3-x2^2*x3^2+2*x2^3*x3);
```

$$[2,\ 1,\ 1]$$
$$[2,\ 2,\ 0]$$
$$[3,\ 1,\ 0]$$
$$2\,\sigma1^2\,\sigma2 + a_2\,\sigma2^2 + a_1\,\sigma1\,\sigma3$$

$$\begin{bmatrix} x1 & x2 & x3 & \sigma1 & \sigma2 & \sigma3 & eq \\ 1 & 1 & 1 & 3 & 3 & 1 & 9 = 54 + 9\,a_2 + 3\,a_1 \\ 2 & 1 & 1 & 4 & 5 & 2 & 35 = 160 + 25\,a_2 + 8\,a_1 \end{bmatrix}$$

$$2\,\sigma1^2\,\sigma2 - 5\,\sigma2^2$$

Отже, однорідна компонента 4-го степеня має представлення $2\sigma_1^2\sigma_2 - 5\sigma_2^2$.

Для однорідної компоненти 2-го степеня отримуємо:

```
> ElSymDecomp(5*x1^2+5*x2^2+5*x3^2);
```

$$[1,\ 1,\ 0]$$
$$[2,\ 0,\ 0]$$

$$5\,\sigma1^2 + a_1\,\sigma2$$

$$\left[\begin{array}{cccccc} x1 & x2 & x3 & \sigma1 & \sigma2 & \sigma3 \\ 1 & 1 & 1 & 3 & 3 & 1 \end{array} \quad eq \quad 15 = 45 + 3\,a_1\right]$$

$$5\,\sigma1^2 - 10\,\sigma2$$

Тобто однорідна компонента 2-го степеня має представлення $5\sigma_1^2 - 10\sigma_2$. Однорідну компоненту 1-го степеня в Maple перевіряти не має смислу. Отримуємо наступне представлення многочлена $f(x)$:

```
> expand(2*sigma1^2*sigma2-5*sigma2^2+5*sigma1^2-10*sigma2-sigma1);
```

$$2\,\sigma1^2\,\sigma2 - 5\,\sigma2^2 + 5\,\sigma1^2 - 10\,\sigma2 - \sigma1$$

Завдання 44. Виразити через елементарні симетричні многочлени многочлен:

44.1. $f(x_1, x_2, x_3) = 3x_1^4 + 3x_2^4 + 3x_3^4 - 2x_1 - 2x_2 - 2x_3$.

44.2. $f(x_1, x_2, x_3) = x_1^2x_2 + x_2^2x_3 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2x_3^2 - 5x_1x_2 - 5x_2x_3 - 5x_1x_3$.

44.3. $f(x_1, x_2, x_3) = (x_1 + x_2 - 2x_3)(x_2 + x_3 - 2x_1)(x_1 + x_3 - 2x_2)$.

44.4. $f(x_1, x_2, x_3) = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$.

44.5. $f(x_1, x_2, x_3) = (x_1x_2 + x_3)(x_1x_3 + x_2)(x_2x_3 + x_1)$.

44.6. $f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 + 3x_1x_2 + 3x_2x_3 + 3x_1x_3$.

44.7. $f(x_1, x_2, x_3) = x_1^3x_2^2 + x_2^3x_3^2 + x_1^3x_3^2 + x_1^2x_2^3 + x_1^2x_3^3 + x_2^2x_3^3 + 2x_1x_2x_3$.

44.8. $f(x_1, x_2, x_3) = (x_1^2 + 2 + x_2^2)(x_2^2 + 2 + x_3^2)(x_1^2 + 2 + x_3^2)$.

44.9. $f(x_1, x_2, x_3) = (x_1 - x_2)^4 + (x_2 - x_3)^4 + (x_1 - x_3)^4$.

44.10. $f(x_1, x_2, x_3) = (x_1^2 + x_2^2)(x_2^2 + x_3^2)(x_1^2 + x_3^2)$.

44.11. $f(x_1, x_2, x_3) = (x_1 - x_2)^4 + (x_2 - x_3)^4 + (x_1 - x_3)^4$.

44.12. $f(x_1, x_2, x_3) = x_1^2(x_2 + 1 + x_3) + x_2^2(x_1 + 1 + x_3) + x_3^2(x_1 + 1 + x_2)$.

44.13. $f(x_1, x_2, x_3) = x_1^4x_2 + x_2^4x_3 + x_1^4x_3 + x_1x_2^4 + x_1x_3^4 + x_2x_3^4$.

44.14. $f(x_1, x_2, x_3) = (x_1^2 + 2x_2x_3)(x_2^2 + 2x_1x_3)(x_3^2 + 2x_1x_2)$.

44.15. $f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 - 2x_1x_2x_3 + 3x_1x_2 + 3x_2x_3 + 3x_1x_3$.

44.16. $f(x_1, x_2, x_3) = (x_1 + 2x_2x_3)(x_2 + 2x_1x_3)(x_3 + 2x_1x_2)$.

44.17. $f(x_1, x_2, x_3) = (x_1 + 3 + x_2)(x_1 + 3 + x_3)(x_2 + 3 + x_3)$.

44.18. $f(x_1, x_2, x_3) = x_1^3 + 3x_1^2x_2^2 + x_2^3 + 3x_2^2x_3^2 + x_3^3 + 3x_1^2x_3^2$.

44.19. $f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 + 2(x_1^2 - x_2^2)(x_2^2 - x_3^2)(x_1^2 - x_3^2)$.

44.20. $f(x_1, x_2, x_3) = (x_1 + x_2)^4 + (x_2 + x_3)^4 + (x_1 + x_3)^4$.

44.21. $f(x_1, x_2, x_3) = (x_1^2 - x_2x_3)(x_2^2 - x_1x_3)(x_3^2 - x_1x_2)$.

44.22. $f(x_1, x_2, x_3) = (2x_1 - x_2 - x_3)(2x_2 - x_3 - x_1)(2x_3 - x_1 - x_2)$.

44.23. $f(x_1, x_2, x_3) = x_1^2x_2^2 + x_2^2x_3^2 + x_1^2x_3^2 + 3x_1 + 3x_2 + 3x_3$.

44.24. $f(x_1, x_2, x_3) = (1 + x_1^2x_2^2)(1 + x_1^2x_3^2)(1 + x_2^2x_3^2)$.

44.25. $f(x_1, x_2, x_3) = (x_1^2 + x_2 + x_3)(x_2^2 + x_1 + x_3)(x_3^2 + x_1 + x_2)$.

2. Розклад многочленів від багатьох змінних в добуток незвідних множників

ТЕОРЕТИЧНІ ВІДОМОСТІ

Означення подільності многочленів, властивості подільності, поняття звідного та незвідного многочлена у кільці $P[x_1, x_2, \ldots, x_n]$ залишаються такими самими, що й в кільці $P[x]$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 45.1. Розкласти на незвідні над полем $\mathbb{Q}$ множники многочлен

$$f(x, y, z) = x^2(y - z)^2 - y^2(z - x)^2 + z^2(x - y)^2,$$

використовуючи теорему Безу і метод невизначених коефіцієнтів;

Розв'язання. Будемо розглядати многочлен $f(x, y, z)$ як многочлен від змінної z над областю цілісності $\mathbb{Q}[x, y]$. Знайдемо значення цього многочлена і при $z = y$:

$$\begin{aligned} \text{при } z = 0\text{:} \qquad f(x, y, 0) &= x^2(y - 0)^2 - y^2(0 - x)^2 + 0(x - y)^2 = \\ &= x^2y^2 - y^2x^2 + 0 = 0, \\ \text{і при } z = y\text{:} \qquad f(x, y, y) &= x^2(y - y)^2 - y^2(y - x)^2 + y^2(x - y)^2 = 0. \end{aligned}$$

Це означає, що $f(x,y,z)$ ділиться на двочлени $\underbrace{z-0}_{z}$ і $z-y$.

Тепер розглядатимемо многочлен $f(x,y,z)$ як многочлен від змінної x над областю цілісності $\mathbb{Q}[y,z]$. Знайдемо його значення

$$\text{при } x=0: \qquad f(0,y,z) \;=\; 0-y^2z^2+z^2y^2=0.$$

Отже, заданий многочлен ділиться на $\underbrace{x-0}_{x}$.

Враховуючи те, що многочлени $z, z-y, x$ попарно взаємно прості, то $f(x,y,z)$ ділиться і на їхній добуток $xz(z-y)$.

Оскільки многочлен $f(x,y,z)$ – однорідний 4-го степеня, а многочлен $xz(z-y)$ має степінь 3, то частка від ділення $f(x,y,z)$ на $xz(z-y)$ є однорідним многочленом від змінних x,y,z 1-го степеня. Знайдемо цей многочлен методом невизначених коефіцієнтів. Маємо:

$$x^2(y-z)^2-y^2(z-x)^2+z^2(x-y)^2=xz(z-y)(ax+by+cz),$$

де $a,b,c\in\mathbb{Q}$. Або

$$-2x^2yz+2x^2z^2+2xy^2z-2xyz^2=ax^2z^2-ax^2yz+bxyz^2-bxy^2z+cxz^3-cxyz^2.$$

Прирівнюємо коефіцієнти при відповідних членах:

$$\begin{array}{r|l} x^2yz & -2=-a,\\ x^2z^2 & 2=a,\\ xy^2z & 2=-b,\\ xyz^2 & -2=b-c,\\ xz^3 & 0=c. \end{array}$$

Маємо: $a=2$, $b=-2$, $c=0$.

Отже, шуканий розклад многочлена $f(x,y,z)$ має вигляд:

$$f(x,y,z)=xz(z-y)(2x-2y)=2xz(z-y)(x-y).$$

Розв'язання в Maple. Як і у випадку многочленів від однієї змінної, для розкладу многочлена $f(x)$ на множники над числовим полем P використовується команда **factor(f, P)**. Якщо другий аргумент **P** не задано, здійснюється розклад многочлена $f(x)$ над полем, до якого належать його коефіцієнти.

```
> f:=x^2*(y-z)^2-y^2*(z-x)^2+z^2*(x-y)^2:
> factor(f);
```

$$-2\,x\,z\,(y-z)\,(x-y)$$

Приклад 45.2. Розкласти на незвідні над полем $\mathbb{Q}$ множники многочлен

$$f(x,y) = x^3 - 2x^2y - x^4y^2 + 3x^3y^3 - x^2y^4 - 2xy^2 + y^3.$$

Розв'язання. Виразимо многочлен $f(x,y)$ через елементарні симетричні многочлени: $\sigma_1 = x + y$, $\sigma_2 = xy$. Для цього запишемо його як суму однорідних многочленів:

$$f(x,y) = h_1(x,y) + h_2(x,y),$$

$$\begin{aligned} \text{де} \quad h_1(x,y) &= x^3 - 2x^2y - 2xy^2 + y^3, \\ h_2(x,y) &= -x^4y^2 + 3x^3y^3 - x^2y^4 \end{aligned}$$

– многочлени 3-го і 6-го степенів відповідно.

Виразимо спочатку многочлен $h_1(x,y)$ через елементарні симетричні многочлени σ_1 і σ_2 (це легко зробити, використовуючи формули скороченого множення):

$$\begin{aligned} h_1(x,y) &= x^3 - 2x^2y - 2xy^2 + y^3 = (x^3 + y^3) - 2xy(x+y) = \\ &= (x+y)(x^2 - xy + y^2) - 2xy(x+y) = (x+y)(x^2 + y^2 - 3xy) = \\ &= (x+y)\left((x+y)^2 - 5xy\right) = (x+y)^3 - 5xy(x+y) = \sigma_1^3 - 5\sigma_2\sigma_1. \end{aligned}$$

Аналогічно

$$\begin{aligned} h_2(x,y) &= -x^4y^2 + 3x^3y^3 - x^2y^4 = -x^2y^2(x^2 - 3xy + y^2) = \\ &= -x^2y^2\left((x+y)^2 - 5xy\right) = -x^2y^2(x+y)^2 + 5x^3y^3 = -\sigma_1^2\sigma_2^2 + 5\sigma_2^3. \end{aligned}$$

Таким чином,

$$\begin{aligned} f(x,y) = h_1(x,y) + h_2(x,y) &= (\sigma_1^3 - 5\sigma_2\sigma_1) + (-\sigma_1^2\sigma_2^2 + 5\sigma_2^3) = \\ &= \sigma_1(\sigma_1^2 - 5\sigma_2) - \sigma_2^2(\sigma_1^2 - 5\sigma_2) = (\sigma_1^2 - 5\sigma_2)(\sigma_1 - \sigma_2^2). \end{aligned}$$

Враховуючи, що $\sigma_1 = x + y$, $\sigma_2 = xy$, маємо:

$$f(x,y) = (x^2 - 3xy + y^2)(x + y - x^2y^2).$$

Розв'язання в Maple. Маємо:

```
> f:=x^3-2*x^2*y-x^4*y^2+3*x^3*y^3-x^2*y^4-2*x*y^2+y^3:
> factor(f);
```

$$-(x^2\,y^2 - x - y)\,(x^2 - 3\,x\,y + y^2)$$

Завдання 45. Розкласти многочлен на незвідні над полем $\mathbb{Q}$ множники:
а) використовуючи теорему Безу і метод невизначених коефіцієнтів;
б) виражаючи многочлен через елементарні симетричні многочлени.

45.1. а) $f(x,y,z) = (x+y)(x-y)^3 + (y+z)(y-z)^3 + (z+x)(z-x)^3$;
б) $f(x,y) = 3x^5 + 17x^4y + 36x^3y^2 - 12x^3y - 12xy^3 + 36x^2y^3 + 17xy^4 + +3y^5 - 32x^2y^2$.

45.2. а) $f(x,y,z) = x^2y^2(x-y) + y^2z^2(y-z) + z^2x^2(z-x)$;
б) $f(x,y) = 2x^3 - 8x^2y - x^4y^2 + 5x^3y^3 - x^2y^4 - 8xy^2 + 2y^3$.

45.3. а) $f(x,y,z) = yz(y^3-z^3) + zx(z^3-x^3) + xy(x^3-y^3)$;
б) $f(x,y) = 2x^4+5x^3y+6x^2y^2+10x^3+15x^2y+15xy^2+2y^4+10y^3+5xy^3$.

45.4. а) $f(x,y,z) = z^3(x-y)^3 + x^3(y-z)^3 + y^3(z-x)^3$;
б) $f(x,y) = 2x^3 + 4x^3y + 8x^2y^2 + 2y^3 + 4xy^3 - 3x^2 - 6xy - 3y^2$.

45.5. а) $f(x,y,z) = (x^2-y^2)^3 + (y^2-z^2)^3 + (z^2-x^2)^3$;
б) $f(x,y) = 2x^4 + 3x^3y - x^2y^2 - x^2 + 3xy^3 + xy + 2y^4 - y^2$.

45.6. а) $f(x,y,z) = (x-y)^5 + (y-z)^5 + (z-x)^5$;
б) $f(x,y) = x^5 + 4x^4y + 7x^3y^2 + 7x^2y^3 + 4xy^4 + y^5 + 3x^2 + 3xy + 3y^2$.

45.7. а) $f(x,y,z) = z(x^2-y^2)^2 - x(y^2-z^2)^2 + y(z^2-x^2)^2$;
б) $f(x,y) = 2x^5y^2+6x^4y^3+6x^3y^4-6x^3y^2+2x^2y^5-6x^2y^3-x^2-2xy-y^2+3$.

45.8. а) $f(x,y,z) = x^4(y-z) + y^4(z-x) + z^4(x-y)$;
б) $f(x,y) = 3x^3 - 15x^2y - x^4y^2 + 6x^3y^3 - x^2y^4 - 15xy^2 + 3y^3$.

45.9. а) $f(x,y,z) = xy(x^2-y^2) - yz(y^2-z^2) + zx(z^2-x^2)$;
б) $f(x,y) = x^4 - 2x^2y^2 - 3x^3 + 3x^2y + 3xy^2 + y^4 - 3y^3$.

45.10. а) $f(x,y,z) = z^2(x^2-y^2)^2 - x^2(y^2-z^2)^2 + y^2(z^2-x^2)^2$;
б) $f(x,y) = 2x^4y + 3x^3y^2 + 10x^3 + 15x^2y + 3x^2y^3 + 15xy^2 + 2xy^4 + 10y^3$.

45.11. а) $f(x,y,z) = x^2(y-z)^3 + y^2(z-x)^3 + z^2(x-y)^3$;
б) $f(x,y) = 2x^3-4x^2y+4x^3y-4xy^2+8x^2y^2+2y^3+4xy^3-5x^2-10xy-5y^2$.

45.12. а) $f(x,y,z) = xy^2z(x^2-z^2) + yz^2x(y^2-x^2) + zx^2y(z^2-y^2)$;
б) $f(x,y) = x^4 + 2x^3y - 6x^2y^2 - x^2 + 2xy^3 + 2xy + y^4 - y^2$.

45.13. а) $f(x,y,z) = x(y^4 - z^4) + y(z^4 - x^4) + z(x^4 - y^4)$;
б) $f(x,y) = 2x^5 + 9x^4y + 17x^3y^2 + 17x^2y^3 + 9xy^4 + 2y^5 - 2x^2 - 3xy - 2y^2$.

45.14. а) $f(x,y,z) = x(y-z)^3 + y(z-x)^3 + z(x-y)^3$;
б) $f(x,y) = 3x^4y + 9x^3y^2 + x^4y^3 - 6x^3y - 12x^2y^2 + x^3y^4 + 9x^2y^3 + 3xy^4 - 2x^3y^3 - 6xy^3$.

45.15. а) $f(x,y,z) = (x-y)(x+y)^3 + (y-z)(y+z)^3 + (z-x)(z+x)^3$;
б) $f(x,y) = x^4 + x^3y - 3x^3 + xy^3 + y^4 - 3y^3$.

45.16. а) $f(x,y,z) = x^3y^3(x-y) + y^3z^3(y-z) + z^3x^3(z-x)$;
б) $f(x,y) = x^4 + x^3y + 3x^3 + xy^3 + y^4 + 3y^3$.

45.17. а) $f(x,y,z) = x^3(y-z) + y^3(z-x) + z^3(x-y)$;
б) $f(x,y) = 2x^3 - 9x^2y + 6x^3y - 9xy^2 + 12x^2y^2 + 2y^3 + 6xy^3 - 5x^2 - 10xy - 5y^2$.

45.18. а) $f(x,y,z) = x^2y^2(x^2-y^2) + y^2z^2(y^2-z^2) + z^2x^2(z^2-x^2)$;
б) $f(x,y) = x^4 + 9x^3y + 22x^2y^2 + 9xy^3 + y^4$.

45.19. а) $f(x,y,z) = x^3(y^2-z^2) + y^3(z^2-x^2) + z^3(x^2-y^2)$;
б) $f(x,y) = 2x^4y + 5x^3y^2 + 5x^2y^3 + 2xy^4 - 2x^2 - 3xy - 2y^2$.

45.20. а) $f(x,y,z) = x(y^4 - z^4) - y(z^4 - x^4) + z(x^4 - y^4)$;
б) $f(x,y) = 3x^4 + 23x^3y + 50x^2y^2 + 23xy^3 + 3y^4$.

45.21. а) $f(x,y,z) = yz(y^2-z^2) + zx(z^2-x^2) + xy(x^2-y^2)$;
б) $f(x,y) = x^4 + 2x^3y + 2x^2y^2 + 4x^3 + 4x^2y + 2xy^3 + y^4 + 4xy^2 + 4y^3$.

45.22. а) $f(x,y,z) = z^2(x+y)^2 - y^2(z+x)^2 + x^2(y+z)^3$;
б) $f(x,y) = 2x^3 + 7x^2y + 6x^3y + 7xy^2 + 15x^2y^2 + 2y^3 + 6xy^3$.

45.23. а) $f(x,y,z) = (x+y+z)^5 - x^5 - y^5 - z^5$;
б) $f(x,y) = 2x^4y + 3x^3y^2 - 2x^3 - 3x^2y + 3x^2y^3 - 3xy^2 + 2xy^4 - 2y^3$.

45.24. а) $f(x,y,z) = z(x^2-y^2)^2 + x(y^2-z^2)^2 + y(z^2-x^2)^2$;
б) $f(x,y) = 3x^5 + 20x^4y + 45x^3y^2 + 6x^3y + 22x^2y^2 + 6xy^3 + 45x^2y^3 + 20xy^4 + 3y^5$.

45.25. а) $f(x,y,z) = x^3(y^2-z^2) - y^3(z^2-x^2) + z^3(x^2-y^2)$;
б) $f(x,y) = x^5 + 4x^3y^2 + 3x^4y + 4x^2y^3 + 3xy^4 + y^5 + 3x^3y + 3xy^3$.

3. Застосування симетричних многочленів до розв'язування задач з елементарної математики

Приклад 46.1. Знайти дійсні розв'язки рівняння

$$\sqrt[4]{629-x}+\sqrt[4]{77+x}=8.$$

Розв'язання. Зробимо заміну: нехай

$$\begin{aligned}\sqrt[4]{629-x}&=u,\\ \sqrt[4]{77+x}&=v.\end{aligned}\tag{V.1}$$

Тоді матимемо систему рівнянь:

$$\begin{cases}u+v=8,\\ u^4+v^4=706.\end{cases}\tag{V.2}$$

Позначимо $u+v=\sigma_1$, $uv=\sigma_2$ і виразимо u^4+v^4 через елементарні симетричні многочлени σ_1 і σ_2. Маємо:

$$u^4+v^4=(u^4+2u^2v^2+v^4)-2u^2v^2=(u^2+v^2)^2-2(uv)^2=[(u+v)^2-2uv]^2-$$
$$-2(uv)^2=(\sigma_1^2-2\sigma)^2-2\sigma_2^2=\sigma_1^4-4\sigma_1^2\sigma_2+4\sigma_2^2-2\sigma_2^2=\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2.$$

Система (V.2) набуде вигляду

$$\begin{cases}\sigma_1=8,\\ \sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2=706,\end{cases}$$

звідки або $\begin{cases}\sigma_1=8,\\ \sigma_2=113;\end{cases}$ або $\begin{cases}\sigma_1=8,\\ \sigma_2=15.\end{cases}$

Повертаючись до змінних u і v, маємо:

$$\begin{cases}u+v=8,\\ uv=113;\end{cases}\quad\text{або}\quad\begin{cases}u+v=8,\\ uv=15.\end{cases}$$

Неважко показати, що перша система рівнянь дійсних розв'язків не має, а розв'язками другої є

$$\begin{cases}u_1=3,\\ v_1=5;\end{cases}\quad\text{і}\quad\begin{cases}u_2=5,\\ v_2=3.\end{cases}$$

Із урахуванням (V.1) знаходимо відповідні значення x. Маємо:

$$\sqrt[4]{629-x}=3\quad\text{або}\quad\sqrt[4]{629-x}=5,$$

звідки

$$x = 548 \quad \text{або} \quad x = 4.$$

Зауваження. На практиці дуже часто зустрічаються симетричні многочлени виду

$$S_k = x_1^k + x_1^k + \ldots + x_n^k,$$

тобто суми k-тих степенів змінних. Їх називають степеневими сумами. Неважко показати, що справедливі наступні співвідношення:

$$\begin{aligned} S_2 &= x_1^2 + x_2^2 + \ldots + x_n^2 = \sigma_1^2 - 2\sigma_2, \\ S_3 &= x_1^3 + x_2^3 + \ldots + x_n^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \end{aligned} \tag{V.3}$$

Аналогічно можна виразити через елементарні симетричні многочлени степеневі суми S_4, S_5 і т.д.

Розв'язання в Maple. Система Maple може розв'язувати алгебраїчні рівняння, нерівності та їхні системи як в аналітичному, так і в чисельному вигляді. По-перше, зауважимо, що два вирази, які поєднані знаком рівності (=), є самостійним типом даних Maple - рівняння (equation). Над рівняннями можна здійснювати перетворення, використовуючи звичайні арифметичні дії, які виконуються окремо для лівої і правої частин рівняння.

Для розв'язування рівняння eq з одним невідомим x використовується команда **solve(eq, x)** (див. §6 розд.I). При цьому радикали виду $\sqrt[n]{g}$ вводимо у форматі $(g)\hat{}(1/n)$, для квадратних коренів можна використовувати формат **sqrt(g)**.

```
> solve((629-x)^(1/4)+(77+x)^(1/4)=8,x);
```

$$4,\ 548$$

Зауваження. В окремих випадках Maple не дає точного розв'язку, навіть якщо він існує, або подає розв'язки за допомогою RootOfs (див. Приклад 38.1). Тоді можна знайти наближений розв'язок і в такий спосіб перевірити отриманий аналітично розв'язок. Для цього один із коефіцієнтів задаємо як число типу float (записуємо із „плаваючою крапкою").

Приклад 46.2. Знайти дійсні розв'язки системи рівнянь:

а) $$\begin{cases} x^2y + xy^2 = 6, \\ xy + x + y = 5; \end{cases}$$

б) $$\begin{cases} x - y + z = 4, \\ x^2 + y^2 + z^2 = 14, \\ x^3 - y^3 + z^3 = 34. \end{cases}$$

Розв'язання. а) Ліва частина кожного із рівнянь заданої системи є симетричним многочленом від змінних x, y. Виразимо кожну з них через елементарні симетричні многочлени $\sigma_1 = x + y$, $\sigma_2 = xy$:

$$x^2y + xy^2 = xy(x + y) = \sigma_2\sigma_1; \qquad xy + x + y = \sigma_2 + \sigma_1.$$

Тоді $\begin{cases} \sigma_2\sigma_1 = 6, \\ \sigma_2 + \sigma_1 = 5. \end{cases}$ Значення змінних σ_1 і σ_2 є коренями многочлена $u^2 - 5u + 6$, значить, $\sigma_1 = 3$, $\sigma_2 = 2$ або навпаки. Розглянемо дані випадки.

Випадок 1: $\sigma_1 = 3$, $\sigma_2 = 2$. Маємо: $\begin{cases} x + y = 3, \\ xy = 2; \end{cases}$ звідси $x = 1, y = 2$ або $x = 2, y = 1$.

Випадок 2: $\sigma_1 = 2$, $\sigma_2 = 3$. Маємо: $\begin{cases} x + y = 2, \\ xy = 3; \end{cases}$ звідси значення x, y є коренями многочлена $v^2 - 2v + 3$ (який дійсних коренів не має).

Отже, задана система рівнянь має лише два дійсних розв'язки: $(1; 2)$ і $(2; 1)$.

б) Введемо заміну: нехай

$$t = -y.$$

Маємо:

$$\begin{cases} x + t + z = 4, \\ x^2 + t^2 + z^2 = 14, \\ x^3 + t^3 + z^3 = 34. \end{cases} \tag{V.4}$$

Ліва частина кожного із рівнянь системи (V.4) є симетричним многочленом від змінних x, t, z. Нехай

$$\begin{aligned} \sigma_1 &= x + t + z, \\ \sigma_2 &= xt + xz + tz, \\ \sigma_3 &= xtz. \end{aligned}$$

Тоді, використовуючи формули (V.3), систему рівнянь (V.4) можна записати у вигляді

$$\begin{cases} \sigma_1 = 4, \\ \sigma_1^2 - 2\sigma_2 = 14, \\ \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 34, \end{cases}$$

звідки

$$\begin{cases} \sigma_1 = 4, \\ \sigma_2 = 1, \\ \sigma_3 = -6; \end{cases} \quad \text{або} \quad \begin{cases} x + t + z = 4, \\ xt + xz + tz = 1, \\ xtz = -6. \end{cases}$$

Значення змінних x, t, z є коренями нормованого многочлена 3-го степеня: $u^3 - 4u^2 + u + 6$. Знаходимо корені даного многочлена: $u_1 = -1$, $u_2 = 2$, $u_3 = 3$. Отже, одним із розв'язків системи рівнянь (V.4) є $(-1, 2, 3)$. Усі інші розв'язки, зважаючи на те, що система (V.4) симетрична, можна дістати перестановкою чисел $-1, 2, 3$. Таким чином,

$$(x; t; z) \in \{(-1; 2; 3), (-1; 3; 2), (2; -1; 3), (2; 3; -1), (3; -1; 2), (3; 2; -1)\}.$$

Враховуючи те, що $y = -t$, отримаємо наступні розв'язки заданої системи:

$$(x; y; z) \in \{(-1; -2; 3), (-1; -3; 2), (2; 1; 3), (2; -3; -1), (3; 1; 2), (3; -2; -1)\}.$$

Розв'язання в Maple. При розв'язуванні систем рівнянь використовується формат **solve({eq1, eq2,...,eqn}, {x1,x2,...,xk})**, де eq1, eq2,...,eqn – рівняння системи, x1,x2,...,xk – невідомі (див. §6 розд.I).

а)

```
> solve({x^2*y+x*y^2=6,x*y+x+y=5},{x,y});
```

$\{x = 2,\ y = 1\},\ \{x = 1,\ y = 2\},$

$\{x = -\mathrm{RootOf}(\_Z^2 - 2\,\_Z + 3) + 2,\ y = \mathrm{RootOf}(\_Z^2 - 2\,\_Z + 3)\}$

Квадратний тричлен $z^2 - 2z + 3$ дійсних коренів не має, тому $\mathrm{RootOf}(\_Z^2 - 2\,\_Z + 3) \notin \mathbb{R}$, а значить, дійсних розв'язків даної системи є лише два: $(2, 1)$, $(1, 2)$.

б)

```
> solve({x-y+z=4, x^2+y^2+z^2=14,x^3-y^3+z^3=34}, {x,y,z});
```

$\{x = 3,\ y = 1,\ z = 2\},\ \{x = 2,\ y = 1,\ z = 3\},\ \{x = 2,\ y = -3,\ z = -1\},$
$\{x = -1,\ y = -3,\ z = 2\}, \{x = 3,\ y = -2,\ z = -1\},\ \{x = -1,\ y = -2,\ z = 3\}$

Завдання 46. Знайти дійсні розв'язки: а) рівняння;
б) системи рівнянь.

46.1. а) $\sqrt[4]{\sqrt{x} + 71} = 2 + \sqrt[4]{11 - \sqrt{x}}$;

б) $\begin{cases} x + y - z = 9, \\ x^2 + y^2 + z^2 = 41, \\ x^3 + y^3 - z^3 = 189. \end{cases}$

46.2. а) $x\frac{11-x}{x+1}(x + \frac{11-x}{x+1}) = 30$;

б) $\begin{cases} (x\sqrt{y}+y\sqrt{x})(x+y)=390, \\ x\sqrt{x}+y\sqrt{y}=35. \end{cases}$

46.3. 15.3 а) $x+\sqrt[3]{28-x^3}-x\sqrt[3]{28-x^3}=1$;

б) $\begin{cases} (x^2+y^2)(x+y)=15xy, \\ (x^4+y^4)(x^2+y^2)=85x^2y^2. \end{cases}$

46.4. а) $\sqrt[4]{x+26}+\sqrt[4]{6-x}=3\sqrt{2}$;

б) $\begin{cases} xy-yz-xz=11, \\ x^3+y^3-z^3=36, \\ xyz=-6. \end{cases}$

46.5. а) $x\sqrt[3]{35-x^3}(x+\sqrt[3]{35-x^3})=30$;

б) $\begin{cases} x^3+x^3y^3+y^3=17, \\ x+xy+y=5. \end{cases}$

46.6. а) $\sqrt[7]{4+\sqrt[3]{x+7}}-\sqrt[7]{9-\sqrt[3]{28-x}}=0$;

б) $\begin{cases} x^2+y^2-x-y=2, \\ x^4+y^4+x+y-2(x^3+y^3)=4. \end{cases}$

46.7. а) $\sqrt[5]{\frac{1}{2}+\sqrt{x}}+\sqrt[5]{\frac{1}{2}-\sqrt{x}}=1$;

б) $\begin{cases} x-y-z=2, \\ x^2+y^2+z^2=6, \\ x^3-y^3-z^3=8. \end{cases}$

46.8. а) $(x+\frac{10+x}{2x-1})x^{\frac{10+x}{2x-1}}=48$;

б) $\begin{cases} x^3+x^3y^3+y^3=17, \\ x+xy+y=0. \end{cases}$

46.9. а) $x+\sqrt{5-x^2}+x\sqrt{5-x^2}=-1$;

б) $\begin{cases} x-y+z=1, \\ xy+yz-zx=4, \\ x^3-y^3+z^3=1. \end{cases}$

46.10. а) $\sqrt{\frac{20+x}{x}}+\sqrt{\frac{20-x}{x}}=\sqrt{6}$;

б) $\begin{cases} \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{13}{3}, \\ x+y+z=\frac{13}{3}, \\ xyz=1. \end{cases}$

46.11. а) $\sqrt[21]{11+\sqrt[3]{15+x^2}}-\sqrt[21]{16-\sqrt[3]{50-x^2}}=0$;

б) $\begin{cases} x^3+y^3-2x^2+xy-2y^2=35, \\ x^2y+xy^2-x-y=15. \end{cases}$

46.12. а) $\sqrt{37-4x^2}+2x+11=6x\sqrt{37-4x^2}$;

б) $\begin{cases} x^2-xy+y^2=19, \\ x^4+x^2y^2+y^4=931. \end{cases}$

46.13. а) $\sqrt[4]{97-x}+\sqrt[4]{x-15}=4$;

б) $\begin{cases} x+y-z=1, \\ x^2+y^2+z^2=3, \\ x^3+y^3-z^3=1. \end{cases}$

46.14. а) $(x+2+\sqrt[3]{9-x^3})x\sqrt[3]{9-x^3}=10$;

б) $\begin{cases} x^2+xy+y^2=4, \\ (x+xy+y)(x^3+y^3)=16. \end{cases}$

46.15. а) $x+\sqrt[3]{126-x^3}+1=7x\sqrt[3]{126-x^3}$;

б) $\begin{cases} x+y=7+\sqrt{xy}, \\ x^2+y^2=9xy+1. \end{cases}$

46.16. а) $\sqrt[3]{10-\sqrt{x-1}}+\sqrt[3]{6+\sqrt{x-1}}=4$;

б) $\begin{cases} x-y+z=6, \\ x^2+y^2+z^2=14, \\ x^3-y^3+z^3=36. \end{cases}$

46.17. а) $3(x+\sqrt[4]{97-x^4})=5x\sqrt[4]{97-x^4}+3$;

б) $\begin{cases} x^7y-xy^7=126, \\ x-y+2xy=5. \end{cases}$

46.18. а) $\sqrt[18]{11+\sqrt[4]{76-3x}}-\sqrt[18]{16-\sqrt[4]{21+3x}}=0$;

б) $\begin{cases} (x^2+1)(y^2+1)=10, \\ (x+y)(xy-1)=3. \end{cases}$

46.19. а) $\sqrt[3]{5+\sqrt{x+2}}=4-\sqrt[3]{23-\sqrt{x+2}}$;

б) $\begin{cases} \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1, \\ x^2+y^2+z^2=41, \\ yz+zx+xy=20. \end{cases}$

46.20. а) $x^{\frac{x+1}{8-x}}(\frac{x+1}{8-x}+x)=70$;

б) $\begin{cases} xy^3+x^3y=78, \\ (x+y)(x^2+y^2)=65. \end{cases}$

46.21. а) $x\sqrt[4]{82-x^4}+2(x+\sqrt[4]{82-x^4})=11$;

б) $\begin{cases} x^4+6x^2y^2+y^4=136, \\ x^3y+xy^3=30. \end{cases}$

46.22. а) $\sqrt[3]{24+\sqrt{x}}-\sqrt[3]{5+\sqrt{x}}=1$;

б) $\begin{cases} x+y-z=1, \\ x^2+y^2+z^2=1, \\ x^3+y^3-z^3=1. \end{cases}$

46.23. а) $\sqrt[3]{35-x^3}+2x\sqrt[3]{35-x^3}+x=17$;

б) $\begin{cases} x-y+z=9, \\ x^2+y^2+z^2=35, \\ xyz=-15. \end{cases}$

46.24. а) $\sqrt[24]{17+\sqrt[4]{\sqrt[3]{x}-2}}-\sqrt[24]{20-\sqrt[4]{19-\sqrt[3]{x}}}=0$;

б) $\begin{cases} x+xy+y=14, \\ (x^2+y^2)(x^3+y^3)=1440. \end{cases}$

46.25. а) $\sqrt[4]{18+5x}+\sqrt[4]{64-5x}=4$;

б) $\begin{cases} \frac{1}{x}+\frac{1}{y}-\frac{1}{z}=\frac{7}{2}, \\ x+y-z=\frac{7}{2}, \\ xyz=-1. \end{cases}$

4. Спільні корені многочленів від багатьох змінних

ТЕОРЕТИЧНІ ВІДОМОСТІ

Коренем многочлена $f \in P[x_1, x_1, ..., x_n]$, де P – поле, називають впорядкований набір $(c_1, c_2, ..., c_n)$ елементів поля P, такий, що $f(c_1, c_2, ..., c_n) = 0$.

Многочлен $f \in P[x_1, x_1, ..., x_n]$, $n \geqslant 2$, взагалі кажучи, може мати і безліч коренів. Тому задача пошуку коренів многочлена від $n \geqslant 2$ змінних (на відміну від випадку $n = 1$) є невизначеною. Водночас, задача пошуку спільних коренів двох (кількох) многочленів має достатньо широке практичне застосування. Розглянемо дану задачу спочатку для випадку $n = 1$.

I. Пошук спільних коренів двох многочленів від однієї змінної. Нехай $P[x]$ – кільце многочленів від однієї змінної x над полем P, F – деяке розширення поля P. Говорять, що елемент $c \in F$ є спільним коренем двох многочленів $f(x)$ і $g(x)$ із кільця $P[x]$, якщо c є коренем як многочлена $f(x)$, так і многочлена $g(x)$. Для знаходження всіх спільних коренів многочленів $f(x)$ і $g(x)$, застосовують наступні способи.

Спосіб I (за допомогою алгоритму Евкліда): елемент $c \in F$ є спільним коренем многочленів $f(x)$ і $g(x)$ тоді і лише тоді, коли c є коренем многочлена $d(x) \sim (f, g)$.

Спосіб II (за допомогою результанта). Результантом многочленів

$$\begin{aligned} f(x) &= a_n x^n + \ldots + a_1 x + a_0, \qquad n \geqslant 1, \\ g(x) &= b_m x^m + \ldots + b_1 x + b_0, \qquad m \geqslant 1, \end{aligned}$$

називається визначник

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & \ldots & a_1 & a_0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & a_n & a_{n-1} & \ldots & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & a_n & \ldots & \ldots & a_3 & a_2 & a_1 & a_0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \ldots & \ldots & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \ldots & b_1 & b_0 & 0 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & b_m & b_{m-1} & \ldots & b_2 & b_1 & b_0 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & 0 & b_m & \ldots & b_3 & b_2 & b_1 & b_0 & \ldots & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & b_m & b_{m-1} & b_{m-2} & b_{m-3} & \ldots & b_1 & b_0 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}$$

порядку $m + n$. В цьому визначнику перші m рядків заповнюються із зсувом на один крок коефіцієнтами многочлена $f(x)$, а решта n рядків – коефіцієнтами многочлена $g(x)$. Елементи визначника, розташовані нижче за a_n і b_m та елементи, що знаходяться вище за a_0 і b_0, всі дорівнюють 0. Відмітимо також, що на головній діагоналі m елементів a_n і n елементів b_m.

Теорема. *Многочлени*

$$\begin{aligned} f(x) &= a_n x^n + \ldots + a_1 x + a_0, \qquad a_n \neq 0, n \geqslant 1 \\ g(x) &= b_m x^m + \ldots + b_1 x + b_0, \qquad b_m \neq 0, m \geqslant 1, \end{aligned}$$

із кільця $P[x]$, P – поле, мають спільний корінь (можливо, в деякому розширенні поля P) тоді і лише тоді, коли їхній результант $R(f, g)$ дорівнює 0.

Якщо від умов $a_n \neq 0$, $b_m \neq 0$ відмовитись, то рівність нулю результанта $R(f,g)$ залишається *необхідною* умовою того, щоб многочлени мали спільний корінь. Тому для розв'язання задачі пошуку параметрів λ, при яких многочлени $f(x)$ і $g(x)$ мають спільний корінь, необхідно:

1) Знайти всі значення параметра λ, при яких результант $R(f,g)$ рівний 0.
2) Для кожного із значень λ обчислити коефіцієнти a_n і b_m; при цьому:
   - якщо хоча б один із коефіцієнтів a_n або b_m – відмінний від 0, то $f(x)$ і $g(x)$ мають спільний корінь;
   - якщо $a_n = b_m = 0$, то потрібна додаткова безпосередня перевірка.

II. Пошук спільних коренів двох многочленів від багатьох змінних. Нехай $P[x_1, x_2, ..., x_n]$ – кільце многочленів від n змінних $x_1, x_2, ..., x_n$ над полем P, F – деяке розширення поля P. Говорять, що впорядкований набір $(c_1, c_2, ..., c_n)$ елементів $c_1, c_2, ..., c_n \in F$ є спільним коренем многочленів f_1, f_2,..., f_k із кільця $P[x_1, x_2, ..., x_n]$, якщо $(c_1, c_2, ..., c_n)$ є коренем кожного із многочленів f_i $(i \in \overline{1,k})$. Тому задача пошуку спільних коренів многочленів f_1, f_2,..., f_k – еквівалентна задачі пошуку розв'язків системи рівнянь:

$$\begin{cases} f_1(x_1, x_2, ..., x_n) &= 0, \\ f_2(x_1, x_2, ..., x_n) &= 0, \\ \dots & \dots \\ f_k(x_1, x_2, ..., x_n) &= 0. \end{cases}$$

У випадку многочленів f_i степеня $\geqslant 2$ побудувати загальну теорію достатньо важко. Для часткового випадку двох многочленів довільного степеня від двох змінних використовують *метод виключення змінної*.

Алгоритм методу виключення змінної

Нехай $f(x,y)$ і $g(x,y)$ – многочлени від двох змінних x і y над полем P.

1) Розглядаємо кожен із многочленів $f(x,y)$ і $g(x,y)$ як многочлен від однієї змінної (для цього впорядковуємо кожен із многочленів $f(x,y)$ і $g(x,y)$ за степенями цієї змінної). Нехай цією змінною вибрано x. Тоді матимемо:

$$\begin{aligned} F(x) &= a_n(y)x^n + a_{n-1}(y)x^{n-1} \dots + a_1(y)x + a_0(y), \\ G(x) &= b_m(y)x^m + b_{m-1}(y)x^{m-1} \dots + b_1(y)x + b_0(y), \end{aligned}$$

де $a_i(y), b_j(y) \in P[y]$ $(i = 0,1,...,n,\ j = 0,1,...,m)$, причому $a_n(y)$ і $b_m(y)$ не є нульмногочленами.

Слід зауважити, що змінну, за степенями якої впорядковуємо многочлени $f(x,y)$ і $g(x,y)$ *бажано* вибирати в такий спосіб, щоб старший коефіцієнт кожного із многочленів $F(x)$ і $G(x)$ був константою.

2) Знаходимо результант $R(y)$:

$$R(y) = \begin{vmatrix} a_n(y) & a_{n-1}(y) & a_{n-2}(y) & ... & \dots & a_1(y) & a_0(y) & 0 & ... & 0 & 0 \\ 0 & a_n(y) & a_{n-1}(y) & ... & \dots & a_2(y) & a_1(y) & a_0(y) & ... & 0 & 0 \\ \dots & \dots & \dots & ... & \dots & \dots & \dots & \dots & ... & \dots & \dots \\ 0 & 0 & 0 & ... & a_n(y) & a_{n-1}(y) & a_{n-2}(y) & a_{n-3}(y) & ... & a_1(y) & a_0(y) \\ b_m(y) & b_{m-1}(y) & b_{m-2}(y) & ... & b_1(y) & b_0(y) & 0 & 0 & ... & 0 & 0 \\ 0 & b_m(y) & b_{m-1}(y) & ... & b_2(y) & b_1(y) & b_0(y) & 0 & ... & 0 & 0 \\ \dots & \dots & \dots & ... & \dots & \dots & \dots & \dots & ... & \dots & \dots \\ 0 & 0 & 0 & ... & 0 & b_m(y) & b_{m-1}(y) & b_{m-2}(y) & ... & b_1(y) & b_0(y) \end{vmatrix}$$

побудований для $F(x)$ і $G(x)$ за тим же принципом, що результант. В розгорнутій формі цей визначник є деяким многочленом від змінної y.

3) Знаходимо всі корені y_0 многочлена $R(y)$.

4) Для кожного із коренів y_0 розглядаємо відповідні многочлени $F^{(0)}(x) = f(x, y_0)$ і $G^{(0)}(x) = g(x, y_0)$ від однієї змінної x і шукаємо їхні спільні корені. Це можна зробити наступним чином:

1 спосіб: знайти корені кожного із многочленів $F^0(x)$ і $G^0(x)$ окремо, серед них вибрати спільні;

2 спосіб: знайти корені найбільшого спільного дільника многочленів $F^{(0)}(x)$ і $G^{(0)}(x)$.

5) Записуємо всі спільні корені (x_0, y_0) многочленів $f(x, y)$ і $g(x, y)$.

При цьому можливі випадки:

Випадок 1. Многочлен $R(y)$ не є нуль-многочленом. Тоді кількість його коренів скінченна. Нехай y_0 – деякий із коренів.

Якщо відповідні цьому кореню y_0 многочлени $F^{(0)}(x)$ і $G^{(0)}(x)$ – обидва нульові, тоді довільний елемент $c \in P$ є їхнім спільним коренем, а значить, кожна пара (c, y_0) є спільним коренем многочленів $f(x, y)$ і $g(x, y)$. Отже, в цьому випадку, многочлени $f(x, y)$ і $g(x, y)$ мають безліч спільних коренів.

Якщо ж із відповідних кореню y_0 многочленів $F^{(0)}(x)$ і $G^{(0)}(x)$ принаймні один – відмінний від нуль-многочлена, то кількість спільних коренів многочленів $F^{(0)}(x)$ і $G^{(0)}(x)$ – скінченна, а отже, і кількість спільних коренів многочленів $f(x, y)$ і $g(x, y)$ також скінченна.

Випадок 2. Многочлен $R(y)$ є нуль-многочленом. Кількість його коренів y_0 нескінченна.

Якщо y_0 не є коренем многочленів $a_n(y)$ і $b_m(y)$ (а таких існує нескінченна кількість), то за твердженням 2 обов'язково знайдеться такий елемент x_0, що (x_0, y_0) – спільний корінь многочленів $f(x, y)$ і $g(x, y)$.

Елементів y_0, які є коренями многочленів $a_n(y)$ і $b_m(y)$ – скінченна кількість. Для кожного із них питання про те, чи знайдеться відповідний йому спільний корінь многочленів $f(x, y)$ і $g(x, y)$ зводиться до питання про існування спільних коренів відповідних многочленів $F^{(0)}(x)$ і $G^{(0)}(x)$.

Отже, в цьому випадку кількість розв'язків системи – нескінченна, проте потребують перевірки ті корені y_0 многочлена $R(y)$, що одночасно є і коренями многочленів $a_n(y)$ і $b_m(y)$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 47. Визначити, при яких значеннях a мають спільний корінь многочлени $f(x) = ax^2 - 3x - 4$ і $g(x) = a(a-1)x^3 + x^2 - ax - 2$ з кільця $\mathbb{R}[x]$.

Розв'язання. Відповідно до алгоритму (див. теоретичні відомості **I**), необхідно спочатку знайти всі значення параметра a, при яких результант $R(f, g)$ многочленів $f(x)$ і $g(x)$ рівний 0. Маємо:

$$R(f,g)=\begin{vmatrix} a & -3 & -4 & 0 & 0 \\ 0 & a & -3 & -4 & 0 \\ 0 & 0 & a & -3 & -4 \\ a(a-1) & 1 & -a & -2 & 0 \\ 0 & a(a-1) & 1 & -a & -2 \end{vmatrix} = -36a^4+70a^3-38a^2+4a.$$

Рівність $R(f,g)=0$ можлива лише у наступних випадках: $a_1=0$, $a_2=1$, $a_{3,4}=\frac{17}{36}\pm\frac{\sqrt{145}}{36}$.

При $a\in\{\frac{17}{36}+\frac{\sqrt{145}}{36},\frac{17}{36}-\frac{\sqrt{145}}{36}\}$ коефіцієнти a_2 і b_3 многочленів $f(x)$ і $g(x)$ – обидва відмінні від 0, тому многочлени $f(x)$ і $g(x)$ мають спільний корінь.

При $a=1$ коефіцієнт a_2 многочлена $f(x)$ відмінний від 0, а значить, і в цьому випадку многочлени $f(x)$ і $g(x)$ мають спільний корінь.

При $a=0$ коефіцієнти a_2 і b_3 многочленів $f(x)$ і $g(x)$ – обидва рівні 0. Це означає, що в цьому випадку многочлени $f(x)$ і $g(x)$ можуть як мати спільні корені, так і не мати. Потрібна додаткова перевірка. Маємо: $f(x)=-3x-4$, $g(x)=x^2-2$. Легко бачити, що многочлени $f(x)$ і $g(x)$ спільних коренів не мають.

Отже, многочлени $f(x)$ і $g(x)$ мають спільні корені лише при $a\in\{1,\frac{17}{36}\pm\frac{\sqrt{145}}{36}\}$.

Розв'язання в Maple. Для пошуку результанта двох многочленів $f(x)$ і $g(x)$ використовується команда **resultant(f,g,x)**:

```
> f:=a*x^2-3*x-4: g:=a*(a-1)*x^3+x^2-a*x-2:
> R:=resultant(f, g, x);
```

$$R := -36\,a^4+70\,a^3-38\,a^2+4\,a$$

Знайдемо корені результанта R:

```
> s:=solve(R,a);
```

$$s := 0,\ 1,\ \frac{17}{36}+\frac{\sqrt{145}}{36},\ \frac{17}{36}-\frac{\sqrt{145}}{36}$$

Далі задаємо коефіцієнти cf і cg многочленів $f(x)$ і $g(x)$

```
> cf:=lcoeff(f,x);
```

$$cf := a$$

```
> cg:=lcoeff(g,x);
```

$$cg := a\,(a-1)$$

і для кожного із 4-х знайдених значень a, при яких $R=0$, обчислюємо коефіцієнти cf і cg; якщо хоча б один із цих коефіцієнтів відмінний від 0,

то число a – шукане, якщо ж обидва коефіцієнти дорівнюють 0, то потрібна додаткова перевірка:

```
> for i from 1 to 4 do
    if subs({a=s[i]},cf)<>0 or subs({a=s[i]},cg)<>0 then
      print(s[i],"maut spilnyi korin")
    else print(s[i],"potribna perevirka")
    end if;
  end do;
```

$$0, \text{"}\textit{potribna perevirka}\text{"}$$
$$1, \text{"}\textit{maut spilnyi korin}\text{"}$$
$$\frac{17}{36}+\frac{\sqrt{145}}{36}, \text{"}\textit{maut spilnyi korin}\text{"}$$
$$\frac{17}{36}-\frac{\sqrt{145}}{36}, \text{"}\textit{maut spilnyi korin}\text{"}$$

Як бачимо, при $a \in \{1, \frac{17}{36} \pm \frac{\sqrt{145}}{36}\}$ многочлени $f(x)$ і $g(x)$ мають спільний корінь, при $a = 0$ потрібна перевірка.

При $a = 0$ розв'язуємо систему рівнянь $\begin{cases} f(x) = 0, \\ g(x) = 0. \end{cases}$

Маємо:

```
> solve({subs({a=0},1), subs({a=0},g)},x);
```

Дана система розв'язків не має, отже, многочлени $f(x)$ і $g(x)$ спільних коренів при $a = 0$ не мають.

Завдання 47. Визначити, при яких значеннях a мають спільний корінь многочлени $f(x)$ і $g(x)$ з кільця $\mathbb{R}[x]$, якщо:

47.1. $f(x) = (a-4)x^3 - 4x + 1$, $g(x) = (a-4)x + 4$.

47.2. $f(x) = x^3 + ax^2 - 20$, $g(x) = x^3 + ax - 14$.

47.3. $f(x) = ax^3 + 2x + 3$, $g(x) = ax^2 + 2ax - 3$.

47.4. $f(x) = (a-1)x^3 - a$, $g(x) = (a-1)x^2 - a$.

47.5. $f(x) = x^3 + 2ax - 2$, $g(x) = x^2 - 2a$.

47.6. $f(x) = (2a-1)x^2 + x + 3$, $g(x) = (2a-1)x^2 - 2$.

47.7. $f(x) = x^3 + (a+1)x - 2a$, $g(x) = x^2 + 3a$.

47.8. $f(x) = ax^3 - 4x + 1$, $g(x) = (2a-1)x^2 - 2$.

47.9. $f(x) = (a+1)x^3 + 1$, $g(x) = (a+1)x - 4$.

47.10. $f(x) = x^3 - ax + 2$, $g(x) = x^2 + ax + 2$.

47.11. $f(x) = x^2 + ax$,
$g(x) = x^3 + (3a-1)x - 4a$.

47.12. $f(x) = (a-1)x^2 - a$,
$g(x) = (a-1)x^- a$.

47.13. $f(x) = ax^2 + 5x + 2$,
$g(x) = ax^3 - 2x - 1$.

47.14. $f(x) = x^3 - 4x^2 + (a-5)x - 5a$,
$g(x) = ax^2 - (7+a)x + 7a$.

47.15. $f(x) = (a-1)x^2 + 5x - 3$,
$g(x) = (a-1)x^2 - 2$.

47.16. $f(x) = x^2 - 2ax$,
$g(x) = x^3 + 2ax - 2a$.

47.17. $f(x) = x^3 + (2a+1)x - a$,
$g(x) = x^2 + a$.

47.18. $f(x) = (a+1)x^2 + 1$,
$g(x) = (a+1)x^2 - 4$.

47.19. $f(x) = ax^3 + 2x + 3$,
$g(x) = ax^2 + 4x - 3$.

47.20. $f(x) = x^3 + ax + 1$,
$g(x) = x^2 + ax + 1$.

47.21. $f(x) = (a-1)x^2 + 3x - 2$,
$g(x) = (a-1)x^2 - 4$.

47.22. $f(x) = x^3 + 5x + 3a$,
$g(x) = x^2 - 2ax - 5$.

47.23. $f(x) = (a-1)x^3 + x + 3$,
$g(x) = (a-1)x^2 - 2$.

47.24. $f(x) = ax^3 + 2x + 3a$,
$g(x) = ax^2 - 1$.

47.25. $f(x) = (a+1)x^2 + 3ax - 2$,
$g(x) = (a+1)x^2 - 4$.

Приклад 48.1. Знайти спільні корені многочленів

$$\begin{aligned} f(x,y) &= x^2 - xy + x - y, \\ g(x,y) &= x^2y + x^2 - 2y \end{aligned}$$

із кільця $\mathbb{R}[x,y]$, розглядаючи їх як многочлени від змінної x над кільцем $\mathbb{R}[y]$.

Розв'язання. Розкладаючи дані многочлени за степенями змінної x, одержимо многочлени

$$\begin{aligned} F(x) &= x^2 + (1-y)x - y, \\ G(x) &= (y+1)x^2 - 2y, \end{aligned}$$

з коефіцієнтами із кільця $\mathbb{R}[y]$.

Знайдемо результант $R(y)$:

$$R(y) = \begin{vmatrix} 1 & 1-y & -y & 0 \\ 0 & 1 & 1-y & -y \\ y+1 & 0 & -2y & 0 \\ 0 & y+1 & 0 & -2y \end{vmatrix} = -y^4 + 3y^2 - 2y = -y(y-1)^2(y+2).$$

Многочлен $R(y)$ не є нуль-многочленом, тому маємо випадок 1). Коренями многочлена $R(y)$ є $0, 1, -2$. Оскільки жоден із цих коренів не є коренем многочленів $a_2(y) = 1$ і $b_2(y) = y + 1$, то кожному із них відповідатиме принаймні один спільний корінь многочленів $f(x, y)$ і $g(x, y)$.

При $y_0 = 0$ многочлени $F^{(0)}$ і $G^{(0)}$ мають вигляд: $F^{(0)} = x^2 + x$, $G^{(0)} = x^2$; їхнім спільним коренем є лише $x_0 = 0$. Отже, одним із спільних коренів многочленів $f(x, y)$ і $g(x, y)$ є $(0, 0)$.

При $y_0 = 1$ маємо: $F^0(x) = x^2 - 1$, $G^0(x) = 2x^2 - 2$. Ці многочлени мають два спільні корені $x_0 = 1$ і $x_0 = -1$. Одержали ще два спільних коренів многочленів $f(x, y)$ і $g(x, y)$: $(1, 1)$, $(-1, 1)$.

При $y_0 = -2$ маємо: $F^0(x) = x^2 + 3x + 2$, $G^0(x) = -x^2 + 4$. Спільним коренем є $x_0 = -2$. Тоді спільним коренем многочленів $f(x, y)$ і $g(x, y)$ буде $(-2, -2)$.

Таким чином, спільними коренями многочленів $f(x, y)$ і $g(x, y)$ є: $(0, 0)$, $(1, 1)$, $(-1, 1)$ і $(-2, -2)$.

Розв'язання в Maple. Для перевірки остаточного результату достатньо розв'язати в систему рівнянь $\begin{cases} x^2 - xy + x - y = 0, \\ x^2y + x^2 - 2y = 0. \end{cases}$

```
> solve({x^2-x*y+x-y,x^2*y+x^2-2*y},{x,y});
```

$\{x = -1, y = 1\}$, $\{x = 0, y = 0\}$, $\{x = -2, y = -2\}$, $\{x = 1, y = 1\}$

Покрокову перевірку здійснюємо, виконуючи всі дії в Maple. Для заданих многочленів $f(x)$ і $g(x)$ знаходимо результант $R(y)$:

```
> f:=x^2-x*y+x-y: g:=x^2*y+x^2-2*y:
> Ry:=resultant(f,g,x);
```

$$Ry := -y^4 + 3\,y^2 - 2\,y$$

та його корені:

```
> solve(Ry=0);
```

$$0,\ -2,\ 1,\ 1$$

Для кожного із коренів результанта знаходимо спільні корені многочленів $f(x)$ і $g(x)$. Нехай $y_0 = 0$:

```
> #y0=0
```

Знаходимо відповідні многочлени $F^(0)$ і $G^(0)$:

```
> f0:=subs({y=0},f); g0:=subs({y=0},g);
```

$$f0 := x^2 + x$$

$$g0 := x^2$$

```
> solve({f0,g0},x);
```

$$\{x = 0\}$$

Спільним коренем многочленів $F^{(}0)$ і $G^{(}0)$ є $x_0 = 0$. Тоді задані многочлени $f(x)$ і $g(x)$ мають спільний корінь $(0, 0)$.

Далі аналогічно при $y_0 = -2$ і $y_0 = 1$ отримуємо:

```
> #y0=-2
  f0:=subs({y=-2},f); g0:=subs({y=-2},g);
  solve({f0,g0},x);
```

$$f0 := x^2 + 3\,x + 2$$

$$g0 := -x^2 + 4$$

$$\{x = -2\}$$

Спільним коренем многочленів f і g є $(-2, -2)$.

```
> #y0=1
  f0:=subs({y=1},f); g0:=subs({y=1},g);
  solve({f0,g0},x);
```

$$f0 := x^2 - 1$$

$$g0 := 2\,x^2 - 2$$

$$\{x = 1\},\ \{x = -1\}$$

Спільними коренями многочленів f і g є також $(1, 1)$, $(-1, 1)$.

Приклад 48.2. Знайти спільні корені многочленів

$$\begin{aligned} f(x, y) &= (y-1)x^2 + 2x - 1 \quad \text{і} \\ g(x, y) &= (y-1)x^2 + 4 \end{aligned}$$

в полі $\mathbb{R}$ дійсних чисел.

Розв'язання. Знайдемо результант $R(y)$:

$$R(y) = \begin{vmatrix} y-1 & 2 & -1 & 0 \\ 0 & y-1 & 2 & -1 \\ y-1 & 0 & 4 & 0 \\ 0 & y-1 & 0 & 4 \end{vmatrix} = (y-1)(25y-9).$$

Коренями многочлена $R(y)$ є: 1 і $\frac{9}{25}$.

Оскільки корінь $y_0 = \frac{9}{25}$ не є коренем многочленів $a_2(y) = y - 1$ і $b_2(y) = y-1$, то йому відповідатиме принаймні один спільний корінь многочленів $f(x, y)$ і $g(x, y)$. Цей корінь знаходимо як і в попередньому прикладі, розглядаючи відповідні многочлени $F^{(0)} = -\frac{16}{25}x^2+2x-1$ і $G^{(0)} = -\frac{16}{25}x^2+4$. Їхнім спільним коренем є $x_0 = \frac{5}{2}$. Тоді спільним коренем многочленів $f(x, y)$ і $g(x, y)$ є: $(\frac{5}{2}, \frac{9}{25})$.

Корінь $y_0 = 1$ многочлена $R(y)$ є також і коренем многочленів $a_2(y) = y - 1$ і $b_2(y) = y - 1$, тому відповідний йому спільний корінь (або корені) многочленів $f(x, y)$ і $g(x, y)$ може як існувати, так і не існувати. Відповідні цьому кореню многочлени $F^{(0)}$ і $G^{(0)}$ мають вигляд $F^{(0)} = 2x - 1$, $G^{(0)} = 4$. Жоден із цих многочленів не є нульовим (достатньо було б, щоб хоча б один із цих многочленів був ненульовий), тому кількість їхніх спільних коренів (якщо вони існують), а значить, і спільних коренів многочленів $f(x, y)$ і $g(x, y)$ – скінченна. Оскільки многочлен $G^{(0)}$ взагалі коренів не має, то це означає, що і відповідного кореню $y_0 = 1$ спільного кореня многочленів $f(x, y)$ і $g(x, y)$ немає.

Зауваження. Зауважимо, що в цьому випадку зручніше було б розглядати $f(x, y)$ і $g(x, y)$ як многочлени від змінної y і шукати відповідний многочлен $R(x)$ (це був би визначник 2-го порядку).

Розв'язання в Maple. Перевіряємо отриману відповідь:

```
> solve({(y-1)*x^2+2*x-1,(y-1)*x^2+4},{x,y});
```

$$\{x = \frac{5}{2},\ y = \frac{9}{25}\}$$

Покрокова перевірка:

```
> f:=(y-1)*x^2+2*x-1: g:=(y-1)*x^2+4:
> Ry:=resultant(f,g,x);
```

$$Ry := 25\,y^2 - 34\,y + 9$$

```
> solve(Ry=0);
```

$$1,\ \frac{9}{25}$$

```
> #y0=1
  f0:=subs({y=1},f); g0:=subs({y=1},g); solve({f0,g0},x);
```

$$f0 := -1 + 2\,x$$

$$g0 := 4$$

Многочлени $F^{(0)}$ і $G^{(0)}$ спільних коренів не мають.

```
> #y0=9/25
  f0:=subs({y=9/25},f); g0:=subs({y=9/25},g); solve({f0,g0},x);
```

$$f0 := -\frac{16}{25}\,x^2 + 2\,x - 1$$

$$g0 := -\frac{16\,x^2}{25} + 4$$

$$\{x = \frac{5}{2}\}$$

Таким чином, многочлени f і g мають лише один спільний корінь: $(\frac{5}{2}, \frac{9}{25})$

Приклад 48.3. Знайти спільні корені многочленів

$$f(x,y) = x^2y^2 + 4y \qquad \text{і} \qquad g(x,y) = x^2y^3 - 2y$$

в полі $\mathbb{C}$.

Розв'язання. Знайдемо результант $R(y)$:

$$R(y) = \begin{vmatrix} y^2 & 0 & 4y & 0 \\ 0 & y^2 & 0 & 4y \\ y^3 & 0 & -2y & 0 \\ 0 & y^3 & 0 & -2y \end{vmatrix} = 4y^6(2y+1)^2.$$

Коренями многочлена $R(y)$ є: 0 і $-\frac{1}{2}$.

Оскільки корінь $y_0 = -\frac{1}{2}$ не є коренем многочленів $a_2(y) = y^2$ і $b_2(y) = y^3$, то за твердженням 2 йому відповідатиме принаймні один спільний корінь многочленів $f(x,y)$ і $g(x,y)$. Маємо: $F^0(x) = \frac{1}{4}x^2 - 2$, $G^0(x) = -\frac{1}{8}x^2 + 1$, звідки $x_0 = \pm\sqrt{8}$. Тоді спільний корінь многочленів $f(x,y)$ і $g(x,y)$ будуть: $(\sqrt{8}, -\frac{1}{2})$ і $(-\sqrt{8}, -\frac{1}{2})$.

Корінь $y_0 = 0$ многочлена $R(y)$ є також і коренем многочленів $a_2(y) = y^2$ і $b_2(y) = y^3$, тому відповідні йому спільні корені многочленів $f(x,y)$ і $g(x,y)$ можуть як існувати, так і не існувати. Відповідні цьому кореню многочлени $F^{(0)}$ і $G^{(0)}$ є нуль-многочленами, тому будь-який елемент $x_0 \in \mathbb{C}$, буде їхнім спільним коренем. Це означає, що спільними коренями многочленів $f(x,y)$ і $g(x,y)$ є кожен впорядкований набір виду $(x_0, 0)$ для всіх $x_0 \in \mathbb{C}$.

Таким чином, спільні корені многочленів $f(x,y)$ і $g(x,y)$: $(\sqrt{8}, -\frac{1}{2})$, $(-\sqrt{8}, -\frac{1}{2})$, $(x_0, 0)$ для всіх $x_0 \in \mathbb{C}$.

Розв'язання в Maple. Перевірка проміжних обчислень:

```
> f:=x^2*y^2+4*y: g:=x^2*y^3-2*y:
> Ry:=resultant(f,g,x);
```

$$Ry := y^4\,(-4\,y^2 - 2\,y)^2$$

```
> solve(Ry=0);
```

$$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ \frac{-1}{2},\ \frac{-1}{2}$$

```
> #y0=0
  f0:=subs({y=0},f); g0:=subs({y=0},g); solve({f0,g0},x);
```

$$f0 := 0$$
$$g0 := 0$$
$$\{x = x\}$$

Отже, спільними коренями многочленів f і g є $(x, 0)$, де $x \in \mathbb{R}$.

```
> #y0=-1/2
  f0:=subs({y=-1/2},f); g0:=subs({y=-1/2},g); solve({f0,g0},x);
```

$$f0 := \frac{x^2}{4} - 2$$

$$g0 := -\frac{x^2}{8} + 1$$

$$\{x = 2\,\mathrm{RootOf}(\_Z^2 - 2,\ label = \_L8)\}$$

Оскільки $\mathrm{RootOf}(\_Z^2 - 2) = \pm\sqrt{2}$, то спільними коренями многочленів f і g є також $(\pm 2\sqrt{2}, -\frac{1}{2})$.

Зауваження. При пошуку коренів результанта $R(y)$ (або $R(x)$) можна порекомендувати використання теоретичного матеріалу §5 розд.VI.

Завдання 48. Знайти спільні корені многочленів $f(x)$ і $g(x)$ з кільця $\mathbb{R}[x]$, якщо:

48.1. $f(x, y) = 30x^2 + 36xy + 11y^2 - 24x - 14y,$
$g(x, y) = 19x^2 + 28xy + 10y^2 - 10x - 8y.$

48.2. $f(x, y) = x^3 - 2x^2y - 4xy^2 + 2y^3 + 6x^2 + 12xy - 16x - 8y,$
$g(x, y) = -3x^3 - 4x^2y - 3xy^2 + 4y^3 + 2x^2 + 24xy - 10y^2 - 12x - 16y + 40.$

48.3. $f(x, y) = 2x^2 + 3xy - 2y^2 - 6x + 3y,$
$g(x, y) = 3x^2 + 7xy + 2y^2 - 7x + y - 6.$

48.4. $f(x, y) = -2x^2 + 4xy + 3y^2 + 24x + 6y - 24,$
$g(x, y) = 11x^2 + 20xy + 8y^2 - 6x - 12y - 8.$

48.5. $f(x, y) = 2y^2 + 2(x - 4)y + 12,$
$g(x, y) = -12y^2 - 12y(x - 4) - 12x^2 + 48x - 72.$

48.6. $f(x, y) = x^2 - 3xy + 2y^2 + x - y,$
$g(x, y) = 2x^2 - 3x + x^3 - 2xy + 3y - x^2y.$

48.7. $f(x, y) = 4x^2 - 7xy + y^2 + 13x - 2y - 3,$
$g(x, y) = 9x^2 - 14xy + y^2 + 28x - 4y - 5.$

48.8. $f(x, y) = 13x^2 + 10xy + 2y^2 - 4x - 2y + 1,$
$g(x, y) = -x^2 + 2xy + y^2 - 8x - 4y - 1.$

48.9. $f(x, y) = 2x^3 - 4x^2y - 2xy^2 - 12xy + 8x + y^3 + 6y^2 - 16y,$
$g(x, y) = 4x^3 - 3x^2y + 10x^2 - 4xy^2 - 24xy + 16x - 3y^3 + 2y^2 - 12y + 40.$

48.10. $f(x,y) = x^2 - 6xy - 16y^2 - 9x + 12y + 18,$
$g(x,y) = 12x^2 + 23xy - 2y^2 - 32x + 11y - 12.$

48.11. $f(x,y) = x^2 - 7xy + 4y^2 - 11x + 28y + 24,$
$g(x,y) = x^2 - 14xy + 9y^2 - 20x + 60y + 51.$

48.12. $f(x,y) = 8x^2 + 2xy + 20y^2 + 5x - 41y + 24 - 3x^3 - 3y^3,$
$g(x,y) = x^2 + 5xy - 7y^2 - 16x + 2y + 3 + 2x^3 + 2y^3.$

48.13. $f(x,y) = x^2 + y^2 - x - 3y,$
$g(x,y) = x^2 - 6xy - y^2 + 11x + 7y - 12.$

48.14. $f(x,y) = x^2 - 7xy + 10y^2 + x - 5y,$
$g(x,y) = 3x^2 - 4x + x^3 - 15xy + 20y - 5x^2y.$

48.15. $f(x,y) = x^3 - 4x^2 + 6x - 3xy^2 + 4y^2 - 4,$
$g(x,y) = -3x^2y + 8xy + y^3 - 6y.$

48.16. $f(x,y) = 16x^2 + 4x + 12x^3 - 4xy - y - 3x^2y,$
$g(x,y) = 12x^2 - 7xy + y^2 + 8x - 2y.$

48.17. $f(x,y) = 5x^2 - 6xy + 5y^2 - 16,$
$g(x,y) = x^2 - xy + 2y^2 - x - y - 4.$

48.18. $f(x,y) = 6x^2 - 7xy + 9x + 2y^2 - 5y + 3,$
$g(x,y) = 4x^2 - y^2 + 2y - 1.$

48.19. $f(x,y) = x^4 - 6x^2y^2 + y^4 + 6x^3 - 12xy^2 + 13x^2 - 6y^2 + 14x + 6,$
$g(x,y) = x^3 - xy^2 + 5x^2 - y^2 + 7x + 3.$

48.20. $f(x,y) = 12x^2 - 7xy + 11x + y^2 - 3y + 2,$
$g(x,y) = 28x^2 + 11x - 7xy - y + 1.$

48.21. $f(x,y) = x^2 + xy - x + y,$
$g(x,y) = x^2y + x^2 + 2y.$

48.22. $f(x,y) = 19x^2 - 27xy + 22y^2 + 3x + 3y - 68,$
$g(x,y) = -12x^2 + 27xy - 21y^2 - 9x - 9y + 60.$

48.23. $f(x,y) = x^2 - 2y^2 + 2xy - 1,$
$g(x,y) = 2x^2 + y^2 - xy - x + 2y - 3.$

48.24. $f(x,y) = x^2 + xy - 4x + y^2 - 2y + 3,$
$g(x,y) = x^3 - 5x^2 + xy + 7x + y^3 - y^2 - 5y - 3.$

48.25. $f(x,y) = x^2y + 3xy + 2y + 3,$
$g(x,y) = 2xy - 2x + 2y + 3.$

Розділ VI

Многочлени над числовими полями

1. Многочлени над полем $\mathbb{C}$ комплексних чисел

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорема. *Нехай* $f(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 \in \mathbb{C}[z]$, $n \geqslant 1$. *Тоді* $f(z)$ *має хоча б один комплексний корінь.*

Тому незвідними над полем $\mathbb{C}$ є тільки многочлени першого степеня, а кожен многочлен n-го степеня над полем $\mathbb{C}$ єдиним чином розкладається над цим полем в добуток лінійних множників:

$$f(z) = a_n(z - z_1)(z - z_2)\ldots(z - z_n),$$

де $z_1, z_2, \ldots, z_n$ – корені многочлена $f(z)$. Отже, поле $\mathbb{C}$ є алгебраїчно замкненим, і для коренів многочлена $f(z)$ у полі $\mathbb{C}$ справедливі формули Вієта:

$$\begin{aligned} z_1 + z_2 + \ldots + z_n &= -\frac{a_{n-1}}{a_n}, \\ z_1z_2 + z_1z_3 + \ldots + z_{n-1}z_n &= \frac{a_{n-2}}{a_n}, \\ \ldots\ldots\ldots &\ \ldots\ldots \\ z_1z_2\ldots z_n &= (-1)^n\frac{a_0}{a_n}. \end{aligned}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 49. Знайти суму квадратів S_2 і суму кубів S_3 коренів многочлена

$$f(x) = x^4 - 3x^2 + 2x + 3. \tag{VI.1}$$

Розв'язання. Нехай x_1, x_2, x_3, x_4 – корені многочлена $f(x)$. Використаємо формули (V.3):

$$\begin{aligned} S_2 &= \sigma_1^2 - 2\sigma_2, \\ S_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \end{aligned}$$

За теоремою Вієта для коренів многочлена $f(x)$ справедливі співвідношення:

$$\begin{cases} x_1+x_2+x_3+x_4=0, \\ x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4=-3, \\ x_1x_2x_3+x_1x_3x_4+x_1x_2x_4+x_2x_3x_4=-2, \\ x_1x_2x_3x_4=3; \end{cases} \quad \text{тобто} \quad \begin{cases} \sigma_1=0, \\ \sigma_2=-3, \\ \sigma_3=-2, \\ \sigma_4=3; \end{cases}$$

а тому

$$S_2=6,$$
$$S_3=-6.$$

Розробка процедур. Створимо процедури **rootsSquares** і **rootsCubes** для пошуку квадратів і кубів коренів многочлена відповідно.

Нехай $n=\deg f$. Знаходимо значення елементарних симетричних многочленів $\sigma_1,\sigma_2,\sigma_3$ в точці $(c_1,c_2,...,c_n)$ (використовуючи теорему Вієта):

```
> for i from 1 to t do
  sigma[i]:=(-1)^i*coeff(f,x,n-i)/coeff(f,x,n); end do;
```

(при $t=2$ або $t=3$ відповідно) і обчислюємо суми квадратів і кубів коренів (використовуючи формули (V.3)):

```
> s2:=sigma[1]^2-2*sigma[2];
  s3:=sigma[1]^3-3*sigma[1]*sigma[2]+3*sigma[3];
```

Коди процедур наступні:

```
rootsSquares:=proc(f)
local i,s2,n,sigma;
   n:=degree(f);
   for i from 1 to 2 do
      sigma[i]:=(-1)^i*coeff(f,x,n-i)/coeff(f,x,n);
   end do;
   s2:=sigma[1]^2-2*sigma[2];
end proc:
```

```
rootsCubes:=proc(f)
local i,s3,n,sigma;
   n:=degree(f);
   for i from 1 to 3 do
      sigma[i]:=(-1)^i*coeff(f,x,n-i)/coeff(f,x,n);
   end do;
   s3:=sigma[1]^3-3*sigma[1]*sigma[2]+3*sigma[3];
end proc:
```

Розв'язання в Maple. Використовуємо створені процедури:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Сума квадратів коренів:

```
> rootsSquares(x^4-3*x^2+2*x+3);
```

$$6$$

Сума кубів коренів:

```
> rootsCubes(x^4-3*x^2+2*x+3);
```

$$-6$$

Завдання 49. Знайти суму квадратів і суму кубів коренів многочлена $f(x)$, якщо:

45.1. $f(x) = x^5 - x^4 + 3x^2 + x - 1$.

49.2. $f(x) = x^5 + x^4 - 2x^3 - x^2 - 1$.

49.3. $f(x) = x^5 - x^4 + x^3 - x^2 - 2$.

49.4. $f(x) = x^5 - 3x^3 + x^2 - 1$.

49.5. $f(x) = x^5 - x^3 + 2x^2 + x - 1$.

49.6. $f(x) = x^5 - x^4 - x^2 - 1$.

49.7. $f(x) = x^5 + x^4 + x^2 - 1$.

49.8. $f(x) = x^5 - x^4 + 2x^3 - x + 1$.

49.9. $f(x) = x^5 + x^3 + 2x - 1$.

49.10. $f(x) = x^5 - x^3 - x^2 - 3$.

49.11. $f(x) = x^5 + x^4 - 2x^3 + x$.

49.12. $f(x) = x^5 - 2x^4 + 3x^3 - 2$.

49.13. $f(x) = x^5 - x^4 + 2x^2 - x - 1$.

49.14. $f(x) = x^5 + x^3 - 2x^2 + 3$.

49.15. $f(x) = x^5 - 3x^2 + 2x - 5$.

49.16. $f(x) = x^5 - x^4 + 3x^3 - 2x^2 + 4$.

49.17. $f(x) = x^5 + x^4 + x^3 - 1$.

49.18. $f(x) = x^5 - x^3 + x^2 - 2$.

49.19. $f(x) = x^5 + 2x^4 - 2x^3 + 2x - 1$.

49.20. $f(x) = x^5 - 4x^4 - 3x^2 + 1$.

49.21. $f(x) = x^5 + 3x^3 + x^2 + 2x - 1$.

49.22. $f(x) = x^5 - x^3 + x^2 - x - 1$.

49.23. $f(x) = x^5 + x^4 - 3x^2 + 2x + 1$.

49.24. $f(x) = x^5 - x^4 + x + 3$.

49.25. $f(x) = x^5 - x^4 + x^3 + 2x - 1$.

Приклад 50. Знайти нормовані многочлени $g_1(x)$ і $g_2(x)$, коренями яких є відповідно квадрати і куби коренів многочлена $f(x) = x^3 - 6x^2 + 5x + 1$ з кільця $\mathbb{Q}[x]$.

Розв'язання. Нехай x_1, x_2, x_3 – корені многочлена $f(x)$. Тоді, за теоремою Вієта, $\sigma_1 = x_1 + x_2 + x_3 = 6$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = 5$, $\sigma_3 = x_1x_2x_3 = -1$.

Коренями многочлена $g_1(x)$ є: x_1^2, x_2^2, x_3^2, коренями многочлена $g_2(x)$: x_1^3, x_2^3, x_3^3. Нехай $g_1(x) = x^3 + a_2x^2 + a_1x + a_0$. Тоді, за теоремою Вієта,

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= -a_2, \\ x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 &= a_1, \\ x_1^2x_2^2x_3^2 &= -a_0. \end{aligned}$$

Звідси

$$\begin{aligned} a_2 &= -(x_1^2 + x_2^2 + x_3^2) = -(\sigma_1^2 - 2\sigma_2) = -(6^2 - 2\cdot 5) = -26, \\ a_1 &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = (x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2 = \\ &= (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2(x_1x_2x_1x_3 + x_1x_2x_2x_3 + x_1x_3x_2x_3) = \\ &= \sigma_2^2 - 2\sigma_3\sigma_1 = 5^2 - 2\cdot(-1)\cdot 6 = 37, \\ a_0 &= -x_1^2x_2^2x_3^2 = -(x_1x_2x_3)^2 = -\sigma_3^2 = -1, \end{aligned}$$

тобто $g_1(x) = x^3 - 26x^2 + 37x - 1$.

Аналогічно для многочлена $g_2(x) = x^3 + b_2x^2 + b_1x + b_0$ одержимо:

$$\begin{aligned} b_2 &= -(x_1^3 + x_2^3 + x_3^3) = -(\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3) = -(6^3 - 3\cdot 6\cdot 5 + 3(-1)) = -123, \\ b_1 &= x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 = (x_1x_2)^3 + (x_1x_3)^3 + (x_2x_3)^3 = \\ &= (x_1x_2 + x_1x_3 + x_2x_3)^3 - 3(x_1x_2 + x_1x_3 + x_2x_3)\cdot \\ &\quad \cdot(x_1x_2x_1x_3 + x_1x_2x_2x_3 + x_1x_3x_2x_3) + 3(x_1x_2x_1x_3x_2x_3) = \\ &= \sigma_2^3 - 3\sigma_2\sigma_3\sigma_1 + 3\sigma_3^2 = 5^3 - 3\cdot 5\cdot(-1)\cdot 6 + 3\cdot(-1)^2 = 218, \\ b_0 &= -x_1^3x_2^3x_3^3 = -\sigma_3^3 = -(-1)^3 = 1. \end{aligned}$$

Отже, $g_2(x) = x^3 - 123x^2 + 218x + 1$.

Розв'язання в Maple. Знаходимо значення елементарних симетричних многочленів $\sigma_1, \sigma_2, \sigma_3$ від коренів многочлена $f(x)$:

```
> f:=x^3-6*x^2+5*x+1:
> n:=degree(f);
```

$$n := 3$$

```
> for i from 1 to n do
    sigma[i]:=(-1)^i*coeff(f,x,n-i)/coeff(f,x,n);
  end do;
```

$$\sigma_1 := 6$$

$$\sigma_2 := 5$$

$$\sigma_3 := -1$$

Далі обчислюємо коефіцієнти шуканого многочлена $g_1(x)$:

```
> a2:=-(sigma[1]^2-2*sigma[2]);
```

$$a2 := -26$$

```
> a1:=(sigma[2]^2-2*sigma[3]*sigma[1]);
```

$$a1 := 37$$

```
> a0:=-sigma[3]^2;
```

$$a0 := -1$$

Отже,

```
> g1:=x^3+a2*x^2+a1*x+a0;
```

$$g1 := x^3 - 26\,x^2 + 37\,x - 1$$

Аналогічно для многочлена $g_2(x)$:

```
> b2:=-(sigma[1]^3-3*sigma[1]*sigma[2]+3*sigma[3]);
```

$$b2 := -123$$

```
> b1:=sigma[2]^3-3*sigma[2]*sigma[3]*sigma[1]+3*sigma[3]^2;
```

$$b1 := 218$$

```
> b0:=-sigma[3]^3;
```

$$b0 := 1$$

```
> g2:=x^3+b2*x^2+b1*x+b0;
```

$$g2 := x^3 - 123\,x^2 + 218\,x + 1$$

Завдання 50. Знайти нормовані многочлени $g_1(x)$ і $g_2(x)$, коренями яких є відповідно квадрати і куби коренів многочлена $f(x)$ з кільця $\mathbb{Q}[x]$, якщо:

50.1. $f(x) = x^3 - 2x^2 + 4$.

50.2. $f(x) = x^3 + 7x^2 - 2x + 1$.

50.3. $f(x) = x^3 + +3x - 5$.

50.4. $f(x) = x^3 + 4x^2 + 7x - 3$.

50.5. $f(x) = x^3 - 2x^2 + x + 4$.

50.6. $f(x) = x^3 + 4x - 4$.

50.7. $f(x) = x^3 + x^2 - 3x + 5$.

50.8. $f(x) = x^3 - 6x^2 + 3$.

50.9. $f(x) = x^3 + 2x^2 - 7x + 4$.

50.10. $f(x) = x^3 - 7x + 5$.

50.11. $f(x) = x^3 + 11x^2 - 2x + 6$.

50.12. $f(x) = x^3 + 13x^2 - 2$.

50.13. $f(x) = x^3 + 7x^2 - 11x + 8$.

50.14. $f(x) = x^3 + x^2 - 13$.

50.15. $f(x) = x^3 - 4x^2 + 2x - 11$.

50.16. $f(x) = x^3 + 2x^2 - 5x + 11$.

50.17. $f(x) = x^3 - 5x^2 + 6x + 10$.

50.18. $f(x) = x^3 + 9x^2 - 4x + 1$.

50.19. $f(x) = x^3 - 3x^2 + 7x - 2$.

50.20. $f(x) = x^3 + 11x^2 - 3$.

50.21. $f(x) = x^3 - 14x + 12$.

50.22. $f(x) = x^3 + 3x^2 - 2x + 5$.

50.23. $f(x) = x^3 - x^2 + 5x - 7$.

50.24. $f(x) = x^3 + 2x^2 - 5x + 3$.

50.25. $f(x) = x^3 - 6x^2 + 4x - 3$.

Приклад 51.1. Розв'язати рівняння: $x^3 - 3x^2 - 10x + a = 0$, якщо його корені x_1, x_2 задовольняють умову

$$2x_1 + x_2 = 1. \tag{VI.2}$$

Розв'язання. Для коренів многочлена $f(x) = x^3 - 3x^2 - 10x + a$ справедливі формули Вієта:

$$\begin{cases} x_1 + x_2 + x_3 = 3, \\ x_1x_2 + x_1x_3 + x_2x_3 = -10, \\ x_1x_2x_3 = -a. \end{cases} \tag{VI.3}$$

Із умови (VI.2) знайдемо

$$x_2 = 1 - 2x_1$$

і підставимо в перше рівняння системи (VI.3):

$$x_1 + (1 - 2x_1) + x_3 = 3,$$

звідки

$$x_3 = 2 + x_1.$$

Підставимо тепер вирази для x_2 і x_3 в друге рівняння системи (VI.3):

$$x_1(1 - 2x_1) + x_1(2 + x_1) + (1 - 2x_1)(2 + x_1) = -10,$$

$$x_1^2 = 4.$$

звідки

$$x_1 = 2 \quad \text{або} \quad x_1 = -2.$$

Тоді розв'язками системи рівнянь (VI.3), а отже, і заданого рівняння, є

$$\begin{cases} x_1 = 2, \\ x_2 = -3, \\ x_3 = 4; \end{cases} \quad \text{або} \quad \begin{cases} x_1 = -2, \\ x_2 = 5, \\ x_3 = 0; \end{cases}$$

при $a = 24$ і $a = 0$ відповідно.

Розв'язання в Maple. Задаємо многочлен:

```
> f:=x^3-3*x^2-10*x+a:
```

Далі розв'язуємо систему рівнянь, до системи (VI.3) додаючи ще співвідношення (VI.2)):

```
> solve({x1+x2+x3=3,x1*x2+x1*x3+x2*x3=-10,x1*x2*x3=-a,
  2*x1+x2=1},{x1,x2,x3,a});
```

$\{a = 24,\ x1 = 2,\ x2 = -3,\ x3 = 4\},\ \{a = 0,\ x1 = -2,\ x2 = 5,\ x3 = 0\}$

Таким чином, при $a = 24$ задане рівняння має розв'язки $x_1 = 2, x_2 = -3, x_3 = 4$; при $a = 0$: $x_1 = -2, x_2 = 5, x_3 = 0$.

Приклад 51.2. Розв'язати рівняння: $x^3 - 20x^2 + ax + b = 0$ і знайти коефіцієнти $a, b \in \mathbb{C}$, якщо його розв'язки x_1, x_2, x_3 задовольняють умову $x_1 : x_2 : x_3 = 2 : 3 : 5$.

Розв'язання. Для коренів $f(x) = x^3 - 20x^2 + ax + b$ справедливі формули Вієта:

$$\begin{cases} x_1 + x_2 + x_3 = 20, \\ x_1x_2 + x_1x_3 + x_2x_3 = a, \\ x_1x_2x_3 = -b. \end{cases} \tag{VI.4}$$

Нехай k – коефіцієнт пропорційності, тоді $x_1 = 2k$, $x_2 = 3k$, $x_3 = 5k$. Підставивши x_1, x_2, x_3 в систему (VI.4), отримаємо:

$$\begin{cases} 2k + 3k + 5k = 20, \\ 2k \cdot 3k + 2k \cdot 5k + 3k \cdot 5k = a, \\ 2k \cdot 3k \cdot 5k = -b, \end{cases} \quad \text{тобто} \quad \begin{cases} 10k = 20, \\ 31k^2 = a, \\ 30k^3 = -b. \end{cases}$$

Із першого рівняння знаходимо $k = 2$, тоді $a = 31 \cdot 2^2 = 124$, $b = -30 \cdot 2^3 = -240$. Тепер знаходимо розв'язки рівняння: $x_1 = 2 \cdot 2 = 4$, $x_2 = 3 \cdot 2 = 6$, $x_1 = 5 \cdot 2 = 10$.

Розв'язання в Maple. Розв'язання аналогічне до попереднього прикладу. Лише співвідношення для коренів рівняння слід буде переписати у вигляді: $x_1 = 1k$, $x_2 = 2k$, $x_3 = 4k$, де k – коефіцієнт пропорційності. Маємо:

```
> f:=x^3-20*x^2+a*x+b:
> solve({x1+x2+x3=20,x1*x2+x1*x3+x2*x3=a,x1*x2*x3=-b,
  x1=2*k, x2=3*k,x3=5*k},{x1,x2,x3,a,b,k});
```

$\{a = 124,\ b = -240,\ k = 2,\ x1 = 4,\ x2 = 6,\ x3 = 10\}$

Отже, задане рівняння має розв'язки $x_1 = 4, x_2 = 6, x_3 = 10$, при цьому $a = 124$, $b = -240$.

Приклад 51.3. Знайти нормований многочлен 3-го степеня, корені якого x_1, x_2, x_3 задовольняють умови $\begin{cases} \frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3}=1, \\ \frac{1}{x_1x_2}+\frac{1}{x_1x_3}+\frac{1}{x_2x_3}=\frac{11}{6}, \\ x_1x_2x_3=6. \end{cases}$

Розв'язання. Зрозуміло, що $x_i \neq 0$, $i = 1, 2, 3$. Домножимо обидві частини першого і другого рівнянь на добуток $x_1x_2x_3$. Отримаємо систему: $\begin{cases} x_2x_3+x_1x_3+x_1x_2=x_1x_2x_3, \\ x_3+x_2+x_3=\frac{11}{6}x_1x_2x_3, \\ x_1x_2x_3=6; \end{cases}$ звідки $\begin{cases} x_2x_3+x_1x_3+x_1x_2=6, \\ x_3+x_2+x_3=11, \\ x_1x_2x_3=6. \end{cases}$
За теоремою Вієта, x_1, x_2, x_3 є коренями многочлена $f(x) = x^3-6x^2+11x-6$.

Розв'язання в Maple. За допомогою Maple можна розв'язати систему рівнянь:

```
> solve({1/x1+1/x2+1/x3=11/6,1/(x1*x2)+1/(x1*x3)+1/(x2*x3)=1,
  x1*x2*x3=6}, {x1,x2,x3});
```

$\{x1 = 3, x2 = 2, x3 = 1\}$, $\{x1 = 2, x2 = 3, x3 = 1\}$, $\{x1 = 3, x2 = 1, x3 = 2\}$, $\{x1 = 1, x2 = 3, x3 = 2\}$, $\{x1 = 2, x2 = 1, x3 = 3\}$, $\{x1 = 1, x2 = 2, x3 = 3\}$
і знайти корені шуканого многочлена $f(x)$: $x_1 = 1$, $x_2 = 2$, $x_3 = 3$:

```
> x1:=1: x2:=2: x3:=3:
```

Знаходимо коефіцієнти шуканого многочлена f:

```
> a2:=-(x1+x2+x3); a1:=x1*x2+x1*x3+x2*x3; a0:=-x1*x2*x3;
```

$$a2 := -6$$
$$a1 := 11$$
$$a0 := -6$$

```
> f:=x^3+a2*x^2+a1*x+a0;
```

$$f := x^3 - 6\,x^2 + 11\,x - 6$$

Завдання 51.

51.1. Розв'язати рівняння: $x^3+4\sqrt{2}x^2+2x+a=0$, якщо один із його коренів більше від іншого на $\sqrt{2}$.

51.2. Розв'язати рівняння: $x^3-12x^2+43x-52=0$, якщо його корені утворюють арифметичну прогресію.

51.3. Розв'язати рівняння: $4x^3-20x^2+x+a=0$, якщо його корені x_1, x_2 задовольняють умову $3x_1+x_2=-2$.

51.4. Розв'язати рівняння: $x^3-20x^2+ax+b=0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1 : x_2 : x_3 = 2 : 3 : 5$.

51.5. Один із коренів многочлена $f(x) = x^3 - 7x + a$ дорівнює подвоєному другому. Знайти $f(x)$ і його корені.

51.6. Розв'язати рівняння: $x^3 + (3i+2)x^2 + 2(3i+2)x + 8 = 0$, якщо його корені утворюють геометричну прогресію.

51.7. Розв'язати рівняння: $x^3 - 17x^2 + ax + b = 0$, якщо його другий корінь на 1 більший за перший, а третій – вдвічі більший за перший.

51.8. Розв'язати рівняння: $x^3 + (4\sqrt{2}-1)x^2 + (2-\sqrt{2})^2 x - 6 = 0$, якщо його корені x_1, x_2 задовольняють умову $5x_1 - 2x_2 = \sqrt{2}$.

51.9. Розв'язати рівняння: $x^3 + 3\sqrt{3}x^2 + a = 0$, якщо два його корені співпадають.

51.10. Розв'язати рівняння: $x^3 - 3\sqrt{3}x^2 + 7x - \sqrt{3} = 0$, якщо його корені утворюють арифметичну прогресію.

51.11. Знайти нормований многочлен 3-го степеня, корені якого x_1, x_2, x_3 задовольняють умови $\begin{cases} \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = 1, \\ \frac{1}{x_1x_2} + \frac{1}{x_1x_3} + \frac{1}{x_2x_3} = \frac{11}{36}, \\ x_1x_2x_3 = 36. \end{cases}$

51.12. Розв'язати рівняння: $x^3 + (1-3\sqrt{3})x^2 - 3\sqrt{3}x + 6x + 6 = 0$, якщо його корені x_1, x_2 задовольняють умову $6x_1 - x_2 = 4\sqrt{3}$.

51.13. Розв'язати рівняння: $x^3 - 2(2+\sqrt{3}i)x^2 + 4\sqrt{3}(2i-\sqrt{3})x + 24\sqrt{3}i = 0$, якщо його корені утворюють геометричну прогресію.

51.14. Розв'язати рівняння: $x^3 + ax - 30 = 0$, якщо його корені x_1, x_2 задовольняють умову $x_1x_2 = 6$.

51.15. Розв'язати рівняння: $x^3 - i\sqrt{3}x^2 + 12x + a = 0$, якщо два його корені комплексно спряжені.

51.16. Розв'язати рівняння: $x^3 - 9ix^2 - 14x + a = 0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1 - 2x_2 = x_3$.

51.17. Розв'язати рівняння: $x^3 - 8ix^2 - 19x + a = 0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1 : x_2 : x_3 = 1 : 3 : 4$.

51.18. Розв'язати рівняння: $x^3 - 31ix^2 - 155x + 125i = 0$, якщо його корені утворюють геометричну прогресію.

51.19. Один із коренів многочлена $f(x) = x^3 - 13x^2 + 33x + a$ дорівнює потроєному другому. Знайти $f(x)$ і його корені.

51.20. Розв'язати рівняння: $x^3 - 2\sqrt{2}x^2 - 10x + a = 0$, якщо його корені x_1, x_2 задовольняють умову $x_1 - 2x_2 = 5\sqrt{2}$.

51.21. Розв'язати рівняння: $x^3 - 4x^2 - 47x + a = 0$, якщо його корені x_1, x_2 задовольняють умову $2x_1 + x_2 = -4$.

51.22. Розв'язати рівняння: $x^3 - 9\sqrt{2}x^2 + 52x - 48\sqrt{2} = 0$, якщо його корені утворюють арифметичну прогресію.

51.23. Розв'язати рівняння: $x^3 - x^2 + ax - 36 = 0$, якщо його корені x_1, x_2, x_3 задовольняють умову $x_1x_2 = x_3$.

51.24. Розв'язати рівняння: $x^3 + (2 - 3i)x^2 - (6i + 8)x + a = 0$, якщо один із його коренів більший від другого на 6.

51.25. Знайти многочлен 3-го степеня зі старшим коефіцієнтом рівним 2, корені якого x_1, x_2, x_3 задовольняють умови $\begin{cases} \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = -\frac{1}{6}, \\ x_1^2 + x_2^2 + x_3^2 = 14, \\ x_1x_2x_3 = -6. \end{cases}$

2. Многочлени над полем $\mathbb{R}$ дійсних чисел

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорема. *Нехай $f(z) = a_nz^n + a_{n-1}z^{n-1} + \ldots + a_1z + a_0 \in \mathbb{R}[z]$. Якщо комплексне число z_0 є коренем многочлена $f(z)$, то спряжене комплексне число $\overline{z_0}$ також є коренем цього многочлена. Крім того, якщо комплексне число z_0 є коренем k-ї кратності многочлена $f(z)$, то спряжене комплексне число $\overline{z_0}$ також є коренем тієї самої кратності.*

Кожен многочлен з дійсними коефіцієнтами, степінь якого більше 2, є звідним над полем $\mathbb{R}$. Кожен многочлен з дійсними коефіцієнтами єдиним чином розкладається над полем $\mathbb{R}$ в добуток лінійних множників і незвідних над $\mathbb{R}$ квадратних тричленів:

$$f(z) = a_n(z - z_0)^{k_1} \ldots (z - z_l)^{k_l}(z^2 + p_{l+1}z + g_{l+1})^{k_{l+1}} \ldots (z^2 + p_mz + g_m)^{k_m}.$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 52. Розв'язати рівняння: $x^4 - 5x^3 + 18x^2 - 34x + 20 = 0$, якщо $x_1 = 1 + 3i$.

Розв'язання. Задане рівняння має дійсні коефіцієнти, тому число $1 - 3i$ також є його коренем. Тоді многочлен $f(x) = x^4 - 5x^3 + 18x^2 - 34x + 20$ ділиться на двочлени $x - (1 + 3i)$ і $x - (1 - 3i)$, які є взаємно простими, а отже, ділиться і на їхній добуток $(x - (1 + 3i))(x - (1 - 3i)) = x^2 - 2x + 10$. Виконаємо ділення „кутом":

$$\begin{array}{r|l} x^4 - 5x^3 + 18x^2 - 34x + 20 & x^2 - 2x + 10 \\ \cline{2-2} \underline{x^4 - 2x^3 + 10x^2} & x^2 - 3x + 2 \\ -3x^3 + 8x^2 - 34x + 20 & \\ \underline{-3x^3 + 6x^2 - 30x} & \\ 2x^2 - 4x + 20 & \\ \underline{2x^2 - 4x + 20} & \\ 0 & \end{array}$$

Таким чином, $f(x) = \left(x^2 - 2x + 10\right)(x^2 - 3x + 2)$. Щоб знайти решту коренів заданого рівняння, розв'яжемо рівняння: $x^2 - 3x + 2 = 0$. Маємо: $x = 2$, $x = 1$. Отже, корені заданого рівняння:

$$x_1 = 1 + 3i, \quad x_2 = 1 - 3i, \quad x_3 = 2, \quad x_4 = 1.$$

Розв'язання в Maple. Для перевірки достатньо розв'язати рівняння:

```
> solve(x^4-5*x^3+18*x^2-34*x+20=0,x);
```

$$1,\ 2,\ 1 + 3\,I,\ 1 - 3\,I$$

Завдання 52. Розв'язати рівняння:

52.1. $x^4 + 5x^3 + 6x^2 + 10x - 100 = 0$,
якщо $x_1 = -1 + 3i$.

52.2. $x^4 + 2x^3 - 25x^2 + 64x - 42 = 0$,
якщо $x_1 = 2 + \sqrt{2}i$.

52.3. $x^4 + 3x^2 - 6x + 10 = 0$,
якщо $x_1 = 1 - i$.

52.4. $x^4 + (2\sqrt{3} - 2)x^3 + (9 - 4\sqrt{3})x^2 + (10\sqrt{3} - 8)x + 20 = 0$,
якщо $x_1 = -\sqrt{3} - i$.

52.5. $x^4 - 10x^3 + 45x^2 - 98x + 98 = 0$,
якщо $x_1 = 3 + \sqrt{5}i$.

52.6. $x^4 + 5x^3 - 5x^2 - 35x + 34 = 0$,
якщо $x_1 = -4 + i$.

52.7. $x^4 + 4x^3 + 16x^2 + 24x + 20 = 0$,
якщо $x_1 = -1 - i$.

52.8. $x^4 - 2x^3 - 12x^2 + 32x - 64 = 0$,
якщо $x_1 = 1 + \sqrt{3}i$.

52.9. $x^4 + (2\sqrt{5} - 4)x^3 + (11 - 8\sqrt{5})x^2 - (24 + 10\sqrt{5})x + 30 = 0$,
якщо $x_1 = 2 - i$.

52.10. $x^4 - x^2 - 6\sqrt{3}x + 28 = 0$,
якщо $x_1 = -\sqrt{3} + 2i$.

52.11. $x^4 - 5x^3 - 2x^2 + 14x - 20 = 0$,
якщо $x_1 = 1 + i$.

52.12. $x^4 - 2\sqrt{2}x^3 - 6x^2 + 18\sqrt{2}x - 27 = 0$,
якщо $x_1 = \sqrt{2} + i$.

52.13. $x^4 + 2x^3 + 2x^2 + 10x + 25 = 0$,
якщо $x_1 = 1 - 2i$.

52.14. $x^4 - 11x^3 + 50x^2 - 134x + 220 = 0$,
якщо $x_1 = 1 - 3i$.

52.15. $x^4 + (2\sqrt{3} + 2)x^3 + (9 + 4\sqrt{3})x^2 + (8 + 10\sqrt{3})x + 20 = 0$,
якщо $x_1 = -1 + 2i$.

52.16. $x^4 - 2x^3 + x^2 + 6x + 14 = 0$,
якщо $x_1 = 2 + \sqrt{3}i$.

52.17. $x^4 + (8 - 2\sqrt{3})x^3 + (21 - 16\sqrt{3})x^2 + (32 - 34\sqrt{3})x + 68 = 0$,
якщо $x_1 = \sqrt{3} + i$.

52.18. $x^4 - 4x^3 - 17x^2 - 26x - 14 = 0$,
якщо $x_1 = -1 + i$.

52.19. $x^4 - 4x^3 + 31x^2 - 54x + 26 = 0$,
якщо $x_1 = 1 + 5i$.

52.20. $x^4 - 4x^2 - 8x + 35 = 0$,
якщо $x_1 = -2 + \sqrt{3}i$.

52.21. $x^4 - (3\sqrt{3} + 2)x^3 + (11 - 6\sqrt{3})x^2 - (12 + 15\sqrt{3})x + 30 = 0$,
якщо $x_1 = 1 + 2i$.

52.22. $x^4 + 6x^3 + 23x^2 + 50x + 50 = 0$,
якщо $x_1 = -2 + i$.

52.23. $x^4 - 6x^3 + 17x^2 - 22x + 14 = 0$,
якщо $x_1 = 2 + \sqrt{3}i$.

52.24. $x^4 - 2\sqrt{5}x^3 - 3x^2 + 18\sqrt{5}x - 54 = 0$,
якщо $x_1 = \sqrt{5} - i$.

52.25. $x^4 - 2x^3 - 10x^2 + 6x + 45 = 0$,
якщо $x_1 = -2 + i$.

Приклад 53. Знайти нормований многочлен найменшого степеня, який має корінь $c_1 = 2 + i$ кратності $k_1 = 4$ і простий корінь $c_2 = 5$, якщо коефіцієнти цього многочлена:

а) довільні комплексні числа;

б) дійсні числа.

Розв'язання. а) Над полем $\mathbb{C}$ кожен многочлен розкладається повністю, тому, знаючи корені c_i многочлена $f(x)$, найпростіше шукати його у вигляді $f(x) = a(x - c_1)^{k_1}(x - c_2)^{k_2}...(x - c_n)^{k_n}$, де a – старший коефіцієнт. Маємо:

$$f(x) = (x - (2 + i))^4(x - 5) =$$
$$= x^5 + (-13 - 4i)x^4 + (58 + 44i)x^3 + (-98 - 164i)x^2 + (33 + 244i)x + 35 - 120i.$$

б) Нехай $g(x)$ – шуканий многочлен. Не всі коефіцієнти многочлена $f(x)$ із п.а) є дійсними, тому $g(x) \neq f(x)$. Як відомо, якщо комплексне число z_0 є коренем (кратності k) многочлена з дійсними коефіцієнтами, то і спряжене до нього число $\overline{z_0}$ також є коренем (тієї самої кратності). Отже, многочлен $g(x)$ має також корінь $2 - i$, кратність якого дорівнює 4. Розклад многочлена $g(x)$ на незвідні над $\mathbb{C}$ множники матиме вигляд

$$g(x) = (x - 5)(x - (2 + i))^4(x - (2 - i))^4.$$

Над полем $\mathbb{R}$ матимемо розклад: $g(x) = (x - 5)(x^2 - 4x + 5)^4$, тобто

$$g(x) = x^9 - 21\,x^8 + 196\,x^7 - 1076\,x^6 + 3846\,x^5 -$$
$$- 9310\,x^4 + 15300\,x^3 - 16500\,x^2 + 10625\,x - 3125.$$

Розробка процедур. Створимо процедуру **mindegPoly**, яка за заданою множиною M коренів знаходитиме нормований многочлен $f(x)$ в залежності від того, якими є коефіцієнти цього многочлена: дійсними чи довільними комплексними числами. Особливості даної процедури:

1) параметр P може набувати значень лише $\mathbb{R}$ або $\mathbb{C}$, в іншому випадку з'являється повідомлення про помилку:

```
> if P<>C and P<>R then error "wrong field" end if;
```

2) заданий параметр **M** (для множини коренів многочлена) в ході процедури змінювати не можна, тому вводимо локальний параметр **M1**:

```
> M1:=M;
```

3) якщо шуканий многочлен $f(x)$ повинен мати дійсні коефіцієнти, то потрібно, щоб разом із кожним коренем $c \notin \mathbb{R}$ множина M містила і комплексно-спряжене до нього число $\overline{c}$:

```
> if P=R then for i from 1 to nops(M) do
     c:=M[i,1]; k:=M[i,2];
     if not type(c,realcons) then
       M1:=M1 union {[conjugate(c),k]}
     end if;
  end do; end if;
```

4) на початку циклу покладемо $f(x) = 1$; поступово в процесі циклу до $f(x)$ дописуємо множники $(x - c)^k$:

```
> f:=1;
  for i from 1 to nops(M1) do
     c:=M1[i,1]; k:=M1[i,2]; f:=f*(x-c)^k;
  end do;
```

Зауважимо, що множину M коренів многочлена необхідно задавати у вигляді $M = \{[c_1, k_1], [c_2, k_2], ..., [c_s, k_s]\}$, де c_i – корені, k_i – їхні кратності відповідно.

Маємо наступний код даної процедури:

```
mindegPoly:=proc(M,P)
local i,c,f,k,M1;
   if P<>C and P<>R then error "wrong field" end if;
   M1:=M;
   if P=R then
      for i from 1 to nops(M) do
         c:=M[i,1]; k:=M[i,2];
         if not type(c,realcons) then
            M1:=M1 union {[conjugate(c),k]}
         end if;
      end do;
   end if;
   f:=1;
   for i from 1 to nops(M1) do
      c:=M1[i,1]; k:=M1[i,2]; f:=f*(x-c)^k;
   end do;
   return(f);
end proc:
```

Розв'язання в Maple. Використовуємо створену процедуру. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

Задаємо множину M коренів шуканого многочлена:

```
> M:={[2+I,4],[5,1]};
```

$$M := \{[5,\, 1],\, [2 + I,\, 4]\}$$

Нормований многочлен найменшого степеня над полем $\mathbb{C}$ має вигляд:

```
> mindegPoly(M,C);
```

$$(x - 5)\,(x - 2 - I)^4$$

Над полем $\mathbb{R}$ маємо інший многочлен:

```
> mindegPoly(M,R);
```

$$(x - 5)\,(x - 2 + I)^4\,(x - 2 - I)^4$$

Завдання 49. Знайти нормований многочлен найменшого степеня, якщо коефіцієнти цього многочлена:

а) довільні комплексні числа; б) дійсні числа;

і він має такі корені:

	Корені		
	прості	подвійні	потрійні
53.1.	–	1	$-4i$ та 2
53.2.	1 та $\sqrt{2}$	–	$-i$ та $2i$
53.3.	-5 та $-i$	$2i$ та 3	–
53.4.	2 та 3	–	1 та i
53.5.	1 та $2i$	2	$-i$
53.6.	$3-i$	1 та 2	0
53.7.	$2i$	$3i$	–
53.8.	–	$\sqrt{2}$	$2i$
53.9.	4 та $-3i$	–	i
53.10.	-2 та 1	–	$1+i$
53.11.	$\sqrt{5}i$	2 та 3	$-2i$
53.12.	1 та $-2i$	5	
53.13.	-2	–	$2i$
53.14.	–	–	2 та $3i$
53.15.	–	$-2i$	$1+\sqrt{2}$
53.16.	$1+\sqrt{3}i$	0	3
53.17.	1 та 2	–	$-4i$
53.18.	-4	$\sqrt{2}i$	$\sqrt{3}$
53.19.	1 та $4i$	–	2
53.20.	–	–	2 та $3i$
53.21.	–	2	$-3i$
53.22.	-5 та 0	i та -2	–
53.23.	$-i$	–	2 та $3i$
53.24.	$\sqrt{3}$	$1+i$	-2
53.25.	–	$2i$ та $-3i$	0

3. Рівняння 3-го і 4-го степенів

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $x^3+a_2x^2+a_1x+a_0=0$ – рівняння третього степеня з комплексними коефіцієнтами. За допомогою підстановки $x=y-\frac{a_2}{3}$ зведемо його до вигляду

$$x^3+px+q=0. \tag{VI.5}$$

Число $D=\frac{q^2}{4}+\frac{p^3}{27}$ називають дискримінантом рівняння (VI.5). Корені цього рівняння знаходять за формулою

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{D}}+\sqrt[3]{-\frac{q}{2}-\sqrt{D}},$$

яка називається формулою Кардано.

Якщо $u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}$ і $v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{D}}$ є тими значеннями кубічних коренів, при яких $x_1 = u_1 + v_1$ є коренем рівняння (VI.5), то решту коренів цього рівняння обчислюють наступним чином:

$$\begin{aligned} x_2 &= -\frac{1}{2}(u_1 + v_1) + \frac{i\sqrt{3}}{2}(u_1 - v_1), \\ x_3 &= -\frac{1}{2}(u_1 + v_1) - \frac{i\sqrt{3}}{2}(u_1 - v_1). \end{aligned}$$

Числа u_1, v_1 знаходять із умови $u_1 v_1 = -\frac{p}{3}$.

Якщо коефіцієнти p і q рівняння (VI.5) є дійсними числами, то:
а) при $D > 0$ рівняння має один дійсний і два комплексні спряжені корені;
б) при $D = 0$ рівняння має три дійсні корені, два з яких рівні між собою;
в) при $D < 0$ рівняння має три дійсні різні корені.

Для розв'язування рівняння 4-го степеня з комплексними коефіцієнтами використовують метод Феррарі, який буде проілюстровано на прикладі 54.2.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 54.1 Розв'язати рівняння: $x^3 + 3x^2 - 3x - 14 = 0$.

Розв'язання. Зведемо задане рівняння до неповного кубічного рівняння $y^3 + py + q = 0$, де $p, q \in \mathbb{R}$. Застосуємо підстановку

$$x = y - \frac{a_2}{3} = y - 1.$$

Для цього розкладемо многочлен $f(x) = x^3 + 3x^2 - 3x - 14$ за степенями двочлена $x + 1$. Маємо:

	1	3	-3	-14
-1	1	2	-5	$\boxed{-9}$
-1	1	1	$\boxed{-6}$	
-1	1	$\boxed{0}$		
-1	$\boxed{1}$			

Отже, ліву частину рівняння можна записати у вигляді $(x + 1)^3 - 6(x + 1)^2 - 9$. Значить, після підстановки отримаємо рівняння:

$$y^3 - 6y - 9 = 0. \tag{VI.6}$$

(Звичайно, можна і безпосередньо підставляти вираз $y - 1$ замість змінної x, однак такий підхід – громіздкіший).

Розв'язки такого рівняння знаходять за формулами Кардано. Обчислимо дискримінант рівняння (VI.6):

$$D = \frac{q^2}{4} + \frac{p^3}{27} = \frac{81}{4} - \frac{216}{27} = \frac{49}{4}.$$

Оскільки всі коефіцієнти рівняння дійсні і $D > 0$, то рівняння (VI.6) має один дійсний і 2 комплексні спряжені корені.

Обчислимо u_0:

$$u_0 = \sqrt[3]{-\frac{q}{2} + \sqrt{D}} = \sqrt[3]{-\frac{-9}{2} + \sqrt{\frac{49}{4}}} = \sqrt[3]{8} = 2.$$

Тоді

$$v_0 = -\frac{p}{3u_0} = -\frac{-6}{3 \cdot 2} = 1.$$

За формулами Кардано маємо наступні корені рівняння (VI.6):

$$\begin{aligned} y_0 &= u_0 + v_0 = 3, \\ y_1 &= -\frac{1}{2}(u_0 + v_0) + \frac{i\sqrt{3}}{2}(u_0 - v_0) = -\frac{3}{2} + \frac{i\sqrt{3}}{2}, \\ y_2 &= -\frac{1}{2}(u_0 + v_0) - \frac{i\sqrt{3}}{2}(u_0 - v_0) = -\frac{3}{2} - \frac{i\sqrt{3}}{2}. \end{aligned}$$

Тоді корені заданого рівняння:

$$\begin{aligned} x_0 &= y_0 - 1 = 2, \\ x_1 &= y_1 - 1 = -\frac{5}{2} + \frac{i\sqrt{3}}{2}, \\ x_2 &= y_2 - 1 = -\frac{5}{2} - \frac{i\sqrt{3}}{2}. \end{aligned}$$

Розробка процедур. Для перевірки правильності одержаного результату достатньо застосувати команду **solve**. Для покрокової перевірки створимо процедуру **solvingCubicR**, за допомогою якої можна буде досліджувати і розв'язувати кубічне рівняння з дійсними коефіцієнтами.

В ході процедури:

1) Здійснюємо перевірку:

а) чи має задане рівняння степінь 3:

```
> if degree(f)<>3 then error "wrong degree"; end if;
```

б) чи є коефіцієнти рівняння дійсними числами:

```
> M:=coeffs(f);
  for i from 1 to 4 do
  if not type(M[i],realcons) then error "wrong coefficients";
  end if;
  end do;
```

якщо якась із даних умов не виконується, з'являється попередження про помилку.

2) Зводимо задане рівняння до неповного кубічного. Для цього:

а) вводимо змінну $f_1 = f$ (це необхідно для того, щоб можна було присвоювати змінній f_1 нові значення):

```
> f1:=f;
```

б) якщо старший коефіцієнт $a_3 = \mathrm{lcoeff(f, x)}$ заданого рівняння відмінний від 1, то ділимо обидві частини на a_3:

```
> if lcoeff(f1,x)<>1 then f1:=f1/lcoeff(f1,x); print(f1);
  end if;
```

в) виконуємо підстановку $x = y - \frac{a_2}{3}$ (зауважимо, що якщо коефіцієнт при x^2 заданого рівняння рівний 0, то така підстановка лише змінить змінну x на змінну y). Результат після перетворення виводимо на екран:

```
> s:=subs({x=y-coeff(f1,x,2)/3},f1);
  f1:=expand(s); print(f1);
```

3) Далі розв'язуємо неповне кубічне рівняння $y^3 + py + q = 0$ за формулами Кардано. Спочатку за допомогою дискримінанта D досліджуємо, якими є розв'язки (дійсними чи ні):

```
> p:=coeff(f1,y,1):
  q:=coeff(f1,y,0):
  D:=q^2/4+p^3/27;
  print('D'=  D);
  if D>0 then print("1Diysnyi 2Complexnospryajeni")
  elif D=0 then print("3Diysni hocha b 2 odnakovi")
  else print("3Diysni rizni");
  end if;
```

а потім знаходимо ці розв'язки:

```
> u0:=simplify((-q/2+sqrt(D))^(1/3));
  print('u0'=u0);
  v0:=-p/(3*u0); print('v0'=v0);
  y[1]:=u0+v0;
  y[2]:=-1/2*(u0+v0)+I*sqrt(3)/2*(u0-v0);
  y[3]:=-1/2*(u0+v0)-I*sqrt(3)/2*(u0-v0);
  print('y[1]'=y[1],'y[2]'=y[2],'y[3]'=y[3]);
  for i from 1 to  3 do x[i]:=y[i]-coeff(f,x,2)/3; end do;
  print('x[1]'=x[1],'x[2]'=x[2],'x[3]'=x[3]);
```

Отже, процедура матиме наступний код:

```
solvingCubicR:=proc(f,x)
local i,M,f1,s,p,q,D,u0,v0,y;
   if degree(f)<>3 then error "wrong degree"; end if;
   M:=coeffs(f);
   for i from 1 to 4 do
      if not type(M[i],realcons) then error "wrong coefficients";
      end if;
   end do;
   f1:=f;
   if lcoeff(f1,x)<>1 then f1:=f1/lcoeff(f1,x); print(f1); end if;
   s:=subs({x=y-coeff(f1,x,2)/3},f1);
   f1:=expand(s); print(f1);
   p:=coeff(f1,y,1):
   q:=coeff(f1,y,0):
   D:=q^2/4+p^3/27;
   print('D'= D);
   if D>0 then print("1Diysnyi 2Complexnospryajeni")
   elif D=0 then print("3Diysni hocha b 2 odnakovi")
   else print("3Diysni rizni");
   end if;
   u0:=simplify((-q/2+sqrt(D))^(1/3)); print('u0'=u0);
   v0:=-p/(3*u0); print('v0'=v0);
   y[1]:=u0+v0;
   y[2]:=-1/2*(u0+v0)+I*sqrt(3)/2*(u0-v0);
   y[3]:=-1/2*(u0+v0)-I*sqrt(3)/2*(u0-v0);
   print('y[1]'=y[1],'y[2]'=y[2],'y[3]'=y[3]);
   for i from 1 to 3 do x[i]:=y[i]-coeff(f,x,2)/3; end do;
   print('x[1]'=x[1],'x[2]'=x[2],'x[3]'=x[3]);
end proc:
```

Розв'язання в Maple. Для перевірки правильності одержаного результату достатньо використати команду **solve**:

```
> solve(x^3+3*x^2-3*x-14=0,x);
```

$$2,\ -\frac{5}{2}+\frac{1}{2}\,I\,\sqrt{3},\ -\frac{5}{2}-\frac{1}{2}\,I\,\sqrt{3}$$

Для перевірки проміжних обчислень застосуємо створену процедуру:

```
> read(`e:/atchlib.m`); with(atchlib):
> solvingCubicR(x^3+3*x^2-3*x-14,x);
```

$$y^3-6\,y-9$$

$$\mathrm{D}=\frac{49}{4}$$

"1Diysnyi 2Complexnospryajeni"

$$u0 = 2$$
$$v0 = 1$$
$$y_1 = 3,\ y_2 = -\frac{3}{2} + \frac{1}{2}\,I\,\sqrt{3},\ y_3 = -\frac{3}{2} - \frac{1}{2}\,I\,\sqrt{3}$$
$$x_1 = 2,\ x_2 = -\frac{5}{2} + \frac{1}{2}\,I\,\sqrt{3},\ x_3 = -\frac{5}{2} - \frac{1}{2}\,I\,\sqrt{3}$$

Приклад 54.2 Розв'язати рівняння: $x^4 + 8x^3 + 22x^2 + 29x + 12 = 0$.

Розв'язання. Зведемо задане рівняння до неповного рівняння 4-го степеня $y^4 + py^2 + qy + r = 0$, де $p, q, r \in \mathbb{R}$. Застосуємо підстановку

$$x = y - \frac{a_3}{4} = y - 2.$$

Для цього розкладемо многочлен $f(x) = x^4 + 8x^3 + 22x^2 + 29x + 12$ за степенями двочлена $x + 2$. Маємо:

	1	8	22	29	12
-2	1	6	10	9	-6
-2	1	4	2	5	
-2	1	2	-2		
-2	1	0			
-2	1				

Після підстановки отримаємо рівняння:

$$y^4 - 2y^2 + 5y - 6 = 0. \tag{VI.7}$$

Застосуємо метод Феррарі. Залишимо в лівій частині рівняння доданок y^4, а решту доданків перенесемо в праву частину:

$$y^4 = 2y^2 - 5y + 6.$$

Додамо до обох частин даної рівності вираз $y^2t + \frac{t^2}{4}$ із допоміжною змінною t (в такий спосіб ліва частина буде повним квадратом):

$$y^4 + 2y^2\frac{t}{2} + \frac{t^2}{4} = (t+2)y^2 - 5y + \left(\frac{t^2}{4} + 6\right).$$

або

$$(y^2 + \frac{t}{2})^2 = (t+2)y^2 - 5y + \left(\frac{t^2}{4} + 6\right). \tag{VI.8}$$

Коефіцієнти многочлена $(t+2)y^2 - 5y + \left(\frac{t^2}{4} + 6\right)$ від змінної y самі є многочленами від змінної t. Підберемо значення змінної t так, щоб і в правій частині рівняння теж був повний квадрат. Для цього необхідно, щоб дискримінант D квадратного (відносно y) тричлена в правій частині дорівнював 0. Матимемо:

$$D = 25 - 4(t+2)\left(\frac{t^2}{4} + 6\right) = -t^3 - 2t^2 - 24t - 23.$$

Значення t, при яких $D = 0$, можна знайти за формулами Кардано (див. Приклад 54.1), але зручніше, якщо це вдається, підбирати їх усно. Помічаємо, що одним із розв'язків рівняння $D = 0$ є число $t = -1$. Підставляємо це значення в рівність (VI.8). Отримаємо:

$$\left(y^2 - \frac{1}{2}\right)^2 = y^2 - 5y + \frac{25}{4},$$

тобто

$$\left(y^2 - \frac{1}{2}\right)^2 = \left(y - \frac{5}{2}\right)^2,$$

звідки

$$\left(y^2 - \frac{1}{2}\right)^2 - \left(y - \frac{5}{2}\right)^2 = 0.$$

Розкладемо ліву частину за формулою різниці квадратів:

$$\left((y^2 - \frac{1}{2}) - (y - \frac{5}{2})\right)\left((y^2 - \frac{1}{2}) + (y - \frac{5}{2})\right) = 0,$$

тобто

$$(y^2 - y + 2)(y^2 + y - 3) = 0,$$

звідки

$$y^2 - y + 2 = 0 \qquad \text{або} \qquad y^2 + y - 3 = 0.$$

Розв'язуючи ці квадратні рівняння, знаходимо 4 розв'язки рівняння (VI.7):

$$y_{1,2} = -\frac{1}{2} \pm \frac{\sqrt{13}}{2}, \quad y_{3,4} = \frac{1}{2} \pm \frac{\sqrt{7}}{2}\, i.$$

Тоді

$$x_{1,2} = -\frac{5}{2} \pm \frac{\sqrt{13}}{2}, \quad x_{3,4} = -\frac{3}{2} \pm \frac{\sqrt{7}}{2}\, i.$$

Розробка процедур. Для перевірки правильності отриманої відповіді достатньо використати команду **solve**. Для покрокової перевірки створимо процедуру **solvingQuartic(f,x)** розв'язування рівняння $f(x) = 0$ 4-го степеня з довільними комплексними коефіцієнтами. В її основу покладемо метод Феррарі. Початок даної процедури (зведення до неповного рівняння 4-го степеня $y^4 + py^2 + qy + r = 0$) аналогічний до процедури із Прикладу 54.1. Далі:

1) відокремлюємо в лівій частині доданок y^4, решту доданків переносимо в праву частину рівняння:

```
> print(isolate(f1,y^4));
```

2) позначаємо ліву частину рівняння (VI.8) через **lp**, а праву через **rp**:

```
> lp:=(y^2+t/2)^2;
  rp:=(t-p)*y^2-q*y+(t^2/4-r);
  print(lp=rp);
```

3) знаходимо резольвенту D та її корені $t0$:

```
> D:=-t^3+p*t^2+4*r*t+(q^2-4*p*r); print('D'=D);
  t0:=solve(D,t); print("koreni resolventy"=t0);
```

4) підставляємо замість t окремо в ліву частину, окремо в праву частинурівності lp=rp один із коренів резольвенти $t0[1]$, тоді обидві частини рівняння є повними квадратами: $(y^2 + t/2)^2 = (Ay + B)^2$:

```
> lps:=subs({t=t0[1]},lp);
  rps:=subs({t=t0[1]},rp);
```

5) вводимо в розгляд квадратні рівняння $eq1 := (y^2 + t/2) - (Ay + B)$ та $eq1 := (y^2 + t/2) + (Ay + B)$, розв'язки y_i яких є розв'язками рівняння $y^4 + py^2 + qy + r = 0$; потім знаходимо відповідні x_i:

```
> eq1:=psqrt(lps)-psqrt(rps);
  eq2:=psqrt(lps)+psqrt(rps);
  y[1]:=solve(eq1)[1];
  y[2]:=solve(eq1)[2];
  y[3]:=solve(eq2)[1];
  y[4]:=solve(eq2)[2];
  print('y[1]'=y[1],'y[2]'=y[2],'y[3]'=y[3],'y[4]'=y[4]);
  for i from 1 to  4 do x[i]:=y[i]-coeff(f,x,3)/4; end do;
  print('x[1]'=x[1],'x[2]'=x[2],'x[3]'=x[3],'x[4]'=x[4]);
```

Процедура матиме наступний код:

```
solvingQuartic:=proc(f,x)
local i,r,f1,D,t0,s,p,lp,rp,lps,rps,q,eq1,eq2,y;
   if degree(f)<>4 then error "wrong degree"; end if;
   f1:=f;
   if lcoeff(f1,x)<>1 then f1:=f1/lcoeff(f1,x); print(f1); end if;
   s:=subs({x=y-coeff(f1,x,3)/4},f1);
   f1:=expand(s); print(f1);
   p:=coeff(f1,y,2):
   q:=coeff(f1,y,1):
   r:=coeff(f1,y,0):
   print(isolate(f1,y^4)); lp:=(y^2+t/2)^2;
   rp:=(t-p)*y^2-q*y+(t^2/4-r); print(lp=rp);
   D:=-t^3+p*t^2+4*r*t+(q^2-4*p*r); print('D'=D);
   t0:=solve(D,t); print("koreni resolventy-t0);
   lps:=subs({t=t0[1]},lp);
   rps:=subs({t=t0[1]},rp);
   eq1:=psqrt(lps)-psqrt(rps);
   eq2:=psqrt(lps)+psqrt(rps);
   y[1]:=solve(eq1)[1];
   y[2]:=solve(eq1)[2];
   y[3]:=solve(eq2)[1];
   y[4]:=solve(eq2)[2];
   print('y[1]'=y[1],'y[2]'=y[2],'y[3]'=y[3],'y[4]'=y[4]);
   for i from 1 to 4 do x[i]:=y[i]-coeff(f,x,3)/4; end do;
   print('x[1]'=x[1],'x[2]'=x[2],'x[3]'=x[3],'x[4]'=x[4]);
end proc:
```

Розв'язання в Maple. Для перевірки правильності отриманої відповіді використовуємо команду **solve**:

```
> solve(x^4+8*x^3+22*x^2+29*x+12);
```

$$-\frac{5}{2}+\frac{\sqrt{13}}{2},\ -\frac{5}{2}-\frac{\sqrt{13}}{2},\ -\frac{3}{2}+\frac{1}{2}\,I\,\sqrt{7},\ -\frac{3}{2}-\frac{1}{2}\,I\,\sqrt{7}$$

Для перевірки проміжних перетворень використовуємо створену процедуру:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

```
> solvingQuartic(x^4+8*x^3+22*x^2+29*x+12,x);
```

$$y^4-2\,y^2+5\,y-6$$

$$y^4=2\,y^2-5\,y+6$$

$$(y^2+\frac{t}{2})^2=(t+2)\,y^2-5\,y+\frac{t^2}{4}+6$$

$$\mathrm{D}=-t^3-2\,t^2-24\,t-23$$

$$\text{"}koreni\ resolventy\text{"} = (-1,\ -\frac{1}{2}+\frac{1}{2}\,I\,\sqrt{91},\ -\frac{1}{2}-\frac{1}{2}\,I\,\sqrt{91})$$

$$y_1=\frac{1}{2}+\frac{1}{2}\,I\,\sqrt{7},\ y_2=\frac{1}{2}-\frac{1}{2}\,I\,\sqrt{7},\ y_3=-\frac{1}{2}+\frac{\sqrt{13}}{2},\ y_4=-\frac{1}{2}-\frac{\sqrt{13}}{2}$$

$$x_1=-\frac{3}{2}+\frac{1}{2}\,I\,\sqrt{7},\ x_2=-\frac{3}{2}-\frac{1}{2}\,I\,\sqrt{7},\ x_3=-\frac{5}{2}+\frac{\sqrt{13}}{2},\ x_4=-\frac{5}{2}-\frac{\sqrt{13}}{2}$$

Завдання 54. Розв'язати рівняння:

54.1. а) $x^3+6x^2+3x-38=0$;
б) $x^4-4x^3+7x^2+2x-21=0$.

54.2. а) $x^3-12x^2+33x-8=0$;
б) $x^4-8x^3+19x^2-2x-30=0$.

54.3. а) $x^3+9x^2+24x+16=0$;
б) $x^4+4x^3+x^2-12x-12=0$.

54.4. а) $x^3+12x^2+42x+44=0$;
б) $x^4-8x^3+22x^2-27x+12=0$.

54.5. а) $x^3-6x^2+18x-13=0$;
б) $x^4+8x^3+22x^2+19x-8=0$.

54.6. а) $x^3-9x^2+15x-7=0$;
б) $x^4-4x^3+3x^2+12x-18=0$.

54.7. а) $x^3-3x^2+12x+16=0$;
б) $x^4-4x^3+3x^2+8x-10=0$.

54.8. а) $x^3+3x^2-12x-18=0$;
б) $x^4-8x^3+25x^2-44x+21=0$.

54.9. а) $x^3-6x^2+32=0$;
б) $x^4+4x^3-x^2-28x-32=0$.

54.10. а) $x^3+3x^2-6x-36=0$;
б) $x^4-4x^3-4x^2+7x-2=0$.

54.11. а) $x^3 - 15x^2 + 57x - 70 = 0$;
б) $x^4 + 4x^3 + 4x^2 - 16x - 32 = 0$.

54.12. а) $x^3 - 12x^2 + 42x - 36 = 0$;
б) $x^4 - 4x^3 + 7x^2 - 12 = 0$.

54.13. а) $x^3 - 9x^2 + 36x - 28 = 0$;
б) $x^4 + 8x^3 + 22x^2 + 36x + 24 = 0$.

54.14. а) $x^3 - 3x^2 - 24x - 28 = 0$;
б) $x^4 - 8x^3 + 25x^2 - 42x + 24 = 0$.

54.15. а) $x^3 - 9x^2 + 33x - 38 = 0$;
б) $x^4 + 4x^3 + 4x^2 - 12x - 21 = 0$.

54.16. а) $x^3 - 6x^2 - 3x + 44 = 0$;
б) $x^4 - 4x^3 - x^2 + 28x - 32 = 0$.

54.17. а) $x^3 + 12x^2 + 30x - 43 = 0$;
б) $x^4 - 8x^3 + 22x^2 - 8x - 39 = 0$.

54.18. а) $x^3 + 6x^2 - 32 = 0$;
б) $x^4 + 8x^3 + 22x^2 + 27x + 12 = 0$.

54.19. а) $x^3 - 9x^2 + 12x + 14 = 0$;
б) $x^4 + 4x^3 + x^2 - 16x - 20 = 0$.

54.20. $x^3 - 6x^2 + 3x - 18 = 0$;
б) $x^4 - 8x^3 + 16x^2 + 9x - 36 = 0$.

54.21. а) $x^3 - 12x^2 + 33x + 18 = 0$;
б) $x^4 - 8x^3 + 14x^2 + 17x - 44 = 0$.

54.22. а) $x^3 - 15x^2 + 48x - 44 = 0$;
б) $x^4 - 4x^3 + x^2 + 12x - 12 = 0$.

54.23. а) $x^3 - 6x^2 + 6x + 8 = 0$;
б) $x^4 + 8x^3 + 21x^2 + 14x - 10 = 0$.

54.24. а) $x^3 - 9x^2 + 24x - 20 = 0$;
б) $x^4 - 8x^3 + 21x^2 - 30x + 18 = 0$.

54.25. а) $x^3 - 12x^2 + 57x - 74 = 0$;

б) $x^4 + 4x^3 - 2x^2 - 21x - 18 = 0$.

Приклад 55. Знайти графічно дійсні корені рівняння:

а) $4x^3 + 24x^2 + 41 + 15 = 0$;

б) $2x^3 + 3x^2 - 1 = 0$;

в) $x^3 + 3x^2 + x - 1 = 0$.

Розв'язання. а) Поділимо обидві частини заданого рівняння на старший коефіцієнт: $x^3+6x^2+10,25x+3,75 = 0$. Для того, щоб зробити рівним нулю коефіцієнт при x^2, виконуємо підстановку $x = y - \frac{a_2}{3} = y - 2$. Одержимо рівняння: $y^3 - 1,75y - 0,75 = 0$ або

$$y^3 = 1,75y + 0,75. \tag{VI.9}$$

Введемо в розгляд функції $z = y^3$ і $z = 1,75y + 0,75$, графіки яких в системі координат YOZ зображено на рисунку 11.

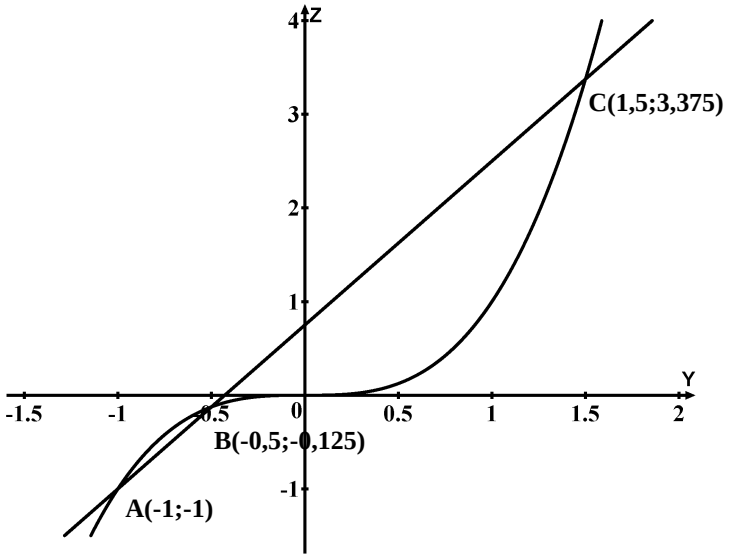


Рис.11

Графіки цих функцій перетинаються в точках A, B і C з абсцисами $y \approx -1$, $y \approx -0,5$ і $y \approx 1,5$ відповідно. При таких значеннях y вирази y^3 і $1,75y+0,75$ набувають рівних значень, тобто числа -1, $-0,5$ і $1,5$ – корені (можливо, наближені) рівняння (VI.9). Підставивши $y_1 = -1$, $y_2 = -0,5$ і $y_3 = 1,5$ у дане рівняння, переконуємось, що -1, $-0,5$ і $1,5$ – точні корені. Тоді $x_1 = -3$, $x_2 = -2,5$, $x_3 = -0.5$.

б) Поділимо обидві частини заданого рівняння на 2: $x^3+1,5x^2-0,5 = 0$ і введемо заміну $x = y - 0,5$. Одержимо рівняння: $y^3 - 0,75y - 0,25 = 0$

або

$$y^3 = 0,75y + 0,25. \qquad \text{(VI.10)}$$

Графіки функцій $z = y^3$ і $z = 0,75y + 0,25$ зображено на рисунку 2.

Розв'язками рівняння (VI.10) є абсциси точок A і B. При цьому точка $A(-0,5;-0,125)$ – точка *дотику* кубічної параболи $z = y^3$ і прямої $z = 0,75y + 0,25$, тому її абсциса $y \approx -0,5$ є подвійним коренем рівняння (VI.9), точка $B(1;1)$ – точка *перетину* графіків, тому її абсциса $y \approx 1$ є простим коренем. Безпосередня перевірка показує, що значення $y_1 = y_2 = -0,5$, $y_3 = 1$ є точними коренями. Тоді $x_1 = x_2 = -1$, $x_3 = 0,5$.

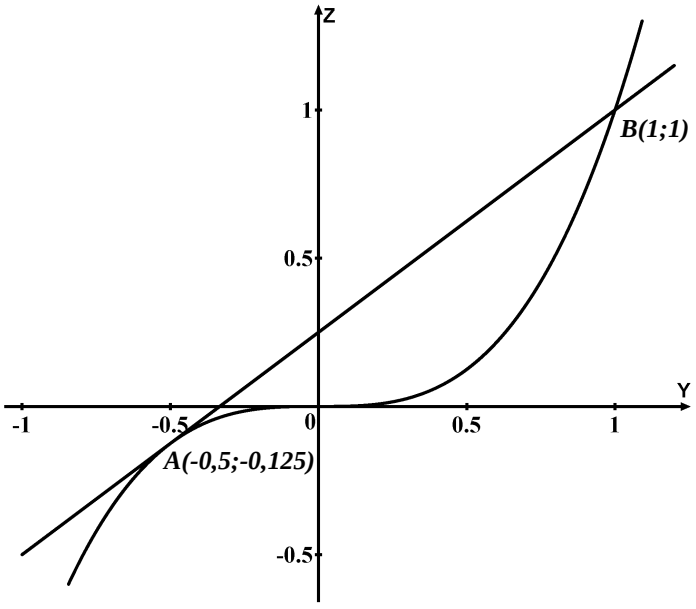


Рис.12

в) Підстановкою $x = y - 1$ зводимо задане рівняння до виду

$$y^3 - 2y - 4 = 0$$

або

$$y^3 = 2y + 4. \qquad \text{(VI.11)}$$

Графіки функцій $z = y^3$ і $z = 2y + 4$ зображено на рис.13.

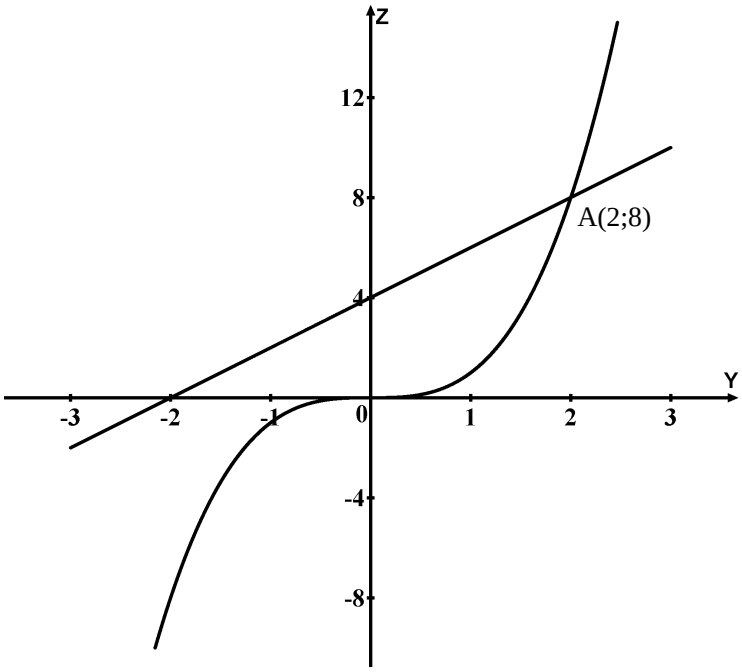
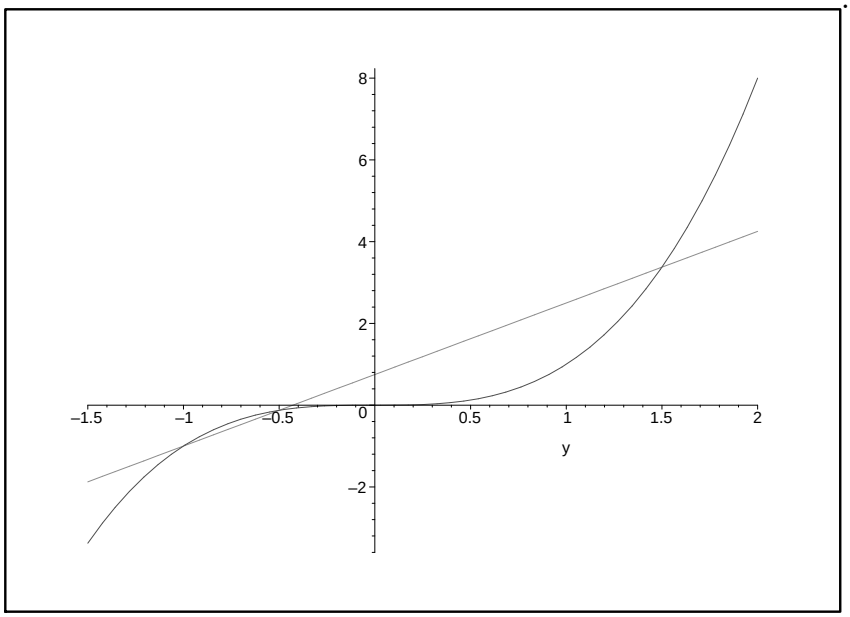


Рис.13

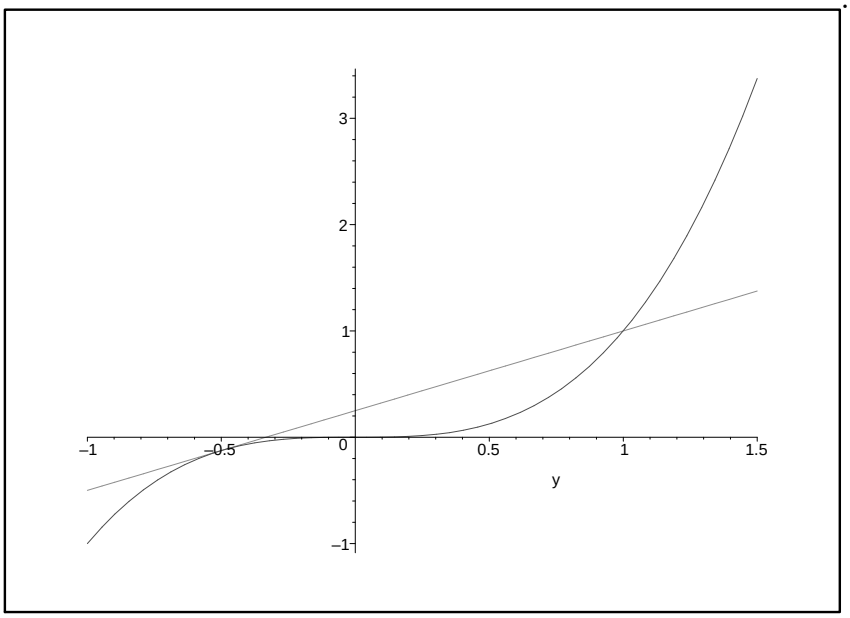
Кубічна парабола $z = y^3$ і пряма $z = 2y + 4$ перетинаються лише в одній точці. Отже, рівняння має лише один дійсний корінь $y \approx 2$. Перевірка показує, що цей корінь є точним. Отже, $y = 2$, тоді $x = 1$.

Розв'язання в Maple. Для побудови графіків функцій в Maple використовується команда **plot({f1, f2,...}, h, v, options)**, де f1, f2, ... - функції, графіки яких будуються, h – горизонтальний проміжок, v - вертикальний проміжок, options - будь-який із необов'язкових параметрів (назви осей, колір, шрифт, масштаб, товщина ліній тощо)

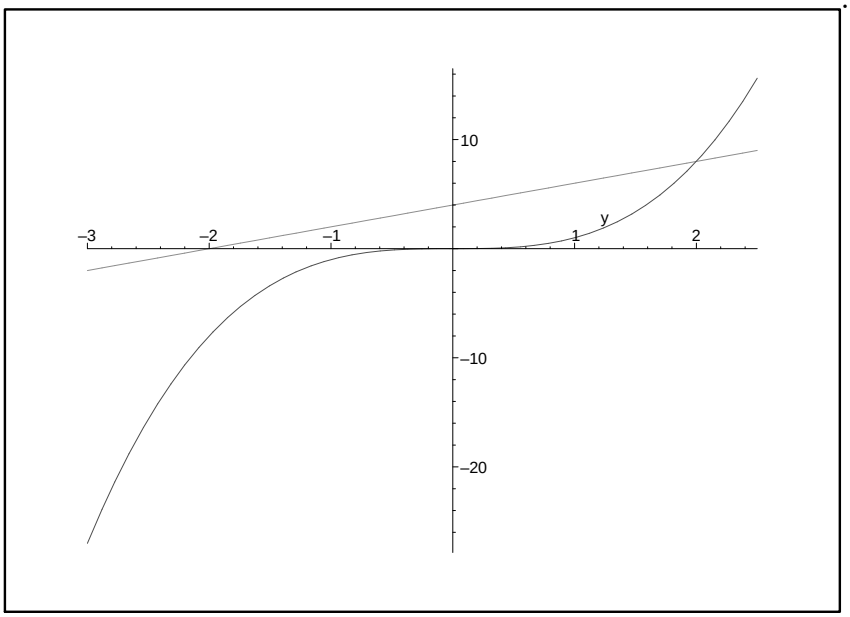
```
> plot({y^3, 1.75*y+0.75}, y=-1.5..2);
```



```
> plot({y^3, 0.75*y+0.25}, y=-1..1.5);
```




```
> plot({y^3, 2*y+4}, y=-3..2.5);
```



Для збільшення масштабу (і уточнення координат точок перетину), зміни інших параметрів побудови можна використовувати команди контекстного меню (викликається натисненням правої кнопки миші).

Завдання 55. Знайти графічно дійсні корені рівняння:

55.1. $4x^3 - 24x^2 + 35x - 12 = 0.$

55.2. $8x^3 + 60x^2 + 126x + 81 = 0.$

55.3. $2x^3 - 24x^2 + 95x - 125 = 0.$

55.4. $4x^3 + 12x^2 - x - 3 = 0.$

55.5. $4x^3 + 36x^2 + 105x + 100 = 0.$

55.6. $3x^3 + 4x^2 - 5x - 2 = 0.$

55.7. $8x^3 - 12x^2 - 50x - 21 = 0.$

55.8. $2x^3 - 15x^2 + 24x + 16 = 0.$

55.9. $2x^3 - 18x^2 + 51x - 55 = 0.$

55.10. $4x^3 - 36x^2 + 89x - 66 = 0.$

55.11. $8x^3 - 36x^2 + 30x + 25 = 0.$

55.12. $4x^3 - 12x^2 + 9x - 27 = 0.$

55.13. $2x^3 + x^2 - 5x + 2 = 0.$

55.14. $2x^3 + 3x^2 - 3x - 2 = 0.$

55.15. $2x^3 + x^2 - 2x - 1 = 0.$

55.16. $2x^3 + 5x^2 + 4x + 1 = 0.$

55.17. $4x^3 + 36x^2 + 81x + 54 = 0.$

55.18. $4x^3 + 24x^2 + 29x + 9 = 0.$

55.19. $8x^3 + 12x^2 - 18x - 27 = 0.$

55.20. $8x^3 + 60x^2 + 130x + 99 = 0.$

55.21. $8x^3 - 12x^2 - 18x + 27 = 0.$

55.22. $2x^3 + 15x^2 + 36x + 27 = 0.$

55.23. $4x^3 + 8x^2 + 5x + 1 = 0.$

55.24. $2x^3 + 9x^2 + 10x + 3 = 0.$

55.25. $2x^3 - 3x^2 - 12x - 7 = 0.$

4. Відокремлення дійсних коренів многочлена

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ – многочлен з комплексними коефіцієнтами, $A = \max\{|a_{n-1}|, \ldots, |a_1|, |a_0|\}$ і $N_0 = 1 + \frac{A}{|a_n|}$. Тоді всі корені многочлена $f(z)$ лежатимуть всередині круга з центром у початку координат і радіусом N_0. Якщо многочлен $f(z)$ має дійсні корені, то вони знаходяться в інтервалі $(-N_0; N_0)$.

Одним із методів знаходження верхньої межі додатних коренів многочлена з дійсними коефіцієнтами є **метод Ньютона**. В основі цього методу лежить той факт, що коли при $x = M$ многочлен $f(x)$ має додатне значення, а всі його похідні невід'ємні, то число M є верхньою межею додатних коренів многочлена. Підібрати таке число M безпосередньо часто буває досить непросто. Оскільки знак многочлена і його похідних в точці $x = M$ співпадає із знаком відповідних коефіцієнтів Тейлора при розкладі за степенями $x - M$, на практиці для відшукання верхньої межі додатних дійсних коренів зручно використовувати схеми Горнера.

	a_n	a_{n-1}	$\dots$	a_2	a_1	a_0
M	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$f(M)$
M	$\dots$	$\dots$	$\dots$	$\dots$	$f'(M)$	
M	$\dots$	$\dots$	$\dots$	$\frac{f''(M)}{2!}$		
$\dots$	$\dots$	$\dots$				
M	$\frac{f^n(M)}{n!}$					

Якщо M_0, M_1, M_2, M_3 – верхні межі додатних коренів многочленів $f(x)$, $y^n f\left(\frac{1}{y}\right)$, $f(-y)$ і $y^n f\left(-\frac{1}{y}\right)$ з дійсними коефіцієнтами відповідно, то додатні корені многочлена $f(x)$ знаходяться в проміжку $\left(\frac{1}{M_1}; M_0\right)$, а від'ємні – в проміжку $\left(-M_2; -\frac{1}{M_3}\right)$.

Нехай $c_1, c_2, \dots, c_m$ – деяка впорядкована послідовність дійсних чисел. Кількість пар сусідніх чисел цієї послідовності, які мають протилежні знаки, називають кількістю змін знаків даної послідовності.

Правило Декарта: *число додатних коренів многочлена з дійсними коефіцієнтами дорівнює або на парне число менше кількості змін знаків у послідовності його коефіцієнтів.*

Це правило за допомогою заміни $x = -y$ можна застосувати для оцінки кількості від'ємних коренів многочлена $f(x)$.

Задача відокремлення дійсних коренів полягає в знаходженні тих інтервалів, у кожному з яких лежить тільки один (можливо, кратний) корінь. Відокремити корені многочлена $f(x)$, який не має кратних коренів, можна **методом Штурма**. При цьому для многочлена будують насамперед ряд Штурма:

$$f(x), f'(x), F_1(x), F_2(x), \dots, F_{m-1}(x), F_m.$$

Щоб знайти многочлени $F_i(x)$, $1 \leqslant i \leqslant m$, застосовують алгоритм, аналогічний алгоритму Евкліда:

$$\begin{aligned}
f(x) &= f'(x)\Phi_1(x) - F_1(x),\\
f'(x) &= F_1(x)\Phi_2(x) - F_2(x),\\
F_1(x) &= F_2(x)\Phi_3(x) - F_3(x),\\
&\dots\dots\dots\dots\dots\dots\\
F_{m-2}(x) &= F_{m-1}(x)\Phi_m(x) - F_m,\\
F_{m-1}(x) &= F_m\Phi_{m+1}(x).
\end{aligned}$$

Відмінність цього алгоритму від алгоритму Евкліда полягає тільки в тому, що всі остачі $r_k(x)$ беруть із протилежними знаками, тобто $F_k(x) = -r_k(x)$.

Після цього застосовують теорему:

Теорема (Штурма)**.** *Якщо a і b – довільні дійсні числа, які не є коренями многочлена $f(x)$ в інтервалі $(a; b)$, то число p різних дійсних коренів многочлена $f(x)$ в інтервалі $(a; b)$ дорівнює $p = s(a) - s(b)$, де $s(a)$ і $s(b)$ – кількість змін знаків у ряді Штурма відповідно при $x = a$ і $x = b$.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 56. Знайти межі додатних і від'ємних дійсних коренів многочлена

$$f(x) = 3x^5 + 2x^4 - x^2 - 4x - 3.$$

Розв'язання. Знайдемо проміжок, в якому містяться дійсні корені многочлена $f(x)$ (якщо вони існують). В даному випадку маємо: $a_n = 3$, $A = \max\{2, 0, 1, 4, 3\} = 4$. Тоді $N_0 = 1 + \frac{4}{3} = 2\frac{1}{3}$. Отже, якщо многочлен має дійсні корені корені, то вони знаходяться в інтервалі $\left(-2\frac{1}{3}; 2\frac{1}{3}\right)$. Для більш точної оцінки верхньої межі додатних дійсних коренів застосуємо метод Ньютона.

Перевіримо число 1:

	3	2	0	-1	-4	-3
1	3	5	5	4	0	$-3 = f(1)$

Оскільки $f(1) = -3 < 0$, то спроба виявилась невдалою. Перевіримо число 1,2:

	3	2	0	-1	-4	-3
1,2	3	5,6	6,72	7,064	4,4768	2,3722

Оскільки рядочок таблиці складається виключно із додатних чисел, то відпадає необхідність в обчисленні наступних рядочків, які будуть складатись лише із додатних чисел, зокрема, числа $f'(1,2), f''(1,2), f'''(1,2), f^{IV}(1,2), f^{V}(1,2)$ будуть додатні. Отже, можна прийняти число $M_0 = 1,2$ за верхню межу додатних дійсних коренів: $M_+ = M_0 = 1,2$.

Щоб знайти нижню межу додатних дійсних коренів многочлена $f(x)$ зробимо заміну $x = \frac{1}{y}$. Тоді $f\left(\frac{1}{y}\right) = \frac{3}{y^5} + \frac{2}{y^4} - \frac{1}{y^2} - \frac{4}{y} - 3$. Розглянемо многочлен $g_1(y) = -y^5 f\left(\frac{1}{y}\right) = 3y^5 + 4y^4 + y^3 - 2y - 3$. Зауважимо, що ми беремо $-y^5 f\left(\frac{1}{y}\right)$ замість $y^5 f\left(\frac{1}{y}\right)$ тому, що для застосування методу Ньютона старший коефіцієнт має бути додатним. На корені многочлена ця зміна знаку, зрозуміло, жодним чином не впливає. Перевіримо число 1:

	3	4	1	0	-2	-3
1	3	7	8	8	6	3

Таким чином, за верхню межу додатних дійсних коренів многочлена $g_1(y)$ можна взяти $M_1 = 1$. Тоді число $m_+ = \frac{1}{M_1} = 1$ буде нижньою межею додатних дійсних коренів многочлена $f(x)$.

Для відшукання нижньої межі від'ємних дійсних коренів многочлена розглянемо многочлен $g_2(y) = -f(-y) = 3y^5 - 2y^4 + y^2 - 4y + 3$. Випробуємо число 1.

	3	−2	0	1	−4	3
1	3	1	1	2	−2	1
1	3	4	5	7	5	

Отже, верхня межа додатних дійсних коренів многочлена $g_2(y)$ дорівнює $M_2 = 1$; тоді для нижньої межі від'ємних коренів многочлена $f(x)$ маємо: $M_- = -M_2 = -1$.

Зробимо тепер заміну $x = -\frac{1}{y}$ і розглянемо многочлен $g_3(y) = -y^5 f\left(-\frac{1}{y}\right) = 3y^5 - 4y^4 + y^3 - 2y + 3$. Випробуємо число 1:

	3	−4	1	0	−2	3
1	3	−1	0	0	−2	1
1	3	2	2	2	0	

Отже, для оцінки верхньої межі додатних дійсних коренів многочлена $g_3(y)$ можна взяти число $M_3 = 1$. Тоді нижня межа від'ємних дійсних коренів многочлена $f(x)$ дорівнює $m_- = -\frac{1}{M_3} = -1$. Разом із знайденим вище результатом $M_- = -1$ це означає, що заданий многочлен $f(x)$ зовсім не має від'ємних дійсних коренів.

Таким чином, додатні корені многочлена $f(x)$ (якщо вони існують) розміщені в інтервалі $(1; 1, 2)$, а від'ємних коренів даний многочлен не має.

Розв'язання в Maple. В Maple для відокремлення коренів дійсних коренів многочлена $f(x)$ з дійсними коефіцієнтами використовується команда **realroot(f, d)**. Інтервали-відповіді подаються у вигляді [a, b]. Довжина кожного з інтервалів не перевищує значення необов'язкового параметру d (який має бути додатним числом). Якщо параметр d не зазначено, то підбирається найбільш зручне значення для кожного із інтервалів. При цьому під записом [a, a] розуміється окрема точка, запис [a, b], де $a < b$, означає інтервал (a, b). Робота команди **realroot** грунтується на правилі Декарта, тому, зрозуміло, що одержану відповідь можна використовувати для порівняння із аналітично отриманою лише наближено.

Використаємо команду **realroot**, не зазначаючи довжини інтервала d:

```
> realroot(3*x^5+2*x^4-x^2-4*x-3);
```

$$[[0,\ 2]]$$

Довжину інтервала, в якому міститься дійсний корінь заданого многочлена, можна зменшити, додаючи другий аргумент d команди **realroot** (наприклад, $d = 0,5$):

```
> realroot(3*x^5+2*x^4-x^2-4*x-3,0.5);
```

$$[[1,\ \frac{3}{2}]]$$

або ще менше:

```
> realroot(3*x^5+2*x^4-x^2-4*x-3,0.2);
```

$$[[\frac{9}{8},\ \frac{5}{4}]]$$

Порівнюючи даний результат із результатом, одержаним аналітично методом Ньютона, отримуємо точнішу оцінку: корінь належить до інтервалу $(1,125; 1,2)$.

Завдання 56. Знайти межі додатних і від'ємних дійсних коренів многочлена:

56.1. $3x^5 - 5x^4 - 7x^3 - 4x^2 - 2x + 14 = 0.$

56.2. $8x^4 - 7x^3 + x^2 - 4x - 1 = 0.$

56.3. $3x^5 + x^4 - 5x^3 + 7x^2 - 4x + 9 = 0.$

56.4. $-x^5 + 5x^4 - 2x^3 + 4x^2 - 1 = 0.$

56.5. $4x^5 - 3x^4 + 10x^3 + 7x^2 - 2x + 3 = 0.$

56.6. $9x^5 - 3x^3 + 7 = 0.$

56.7. $3x^5 - 4x^4 - 7x^3 + 2x^2 + 6x + 1 = 0.$

56.8. $7x^5 + 2x^4 + x^2 - 3x + 8 = 0.$

56.9. $x^4 - x^3 - 5x^2 - 14x + 10 = 0.$

56.10. $-2x^4 + 4x^3 - x^2 - 4x + 5 = 0.$

56.11. $2x^5 - 9x^4 + 13x^3 + x^2 - x + 1 = 0.$

56.12. $7x^5 + 4x^4 + 3x^3 - x^2 - 7x + 2 = 0.$

56.13. $252x^4 + 66x^3 - 60x^2 - 11x + 3 = 0.$

56.14. $7x^5 - 4x^4 - 5x^3 + 14x^2 - 5x - 8 = 0.$

56.15. $7x^5 - 3x^3 + 5x^2 - 2x - 10 = 0.$

56.16. $3x^4 - 7x^3 + 2x^2 - 4x - 7 = 0.$

56.17. $x^5 - 7x^4 + 10x^3 + 3x^2 - 2x - 7 = 0.$

56.18. $735x^4 - 196x^3 - 211x^2 + 4x + 4 = 0.$

56.19. $x^5 + 3x^4 + 8x^3 - 5x^2 - 5x + 3 = 0.$

56.20. $-4x^5 + 5x^3 - 13x^2 - 4x + 5 = 0.$

56.21. $4x^5 + 11x^4 - 8x^2 - 6x + 7 = 0.$

56.22. $5x^5 + 11x^4 - 3x^3 - x^2 - x - 5 = 0.$

56.23. $3x^4 - 2x^3 - 4x^2 - 4x + 1 = 0.$

56.24. $6x^5 - 2x^4 + 7x^3 + 5x^2 - x + 7 = 0.$

56.25. $9x^4 + 9x^3 - x^2 - 66x + 40 = 0.$

Приклад 57.1. Відокремити дійсні корені многочлена

$$f(x) = 8x^5 - 10x - 3.$$

Розв'язання. Застосуємо метод Штурма до многочлена $f(x)$. Зауважимо, що в процесі ділення дозволяється, на відміну від алгоритму Евкліда, множити або ділити лише на довільні *додатні* числа, оскільки знаки остач відіграють в методі Штурма основну роль.

Оскільки $f'(x) = 40x^4 - 10 = 10(4x^4 - 1)$, то можна прийняти $F_0(x) = 4x^4 - 1$. Поділимо $f(x)$ на $F_0(x)$:

$$\begin{array}{r|l} f(x) = 8x^5 - 10x - 3 & 4x^4 - 1 = F_0(x) \\ \hline 8x^5 - 2x & 2x \\ \hline -8x - 3 & \end{array}$$

Остача $r_1(x) = -8x - 3$, тому можна взяти $F_1(x) = -r_1(x) = 8x + 3$. Далі ділимо $F_0(x)$ на $F_1(x)$:

$$
\begin{array}{rl|l}
F_0(x) = & 4x^4 - 1 & 8x + 3 \quad = F_1(x) \\
\text{(* на 2)} & 8x^4 - 2 & \hline x^3 - 3x^2 + 9x - 27 \\
& 8x^4 + 3x^3 & \\
\hline
& -3x^3 - 2 & \\
\text{(* на 8)} & -24x^3 - 16 & \\
& -24x^3 - 9x^2 & \\
\hline
& 9x^2 - 16 & \\
\text{(* на 8)} & 72x^2 - 128 & \\
& 72x^2 + 27x & \\
\hline
& -27x - 128 & \\
\text{(* на 8)} & -216x - 1024 & \\
& -216x - 81 & \\
\hline
& -943 &
\end{array}
$$

Оскільки $-r_2(x) = 943$, то можна взяти $F_2(x) = 1$.

Таким чином, ряд Штурма для многочлена $f(x)$ має наступний вигляд:

$$
\begin{aligned}
f(x) &= 8x^5 - 10x - 3, \\
F_0(x) &= 4x^4 - 1, \\
F_1(x) &= 8x + 3, \\
F_2(x) &= 1.
\end{aligned}
\tag{VI.12}
$$

Остання функція ряду Штурма $F_2(x)$ є сталою, значить, многочлен $f(x)$ не має кратних множників, тобто всі його корені – різні. В такому випадку за допомогою теореми Штурма можна знайти кількість всіх дійсних коренів многочлена. Для цього визначимо знаки многочленів ряду (VI.12) при $x = -\infty$ і $x = \infty$; при цьому, зрозуміло, достатньо дивитись лише на знаки старших коефіцієнтів і на степені многочленів. Одержимо наступну таблицю:

	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	Число змін знаків $s(x)$
$-\infty$	$-$	$+$	$-$	$+$	3
∞	$+$	$+$	$+$	$+$	0

При переході від $-\infty$ до ∞ ряд Штурма втрачає $s(-\infty) - s(\infty) = 3 - 0 = 3$ зміни знаку, тому, відповідно до теореми Штурма, многочлен має рівно 3 дійсні корені.

Для відокремлення цих коренів (знаходження таких інтервалів, у кожному з яких лежить точно один дійсний корінь) визначимо спочатку

межі дійсних коренів многочлена $f(x)$. Маємо: $A = \max\{10, 3\} = 10$, $N_0 = 1 + \frac{10}{8} = 2,25$. Отже, дійсні корені цього многочлена розташовані в інтервалі $(-2,25; 2,25)$.

Продовжимо попередню таблицю. Зауважимо, що число змін знаків в точках $x = -2,25$ і $x = 2,25$ визначати не потрібно: поза межами інтервалу $(-2,25; 2,25)$ многочлен $f(x)$ не має дійсних коренів, тому $s(-2,25) = s(-\infty) = 3$, $s(2,25) = s(\infty) = 0$.

	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$s(x)$	
$-2,25$					3	
-2	$-$	$+$	$-$	$+$	3	
-1	$-$	$+$	$-$	$+$	3	] 2 корені
0	$-$	$-$	$+$	$+$	1	
1	$-$	$+$	$+$	$+$	1	
2	$+$	$+$	$+$	$+$	0	] 1 корінь
$2,25$					0	

Таким чином, ряд Штурма многочлена $f(x)$ втрачає дві зміни знаку при переході від -1 до 0 і одну зміну знаку – від 1 до 2. Тому два корені цього многочлена належать до інтервалу $(-1; 0)$, а один – до інтервалу $(1; 2)$. Для уточнення розташування від'ємних коренів в даному випадку достатньо обчислити $f(-0,5) = 1,75 > 0$. Оскільки $f(1) < 0$ і $f(0) < 0$, то можна одразу зробити висновок (без використання ряду Штурма), що корені лежать по одному в інтервалах $(-1; -0,5)$ і $(-0,5; 0)$.

Отже, корені x_1, x_2, x_3 многочлена $f(x)$ розміщені наступним чином: $x_1 \in (-1; -0,5)$, $x_2 \in (-0,5; 0)$, $x_3 \in (1; 2)$.

Зауваження 1. Часто доцільно, щоб зменшити число спроб, визначити знаки функцій Штурма в точках, які приблизно є серединами вже досліджених проміжків. Так, у розглянутому вище прикладі спочатку з'ясувати, що на проміжку $(-2,5; 0)$ містяться два корені, а на проміжку $(0; 2,5)$ – один. Для відокремлення від'ємних коренів обчислюємо значення функцій ряду Штурма в точці $x = -1$ і робимо висновок, що обидва ці корені належать інтервалу $(-1; 0)$. Поділ цього інтервалу навпіл точкою $x = -0,5$ відокремлює корені. Щоб уточнити розташування додатного кореня, визначаємо $f(1) < 0$. Оскільки $f(2,5) > 0$, то цей корінь лежить в правій частині інтервалу $(0; 2,5)$, а саме між 1 і 2,5 і т.д.

Розв'язання в Maple. Для відшукання функцій ряду Штурма для многочлена $f(x)$ використовується команда **sturmseq(f, x)**. Відмітимо, що всі функції ряду Штурма в Maple мають старший коефіцієнт 1 або -1, то-

му одержаний результат повинен збігатись (якщо всі корені – прості) з точністю до сталого додатного множника (нагадаємо, що для спрощення обчислень в процесі ділення з остачею дозволяється множити/ділити на додатні числа). Маємо:

```
> s := sturmseq(8*x^5-10*x-3, x);
```

$$s := [x^5 - \frac{5}{4}\,x - \frac{3}{8},\ x^4 - \frac{1}{4},\ x + \frac{3}{8},\ 1]$$

Для знаходження числа змін знаків на проміжку $(a, b]$ існує команда **sturm(s, x, a, b)**, де **s** – послідовність функцій ряду Штурма, знайдена вище.

```
> sturm(s,x,-2.25,-2);
```

$$0$$

```
> sturm(s,x,-2,-1);
```

$$0$$

```
> sturm(s,x,-1,0);
```

$$2$$

```
> sturm(s,x,0,1);
```

$$0$$

```
> sturm(s,x,1,2);
```

$$1$$

```
> sturm(s,x,2,2.25);
```

$$0$$

Робимо висновок, що на півінтервалі $(-1, 0]$ є 2 корені, а на півінтервалі $(1, 2]$ лише 1 корінь.

Приклад 57.2. Відокремити дійсні корені многочлена

$$f(x) = 27x^5 - 45x^4 + 21x^3 + 366x^2 - 246x + 41.$$

Розв'язання. Неважко перевірити, що рядом Штурма для многочлена $f(x)$ буде ряд

$$\begin{aligned} f(x) &= 27x^5 - 45x^4 + 21x^3 + 366x^2 - 246x + 41, \\ F_0(x) &= 45x^4 - 60x^3 + 21x^2 + 244x - 82, \\ F_1(x) &= 18x^3 - 1119x^2 + 740x - 123, \\ F_2(x) &= -2020227x^2 + 1343882x - 223491, \\ F_3(x) &= -3x + 1. \end{aligned} \tag{VI.13}$$

Остання функція $F_3(x)$ ряду Штурма не є сталою. Це означає, що многочлен $f(x)$ має кратні корені і, застосовуючи теорему Штурма, ми знайдемо не число *всіх* його дійсних коренів, а число *різних* дійсних коренів цього многочлена без урахування їхньої кратності.

Знайдемо число $s(x)$ змін знаків в ряді Штурма при $x = -\infty$ і $x = \infty$.

	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$F_3(x)$	$s(x)$
$-\infty$	$-$	$+$	$-$	$-$	$+$	3
∞	$+$	$+$	$+$	$-$	$-$	1

Таким чином, многочлен $f(x)$ має $s(-\infty) - s(\infty) = 3 - 1 = 2$ різні дійсні корені. Визначимо інтервал, в якому містяться ці корені. Маємо: $A = \max\{45, 21, 366, 246, 41\} = 366$, $N_0 = 1 + \frac{366}{27} = 14\frac{5}{9}$. Отже, корені многочлена $f(x)$ належать інтервалу $\left(-14\frac{5}{9}, 14\frac{5}{9}\right)$.

Щоб зменшити число спроб (див. Зауваження 1), поділимо даний інтервал на дві рівні частини. Зауважимо, що $s(-14\frac{5}{9}) = s(-\infty) = 3$ і $s(14\frac{5}{9}) = s(\infty) = 1$. Маємо:

	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$F_3(x)$	$s(x)$	
$-14\frac{5}{9}$						3	] 1 корінь
0	$+$	$-$	$-$	$-$	$+$	2	
$14\frac{5}{9}$						1	] 1 корінь

Оскільки $s(-14\frac{5}{9}) - s(0) = 3 - 2 = 1$ і $s(0) - s(14\frac{5}{9}) = 2 - 1 = 1$, то один із коренів многочлена від'ємний і належить інтервалу $\left(-14\frac{5}{9}, 0\right)$; а ще один – додатний і міститься в інтервалі $\left(0, 14\frac{5}{9}\right)$.

Уточнимо місце від'ємного кореня x_1. Оскільки $f(-14\frac{5}{9}) < 0$, $f(0) > 0$, то цей корінь має непарну кратність, а значить, достатньо враховувати лише знаки значень функції $f(x)$ (не обчислюючи значення інших функцій ряду Штурма) на кінцях шуканого проміжку. Розіб'ємо інтервал $\left(-14\frac{5}{9}, 0\right)$ на два інтервали $\left(-14\frac{5}{9}, -8\right)$ і $(-8, 0)$. Оскільки $f(-8) = -1054375 < 0$, а $f(0) > 0$, подальшого дослідження потребує інтервал $(-8, 0)$. Знову розбиваємо одержаний інтервал на дві частини точкою $x = -4$ і обчислюємо значення $f(-4) = -3361 < 0$ – наступний досліджуваний інтервал $(-4, 0)$. Продовжуючи міркування далі, маємо: $f(-2) = 245 > 0$, $f(-3) = -6700 < 0$. Це означає, що $x_1 \in (-3, -2)$.

Уточнимо тепер місце додатного кореня x_2. Оскільки в точках $x = 0$ і $x = 14\frac{5}{9}$ многочлен $f(x)$ набуває однакових за знаком значень, то x_2 має парну кратність, а значить, використати лише функцію $f(x)$ для подальшого дослідження, як це було зроблено для від'ємного кореня, не вдасться.

Використаємо загальний метод: знайдемо значення функцій ряду Штурма при $x = 1$:

	$f(x)$	$F_0(x)$	$F_1(x)$	$F_2(x)$	$F_3(x)$	$s(x)$	
0	+	−	−	−	+	2	] 1 корінь
1	+	+	−	−	−	1	
$14\frac{5}{9}$						1	

Значення $s(x)$ зменшується при переході від 0 до 1, тому корінь x_2 належить інтервалу $(0; 1)$.

Отже, корені x_1, x_2 многочлена $f(x)$ розміщені наступним чином: $x_1 \in (-3, -2)$, $x_2 \in (0, 1)$.

Зауваження 2. В даному випадку додатний корінь можна легко безпосередньо знайти, використовуючи останню функцію ряду Штурма $F_3(x) = -3x+1 = -3(x-\frac{1}{3})$: множник $x - \frac{1}{3}$ буде множником 2-ої кратності многочлена $f(x)$, а значить, число $\frac{1}{3}$ – корінь 2-ої кратності.

Розв'язання в Maple. У випадку, коли многочлен має кратні дійсні корені, ряд функцій Штурма, одержаний в Maple, буде відрізнятись не лише множниками, але й навіть кількістю таких функцій в послідовності (порівн. із (VI.13)).

```
> f:=27*x^5-45*x^4+21*x^3+366*x^2-246*x+41:
  s := sturmseq(f, x);
```

$$s := [-x^4 + \frac{4}{3}x^3 - \frac{1}{3}x^2 - \frac{41}{3}x + \frac{41}{9},\ -x^3 + x^2 - \frac{2}{15}x - \frac{82}{15},\ -x^2 + \frac{371}{6}x - \frac{41}{2},\ x - \frac{223491}{673409},\ 1]$$

Це пов'язано з тим, що кратність коренів даною командою не враховується (тобто кратні корені розглядаються як прості).

Дійсно, для многочлена $f_1(x)$, який має ті ж корені, що й $f(x)$, але 1-ої кратності,

```
> factor(f);
```

$$(3\,x^3 - 3\,x^2 + 41)\,(3\,x - 1)^2$$

```
> f1:=(3*x^3-3*x^2+41)*(3*x-1):
```

ряд функцій Штурма збігається з точністю до знаку:

```
> sturmseq(f1,x);
```

$$[x^4 - \frac{4}{3}x^3 + \frac{1}{3}x^2 + \frac{41}{3}x - \frac{41}{9},\ x^3 - x^2 + \frac{1}{6}x + \frac{41}{12},\ x^2 - \frac{371}{6}x + \frac{41}{2},\ -x + \frac{44772}{134683},\ -1]$$

Однак за допомогою процедури **sturm** і в цьому випадку можна виділити інтервали, на яких містяться корені.

```
> sturm(s,x,-(14+5/9),0);
```

1

```
> sturm(s,x,0,14+5/9);
```

1

Отже, один із коренів многочлена $f(x)$ від'ємний і належить до інтервалу $\left(-14\frac{5}{9}, 0\right)$; ще один – додатний і міститься в інтервалі $\left(0, 14\frac{5}{9}\right)$.

```
> sturm(s,x,-1,0);
```

0

```
> sturm(s,x,-2,-1);
```

0

```
> sturm(s,x,-3,-2);
```

1

```
> sturm(s,x,0,1);
```

1

Отже, корені x_1, x_2 многочлена $f(x)$ розміщені наступним чином: $x_1 \in (-3, -2)$, $x_2 \in (0, 1)$.

Завдання 57. Відокремити дійсні корені многочлена:

57.1. а) $f(x) = x^5 - 3x^2 + 7$;
б) $f(x) = 27x^3 - 225x + 250$.

57.2. а) $f(x) = x^4 - 4x^3 + 10x^2 - 10$;
б) $f(x) = 25x^4 - 10x^3 - 74x^2 + 30x - 3$.

57.3. а) $f(x) = x^4 - 5x^3 + 2$;
б) $f(x) = 27x^3 - 9x^2 - 120x + 112$.

57.4. а) $f(x) = 27x^4 + 9x^3 - 6$;
б) $f(x) = 343x^3 - 21x + 2$.

57.5. а) $f(x) = x^4 - 16x^3 + 13x^2 - 1$;
б) $f(x) = 343x^3 - 2205x^2 + 13500$.

57.6. а) $f(x) = -x^5 + 5x^2 + 11$;
б) $f(x) = 315x^4 - 192x^3 + 14x^2 + 8x - 1$.

57.7. а) $f(x) = x^5 + 5x^2 - 5x + 1$;
б) $f(x) = 1331x^3 - 33x + 2$.

57.8. а) $f(x) = x^4 + 4x^2 - 8x + 17$;
б) $f(x) = 27x^3 - 81x^2 - 144x - 52$.

57.9. а) $f(x) = x^4 - 4x^3 - 17x - 9$;
б) $f(x) = 1029x^3 + 441x^2 + 63x + 3$.

57.10. а) $f(x) = x^5 - 3x^2 - 4x - 1$;
б) $f(x) = 36x^4 + 12x^3 - 251x^2 - 84x - 7$.

57.11. а) $f(x) = x^5 - 2x^3 + 7x + 7$;
б) $f(x) = 49x^4 - 14x^3 - 244x^2 + 70x - 5$.

57.12. а) $f(x) = x^5 + 10x^3 - 5x - 1$;
б) $f(x) = 27x^3 - 36x + 16$.

57.13. а) $f(x) = 2x^4 + 8x^3 + 16x^2 - 16x + 103$;
б) $f(x) = 27x^3 + 81x^2 - 63x + 11$.

57.14. а) $f(x) = 6x^4 - 8x^3 - 4$;
б) $f(x) = 245x^4 - 21x^2 - 9x + 1$.

57.15. а) $f(x) = 15x^4 - 5x^3 - 20x^2 + 3$;
б) $f(x) = 216x^3 + 324x^2 - 126x - 245$.

57.16. а) $f(x) = x^5 + 5x^2 - 2$;
б) $f(x) = 9x^4 + 3x^3 + 4x^2 - 5x + 1$.

57.17. а) $f(x) = x^5 - 15x^2 - 5x + 7$;
б) $f(x) = 75x^3 - 5x^2 - 7x + 1$.

57.18. а) $f(x) = x^5 + 5x^2 - 8x + 3$;
б) $f(x) = 9x^5 + 24x^4 + 16x^3 - 18x^2 - 48x - 32$.

57.19. а) $f(x) = x^5 - 10x^2 + 13$;
б) $f(x) = 27x^3 - 9x + 2$.

57.20. а) $f(x) = -2x^4 + 8x^3 - 8x^2 + 1$;
б) $f(x) = 343x^3 - 735x^2 + 500$.

57.21. а) $f(x) = 3x^4 - 2x^3 + 9x^2 - 6x + 7$;
б) $f(x) = 108x^3 - 1521x + 2197$.

57.22. а) $f(x) = x^4 + 2x^3 - 6$;
б) $f(x) = 9x^4 - 6x^3 - 17x^2 + 12x - 2$.

57.23. а) $f(x) = x^5 - 9x^2 + 7$;
б) $f(x) = 27x^3 - 54x^2 - 45x - 8$.

57.24. а) $f(x) = 3x^4 + x^2 + 8x - 91$;
б) $f(x) = 48x^3 - 8x^2 - 5x + 1$.

57.25. а) $f(x) = x^5 + 5x^4 - 15x + 3$;
б) $f(x) = 27x^3 - 1521x + 4394$.

5. Многочлени над полем $\mathbb{Q}$ раціональних чисел

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$ многочлен з цілими коефіцієнтами.

Для того, щоб нескоротний раціональний дріб $\frac{p}{q}$ був коренем многочлена $f(x)$ необхідно, щоб виконувались наступні умови:

1°. число p було дільником вільного члена a_0;
2°. число q було дільником старшого коефіцієнта a_n;
3°. число $p - mq$ було дільником $f(m)$ при будь-якому $m \in \mathbb{Z}$.

Умову 3° на практиці найчастіше використовують для $m = \pm 1$, тобто перевіряють, чи є числа $\frac{f(1)}{p-q}$ і $\frac{f(-1)}{p+q}$ цілими.

Теорема (ознака незвідності Айзенштайна)**.** *Якщо одночасно виконуються умови:*

1) коефіцієнти $a_{n-1}, \ldots, a_1, a_0$ многочлена з кільця $\mathbb{Z}[x]$ діляться на деяке просте число p;

2) вільний член a_0 не ділиться на p^2;

3) старший коефіцієнт a_n не ділиться p,

то многочлен $f(x)$ незвідний над полем $\mathbb{Q}$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 58.1. Розв'язати рівняння:

$$12x^6 + 8x^5 - 97x^4 + x^3 + 100x^2 - 57x + 9 = 0.$$

Розв'язання. Знайдемо спочатку раціональні розв'язки цього рівняння (якщо вони є). Перевіримо, чи є числа $0, 1, -1$ коренями многочлена $f(x) = 12x^6 + 8x^5 - 97x^4 + x^3 + 100x^2 - 57x + 9$. Оскільки вільний член многочлена $f(x)$ відмінний від 0, то число 0 не є коренем. Числа 1 і -1 також не є коренями цього многочлена, оскільки $f(1) = -24$, $f(-1) = 72$.

Вільний член має наступні дільники p: $\pm1;\pm3;\pm9$. Випишемо тепер всі дільники q старшого коефіцієнта: $\pm1;\pm2;\pm3;\pm4;\pm6;\pm12$. Отже, раціональні корені $\frac{p}{q}$ необхідно шукати серед чисел виду:

$$\pm3;\ \ \pm9;\ \ \pm\frac{1}{2};\ \ \pm\frac{3}{2};\ \ \pm\frac{9}{2};\ \ \pm\frac{1}{3};\ \ \pm\frac{1}{4};\ \ \pm\frac{3}{4};\ \ \pm\frac{9}{4};\ \ \pm\frac{1}{6};\ \ \pm\frac{1}{12}. \quad \text{(VI.14)}$$

(Числа ±1 вже було досліджено вище, тому частки $\frac{p}{q}=\pm1$ виключаємо з розгляду.)

Дійсні корені многочлена $f(x)$ повинні міститись в інтервалі $(-N_0;N_0)$ (див. §4). Маємо: $A=\max\{8,97,1,100,57,9\}=100$, тоді $N_0=1+\frac{A}{|a_n|}=1+\frac{100}{12}=9\frac{1}{3}$. Отже, корені многочлена містяться в інтервалі $(-9\frac{1}{3};9\frac{1}{3})$. Як бачимо, до цього інтервалу належать всі числа множини (VI.14) (якби деякі числа множини (VI.14) до інтервалу не належали, їх можна було б виключити із подальшого розгляду).

Визначимо, для яких чисел $\frac{p}{q}$ ряду (VI.14) виконується умова 3). Для цього перевіримо, чи є числа $\frac{-24}{p-q}$ і $\frac{72}{p+q}$ цілими. (Зрозуміло, що для дробів, для яких число $\frac{-24}{p-q}$ не є цілим (позначені знаком "$-$") знаходити значення $\frac{72}{p+q}$ не потрібно).

$\frac{p}{q}$	3	-3	9	-9	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{3}{2}$	$-\frac{3}{2}$	$\frac{9}{2}$	$-\frac{9}{2}$	$\frac{1}{3}$
$p-q$	2	-4	8	-10	-1	-3	1	-5	7	-11	-2
$\frac{-24}{p-q}$	$+$	$+$	$+$	$-$	$+$	$+$	$+$	$-$	$-$	$-$	$+$
$p+q$	4	-2	10		3	1	5				4
$\frac{72}{p+q}$	$+$	$+$	$-$		$+$	$+$	$-$				$+$

$\frac{p}{q}$	$-\frac{1}{3}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{3}{4}$	$-\frac{3}{4}$	$\frac{9}{4}$	$-\frac{9}{4}$	$\frac{1}{6}$	$-\frac{1}{6}$	$\frac{1}{12}$	$-\frac{1}{12}$
$p-q$	-4	-3	-5	-1	-7	5	-13	-5	-7	-11	-13
$\frac{-24}{p-q}$	$+$	$+$	$-$	$+$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$p+q$	2	5		7							
$\frac{72}{p+q}$	$+$	$-$		$-$							

Таким чином, умова 3) не виконується для чисел $\pm9;\ \pm\frac{3}{2};\ \pm\frac{9}{2};\ \pm\frac{1}{4};\ \pm\frac{3}{4};\ \pm\frac{9}{4};\ \pm\frac{1}{6};\ \pm\frac{1}{12}$. Залишається дослідити наступні значення:

$$\pm3;\ \ \pm\frac{1}{2};\ \ \pm\frac{1}{3}.$$

Для цього застосуємо схему Горнера. Спочатку перевіримо, чи є число 3 коренем заданого рівняння:

	12	8	−97	1	100	−57	9
3	12	44	35	106	418	1197	3600

Отже, $f(3) = 3600$, число 3 не є коренем. Далі перевіряємо число -3. Продовжуємо схему Горнера:

	12	8	−97	1	100	−57	9
3	12	44	35	106	418	1197	3600
−3	12	−28	−13	40	−20	3	0

Оскільки $f(-3) = 0$, число -3 є коренем рівняння. Діленням на $x + 3$ можна понизити степінь рівняння. Одержимо рівняння: $12x^5 - 28x^4 - 13x^3 + 40x^2 - 20x + 3 = 0$, коефіцієнти якого розташовані в останньому рядку схеми Горнера. Тому для подальших досліджень використовуємо коефіцієнти останнього рядка (числа цього рядка виділяємо).

Корінь $x = -3$ може мати кратність > 1. Тому знову застосуємо схему Горнера для числа -3:

	12	8	−97	1	100	−57	9
3	12	44	35	106	418	1197	3600
−3	**12**	**−28**	**−13**	**40**	**−20**	**3**	0
−3	12	−64	179	−497	1471	−4410	

Число -3 є простим коренем заданого рівняння. Продовжимо перевірку:

	12	8	−97	1	100	−57	9	
3	12	44	35	106	418	1197	3600	
−3	**12**	**−28**	**−13**	**40**	**−20**	**3**	0	
−3	12	−64	179	−497	1471	−4410		
$\frac{1}{2}$	**12**	**−22**	**−24**	**28**	**−6**	0		
$\frac{1}{2}$	**12**	**−16**	**−32**	**12**	0			
$\frac{1}{2}$	12	−10	−37	$-\frac{13}{2}$				число $\frac{1}{2}$ є коренем кратності 2
$-\frac{1}{2}$	12	−22	−21	4				число $-\frac{1}{2}$ не є коренем
$\frac{1}{3}$	**12**	**−12**	**−36**	0				
$\frac{1}{3}$	12	−8	$-\frac{116}{3}$					число $\frac{1}{3}$ є простим коренем
$-\frac{1}{3}$	12	−12	$-\frac{104}{3}$					число $-\frac{1}{3}$ не є коренем

Таким чином, задане рівняння має лише 3 різні раціональні корені: $-3, \frac{1}{2}$ і $\frac{1}{3}$. Щоб знайти решту коренів, прирівняємо до нуля частку $12x^2-12x-36$, одержану від послідовного ділення многочлена $f(x)$ на $(x+3)(x-\frac{1}{2})^2(x-\frac{1}{3})$ (її коефіцієнти містяться в останньому виділеному рядку схеми Горнера). Маємо: $12x^2-12x-36=0$, тобто $x^2-x-3=0$. Це рівняння має корені $\frac{1\pm\sqrt{13}}{2}$. А отже, задане рівняння має

прості корені: $-3, \frac{1}{3}; \frac{1\pm\sqrt{13}}{2}$
корінь $\frac{1}{2}$ кратності 2.

Зауважимо, що, одержавши частку, що є квадратним тричленом (в нашому випадку $12x^2-12x-36$), подальшу перевірку раціональних дробів ряду (VI.14) можна не проводити, а одразу розв'язати квадратне рівняння.

Розробка процедур. Для перевірки остаточного результату достатньо застосувати команду **solve** або команду **roots**. Для перевірки проміжних обчислень створимо процедуру **Qroots**, за допомогою якої можна буде знаходити раціональні корені многочлена з раціональними коефіцієнтами.

Задаємо множину R, до якої будемо заносити корені многочлена $f(x)$:

```
> R:={}:
```

Якщо вільний член a_0 заданого многочлена дорівнює 0, то число 0 є його коренем (число 0 додаємо до множини R) і ділимо $f(x)$ на x, що дасть змогу працювати із многочленом меншого степеня. Якщо вільний член отриманого многочлена також рівний 0, то знову ділимо на x і т.д., доки не отримаємо многочлен, вільний член якого відмінний від 0. При цьому необхідно ввести локальну змінну $f1$:

```
> f1:=f:
> a[0]:=coeff(f,x,0):
  if a[0]=0 then R:=R union {0};
     while rem(f1,x,x)=0 do f1:=quo(f1,x,x); end do;
  end if;
```

Далі перевіряємо, чи є коренем многочлена $f(x)$ число 1. Якщо так, то додаємо число 1 до множини R і ділимо $f(x)$ на $x-1$ доки це можливо:

```
> if subs({x=1},f1)=0 then R:=R union {1};
     while rem(f1,x-1,x)=0 do f1:=quo(f1,x-1,x); end do;
  end if;
```

Аналогічно для числа -1:

```
> if subs({x=-1},f1)=0 then R:=R union {-1};
     while rem(f1,x+1,x)=0 do f1:=quo(f1,x+1,x); end do;
  end if;
```

В результаті отримаємо многочлен $f_1(x) = \frac{f(x)}{x^{k_1}(x-1)^{k_2}(x-1)^{k_2}}$, де k_1, k_2, k_3 – кратності коренів 0, 1 і -1 відповідно, зокрема, можливо, що $k_i = 0$, $i \in \overline{1,3}$.

Знайдемо тепер дільники вільного члена (множина P) і дільники старшого коефіцієнта (множина Q):

```
> a[0]=coeff(f1,x,0);
  P:=divisors(a[0]);
  print('P'=P);
> n:=degree(f1):
  a[n];=coeff(f1,x,n);
  Q:=divisors(a[n]);
  print('Q'=Q);
```

(команда **divisors** міститься в спеціалізованому пакеті **numtheory**, тому в описі процедури слід буде додати рядок uses numtheory).

Тепер знаходимо множину M всіх можливих часток $a = \frac{p}{q}$ і $b = -\frac{p}{q}$, де $p \in P$, $q \in Q$:

```
> M:={}:
  for i from 1 to nops(P) do
     for j from 1 to nops(Q) do
       a:=P[i]/Q[j]; b:=-P[i]/Q[j]; M:=M union {a,b};
     end do;
  end do;
```

Із цієї множини вилучаємо числа 1 і -1 (вони не є коренями многочлена $f_1(x)$) і виводимо множину M на екран:

```
> M:=M minus {1,-1};
  print(M);
```

Далі досліджуємо елементи множини M. Спочатку знаходимо інтервал $(-N_0; N_0)$, в якому містяться раціональні корені многочлена $f_1(x)$. Для цього зручно виділити набір коефіцієнтів цього многочлена за допомогою команди **CoefficientList(f1,x)** із пакету **PolynomialTools**. (Відмітимо, опція termorder=reverse встановлена для того, щоб коефіцієнти многочлена було розміщено в порядку спадання степенів; за замовчуванням порядок слідування коефіцієнтів – зворотній).

```
> cl:=CoefficientList(f1,x,termorder=reverse);
```

Далі знаходимо числа A, N_0:

```
> A:=max(seq(abs(cl[i]),i=2..n));
  N0:=1+A/abs(cl[1]);
```

і перевіряємо, чи всі елементи множини M належать до інтервалу $(-N_0; N_0)$; якщо якийсь із елементів не належить, то його вилучаємо із множини M:

```
> for i from 1 to nops(M) do
     if  M[i]<=-N0 or M[i]>=N0  then M:=M minus {M[i]}; end if;
  end do:
```

Тепер знаходимо значення многочлена $f_1(x)$ в точках 1 і -1:

```
> fp1:=subs({x=1},f1);  fm1:=subs({x=-1},f1);
```

Результати наступних дій будемо заносити в таблицю розмірності $5 \times (m+1)$, де m – кількість елементів множини M.

```
> m:=nops(M):
  B := Array(1..5,1..nops(M)+1):
```

Заповнюємо перший рядок цієї таблиці. В клітинку $B[1,1]$ заносимо символ $\frac{p}{q}$. В клітинки $B[1,2]$, $B[1,3]$, ..., $B[1,m+1]$ вписуємо елементи множини M:

```
> B[1,1]:=‘p‘/‘q‘:
  for j from 2 to m+1 do B[1,j]:=M[j-1]: end do:
```

Тепер заповнюємо другий рядок. В клітинку $B[2,1]$ заносимо позначення $p-q$, в клітинки $B[2,2]$, $B[2,3]$, ..., $B[2,m+1]$ заносимо значення $p-q$ для відповідних чисел $\frac{p}{q}$ (за допомогою команди **numer(c)** знаходимо чисельник дробу $c=\frac{p}{q}$, а команди **denom(c)** – знаменник).

```
> B[2,1]:=‘p-q‘:
```

```
> for j from 2 to m+1 do
     B[2,j]:=numer(B[1,j])-denom(B[1,j]):
  end do:
```

Далі заповнюємо третій рядок. В клітинку $B[3,1]$ заносимо позначення $\frac{f(1)}{(p-q)}$, в клітинках $B[3,2]$, $B[3,3]$, ..., $B[3,m+1]$ ставимо знак $+$, якщо частка $\frac{f(1)}{(p-q)}$ – число ціле, і знак – в іншому випадку.

```
> B[3,1]:=‘f(1)‘/‘p-q‘:
```

```
> for j from 2 to m+1 do
     if (fp1 mod B[2,j])=0 then B[3,j]:=‘+‘
     else B[3,j]:=‘-‘
     end if;
  end do;
```

Четвертий і п’ятий рядки заповнюємо аналогічно з єдиною відмінністю: заповнюємо лише ті клітинки, над якими в 3-му рядку стояв знак $+$.

```
> B[4,1]:=‘p+q‘: B[5,1]:=‘f(-1)‘/‘p+q‘:
```

```
> for j from 2 to m+1 do
    if B[3,j]=‘+‘ then B[4,j]:= numer(B[1,j])+denom(B[1,j]);
      if (fm1 mod B[4,j])=0 then B[5,j]:=‘+‘
      else B[5,j]:=‘-‘
      end if;
    else B[4,j]:=‘‘; B[5,j]:=‘‘
    end if;
  end do;
```

Виводимо таблицю B на екран. Відмітимо, що якщо множина M має досить велику кількість елементів (а значить, таблиця B матиме велику кількість стовпців), то, щоб побачити всю таблицю повістю, слід ввести:

```
> interface(rtablesize=m+1):
  print(B);
```

Далі для кожної клітинки 5-го рядка $B[5,i]$, в якій стоїть знак $+$, визначаємо, чи є елемент $\frac{p}{q} = B[1,i]$ коренем многочлена $f_1(x)$. Якщо так, заносимо цей елемент до множини R коренів.

```
> for i from 2 to m do
    if B[5,i]=‘+‘ and subs({x=B[1,i]},f)=0 then
       R:=R union {B[1,i]};
    end if;
  end do:
```

В результаті отримаємо множину R раціональних коренів заданого многочлена $f(x)$:

```
> print('R'=R);
```

Залишається знайти кратності цих коренів. Для цього можемо використати процедуру **rootMult**, створену при розв'язанні Прикладу 42.1:

```
> for i from 1 to nops(R) do
  k[i]:=rootMult(f,R[i]);
  print([R[i],k[i]])
  end do;
```

Відповідь отримуємо у вигляді набору пар $[\frac{p}{q}, k]$, де $\frac{p}{q}$ – раціональний корінь многочлена $f(x)$ кратності k.

Код даної процедури наступний:

```
Qroots:=proc(f)
uses numtheory,PolynomialTools;
local i,R,f1,a,P,Q,M,n,j,b,cl,fp1,fm1,A,N0,m,B,k;
   R:={ }: f1:=f:
   a[0]:=coeff(f,x,0):
```

```
    if a[0]=0 then R:=R union {0};
       while rem(f1,x,x)=0 do f1:=quo(f1,x,x); end do;
    end if;
    if subs({x=1},f1)=0 then R:=R union {1};
       while rem(f1,x-1,x)=0 do f1:=quo(f1,x-1,x); end do;
    end if;
    if subs({x=-1},f1)=0 then R:=R union {-1};
       while rem(f1,x+1,x)=0 do f1:=quo(f1,x+1,x); end do;
    end if;
    a[0]:=coeff(f1,x,0): P:=divisors(a[0]); print('P'=P);
    n:=degree(f1): a[n]:=coeff(f1,x,n): Q:=divisors(a[n]); print('Q'=Q);
    M:={}:
    for i from 1 to nops(P) do
       for j from 1 to nops(Q) do
          a:=P[i]/Q[j]; b:=-P[i]/Q[j]; M:=M union {a,b };
       end do;
    end do;
    M:=M minus {1,-1 }; print(M);
    cl:=CoefficientList(f1,x,termorder=reverse);
    A:=max(seq(abs(cl[i]),i=2..n)); N0:=1+A/abs(cl[1]);
    for i from 1 to nops(M) do
       if M[i]<=-N0 or M[i]>=N0 then M:=M minus {M[i] }; end if;
    end do:
    fp1:=subs({x=1 },f1); fm1:=subs( {x=-1 },f1);
    m:=nops(M): B := Array(1..5,1..nops(M)+1):
    B[1,1]:=`p`/`q`:
    for j from 2 to m+1 do B[1,j]:=M[j-1]: end do:
    B[2,1]:=`p-q`:
    for j from 2 to m+1 do B[2,j]:=numer(B[1,j])-denom(B[1,j]): end do:
    B[3,1]:=`f(1)`/`p-q`:
    for j from 2 to m+1 do
       if (fp1 mod B[2,j])=0 then B[3,j]:=`+` else B[3,j]:=`-` end if;
    end do;
    B[4,1]:=`p+q`: B[5,1]:=`f(-1)/(p+q)`:
    for j from 2 to m+1 do
       if B[3,j]=`+` then B[4,j]:=numer(B[1,j])+denom(B[1,j]);
          if (fm1 mod B[4,j])=0 then B[5,j]:=`+` else B[5,j]:=`-` end if;
       else B[4,j]:=``; B[5,j]:=``
       end if;
    end do;
    interface(rtablesize=m+1): print(B);
    for i from 2 to m do
       if B[5,i]=`+` and subs({x=B[1,i]},f)=0 then R:=R union {B[1,i]};
       end if;
    end do:
    print('R'=R);
    for i from 1 to nops(R) do k[i]:=rootMult(f,R[i]); print([R[i],k[i]])
       end do;
 end proc:
```

Розв'язання в Maple. Для перевірки остаточного результату застосовуємо або команду **solve** (яка знайде всі розв'язки без урахування їхньої кратності):

```
> f:=12*x^6+8*x^5-97*x^4+x^3+100*x^2-57*x+9:
> solve(f);
```

$$\frac{1}{3},\ -3,\ \frac{1}{2}+\frac{\sqrt{13}}{2},\ \frac{1}{2}-\frac{\sqrt{13}}{2},\ \frac{1}{2},\ \frac{1}{2}$$

або команду **roots** (яка знайде всі дійсні розв'язки та їхні кратності):

```
> roots(f);
```

$$[[\frac{1}{2},\ 2],\ [\frac{1}{3},\ 1],\ [-3,\ 1]]$$

Для покрокової перевірки використаємо створену процедуру **Qroots**:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> Qroots(12*x^6+8*x^5-97*x^4+x^3+100*x^2-57*x+9);
```

$$P = \{1,\ 3,\ 9\}$$

$$Q = \{1,\ 2,\ 3,\ 4,\ 6,\ 12\}$$

$$\{-9,\ -3,\ 3,\ 9,\ \frac{-9}{2},\ \frac{-9}{4},\ \frac{-3}{2},\ \frac{-3}{4},\ \frac{-1}{2},\ \frac{-1}{3},\ \frac{-1}{4},\ \frac{-1}{6},\ \frac{-1}{12},\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{6},\ \frac{1}{12},\ \frac{3}{2},\ \frac{3}{4},\ \frac{9}{2},\ \frac{9}{4}\}$$

$$\left[\begin{array}{cccccccccccccccccccccc}
\frac{p}{q} & -9 & -3 & 3 & 9 & \frac{-9}{2} & \frac{-9}{4} & \frac{-3}{2} & \frac{-3}{4} & \frac{-1}{2} & \frac{-1}{3} & \frac{-1}{4} & \frac{-1}{6} & \frac{-1}{12} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{6} & \frac{1}{12} & \frac{3}{2} & \frac{3}{4} & \frac{9}{2} & \frac{9}{4} \\
p-q & -10 & -4 & 2 & 8 & -11 & -13 & -5 & -7 & -3 & -4 & -5 & -7 & -13 & -1 & -2 & -3 & -5 & -11 & 1 & -1 & 7 & 5 \\
\frac{f(1)}{p-q} & - & + & + & + & - & - & - & - & + & + & - & - & - & + & + & + & - & - & + & + & - & - \\
p+q & & -2 & 4 & 10 & & & & & 1 & 2 & & & & 3 & 4 & 5 & & & 5 & 7 & & \\
\frac{f(-1)}{p+q} & & + & + & - & & & & & + & + & & & & + & + & - & & & - & - & &
\end{array}\right]$$

$$R = \{-3,\ \frac{1}{2},\ \frac{1}{3}\}$$

$$[-3,\ 1]$$

$$[\frac{1}{2},\ 2]$$

$$[\frac{1}{3},\ 1]$$

Отже, многочлен $f(x)$ має 3 раціональні корені: $-3, \frac{1}{2}, \frac{1}{3}$ кратності $1, 2, 1$ відповідно. Щоб знайти решту коренів, треба розділити многочлен $f(x)$ на добуток $(x+3)(x-\frac{1}{2})^2(x-3)$ і знайти корені отриманої частки:

```
> g:=quo(12*x^6+8*x^5-97*x^4+x^3+100*x^2-57*x+9,
  (x+3)*(x-1/2)^2*(x-1/3),x);
```

$$g := 12\,x^2 - 12\,x - 36$$

```
> solve(g);
```

$$\frac{1}{2}+\frac{\sqrt{13}}{2}, \frac{1}{2}-\frac{\sqrt{13}}{2}$$

Таким чином, задане рівняння окрім розв'язків $-3, \frac{1}{2}, \frac{1}{3}$ кратності $1, 2, 1$ відповідно має ще й розв'язки $\frac{1\pm\sqrt{13}}{2}$ 1-ої кратності.

Приклад 58.2. Розв'язати рівняння:

$$2x^7 + x^6 - 15x^5 + 5x^4 + 13x^3 - 6x^2 = 0.$$

Розв'язання. Перевіримо, чи є числа $0, 1, -1$ коренями многочлена $f(x) = 2x^7 + x^6 - 15x^5 + 5x^4 + 13x^3 - 6x^2$. Оскільки вільний член многочлена $f(x)$ дорівнює 0, то число 0 є коренем. Розділимо $f(x)$ на x^2, отримаємо многочлен $2x^5 + x^4 - 15x^3 + 5x^2 + 13x - 6$, для якого число 0 не є коренем.

Далі перевіряємо, чи є числа 1 і -1 коренями цього многочлена. Оскільки $f(1) = 0$ і $f(-1) = 0$, то 1 і -1 є коренями. Знайдемо їхню кратність. В даному випадку можна використати обидва способи: і критерій кратності кореня (за допомогою похідної), і схему Горнера. Зауважимо, що, використовуючи схему Горнера, можна одразу знайти і частку. Маємо:

	2	1	−15	5	13	−6
1	2	3	−12	−7	6	0
1	2	5	−7	−14	−8	

Отже, кратність кореня $x = 1$ дорівнює 1. В результаті ділення многочлена $2x^5 + x^4 - 15x^3 + 5x^2 + 13x - 6$ на $x - 1$ отримаємо частку $2x^4 + 3x^3 - 12x^2 - 7x + 6$. Знайдемо кратність кореня $x = -1$:

	2	3	−12	−7	6
−1	2	1	−13	6	0
−1	2	−1	−12	18	

Отже, кратність кореня $x = -1$ також дорівнює 1.

Решту коренів заданого многочлена шукатимемо серед коренів многочлена $f_1(x) = \frac{f(x)}{x^2(x-1)(x+1)} = 2x^3 + x^2 - 13x + 6$.

Вільний член многочлена $f_1(x)$ має наступні дільники p: $\pm1; \pm2; \pm3; \pm6$. Випишемо тепер всі дільники q старшого коефіцієнта: $\pm1; \pm2$.

Отже, раціональні корені $\frac{p}{q}$ многочлена $f_1(x)$ необхідно шукати серед чисел виду:

$$\pm2; \quad \pm3; \quad \pm6; \quad \pm\frac{1}{2}; \quad \pm\frac{3}{2}. \tag{VI.15}$$

Дійсні корені многочлена $f_1(x)$ повинні міститись в інтервалі $(-N_0; N_0)$ (див. §4). Маємо: $|a_n| = \max\{1, 13, 6\} = 13$, тоді $N_0 = 1 + \frac{A}{|a_n|} = 1 + \frac{13}{2} = 7,5$. Отже, корені многочлена містяться в інтервалі $(-7,5; 7,5)$. До цього інтервалу належать всі числа множини (VI.15).

Далі знаходимо значення $f_1(1) = -4$, $f_1(-1) = 18$ і для кожного числа $\frac{p}{q}$ із (VI.15) перевіряємо, чи є числа $\frac{-4}{p-q}$ і $\frac{18}{p+q}$ цілими.

$\frac{p}{q}$	2	-2	3	-3	6	-6	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{3}{2}$	$-\frac{3}{2}$
$p-q$	1	-3	2	-4	5	-7	-1	-3	1	-5
$\frac{-4}{p-q}$	$+$	$-$	$+$	$+$	$-$	$-$	$+$	$-$	$+$	$-$
$p+q$	3		4	-2			3		5	
$\frac{72}{p+q}$	$+$		$-$	$+$			$+$		$-$	

Залишається дослідити наступні значення: $2; -3; \frac{1}{2}$. Для цього застосуємо схему Горнера.

	2	1	-13	6
2	**2**	**5**	**-3**	0
2	2	11	19	

Отже, число 2 є коренем кратності 1. При цьому $\frac{f(x)}{x-2} = 2x^2 - 5x - 3$. Решту коренів зручніше знайти, розв'язавши квадратне рівняння $2x^2 - 5x - 3 = 0$. Розв'язками даного рівняння є: $\frac{1}{2}$ і -3. Значить, коренями многочлена $f_1(x)$ є числа $2, \frac{1}{2}, -3$ (всі вони є простими коренями). Тоді коренями многочлена $f(x)$ (тобто розв'язками заданого рівняння) є:

простi корені: $2, \frac{1}{2}, -3, 1, -1$;

корінь 0 кратності 2.

Розв'язання в Maple. Застосовуємо процедуру **Qroots** із Прикладу 58.1.

```
> read(‘e:/atchlib.m‘); with(atchlib):

> Qroots(2*x^7+x^6-15*x^5+5*x^4+13*x^3-6*x^2);
```

$$P = \{1,\ 2,\ 3,\ 6\}$$

$$Q = \{1,\ 2\}$$

$$\{-6,\ -3,\ -2,\ 2,\ 3,\ 6,\ \frac{-3}{2},\ \frac{-1}{2},\ \frac{1}{2},\ \frac{3}{2}\}$$

$$\left[\begin{array}{cccccccccc}
\frac{p}{q} & -6 & -3 & -2 & 2 & 3 & 6 & \frac{-3}{2} & \frac{-1}{2} & \frac{1}{2} & \frac{3}{2} \\
p-q & -7 & -4 & -3 & 1 & 2 & 5 & -5 & -3 & -1 & 1 \\
\frac{f(1)}{p-q} & - & + & - & + & + & - & - & - & + & + \\
p+q & & -2 & & 3 & 4 & & & & 3 & 5 \\
\frac{f(-1)}{p+q} & & + & & + & - & & & & + & -
\end{array}\right]$$

$$R = \{-3,\ -1,\ 0,\ 1,\ 2,\ \frac{1}{2}\}$$

$$[-3,\ 1]$$
$$[-1,\ 1]$$
$$[0,\ 2]$$
$$[1,\ 1]$$
$$[2,\ 1]$$
$$[\frac{1}{2},\ 1]$$

Таким чином, многочлен $f(x)$ має прості корені: $-3, -1, 1, 2, \frac{1}{2}$ і подвійний корінь 0. Можливо, многочлен $f(x)$ має ще й корені, які не є раціональними числами. Знаходимо частку $\frac{f(x)}{x^2(x+3)(x+1)(x-1)(x-2)(x-\frac{1}{2})}$:

```
> g:=quo(2*x^7+x^6-15*x^5+5*x^4+13*x^3-6*x^2,
  x^2*(x+3)*(x+1)*(x-1)*(x-2)*(x-1/2),x);
```

$$g := 2$$

Многочлен $g(x)$, одержаний в частці, коренів не має, отже, многочлен $f(x)$ має лише раціональні корені, знайдені вище.

Завдання 58. Розв'язати рівняння:

58.1. $16x^5 - 104x^4 + 265x^3 - 231x^2 - 172x - 24 = 0.$

58.2. $9x^5 - 84x^4 + 244x^3 - 269x^2 + 124x - 20 = 0.$

58.3. $9x^5 - 6x^4 + 10x^3 + 84x^2 - 59x + 10 = 0.$

58.4. $36x^5 - 141x^4 + 97x^3 + 288x^2 + 52x - 32 = 0.$

58.5. $9x^5 + 6x^4 - 17x^3 - 48x^2 - 26x - 4 = 0.$

58.6. $48x^5 - 88x^4 - 213x^3 - 23x^2 + 22x + 4 = 0.$

58.7. $5x^5 - x^4 - 35x^3 - 13x^2 + 104x - 20 = 0.$

58.8. $108x^5 + 216x^4 - 189x^3 - 29x^2 + 21x - 2 = 0.$

58.9. $9x^5 + 89x^4 + 359x^3 + 715x^2 + 564x - 72 = 0.$

58.10. $9x^5 - 59x^4 + 98x^3 + 20x^2 - 88x - 32 = 0.$

58.11. $18x^5 - 51x^4 + 62x^3 - 18x^2 - 16x + 8 = 0.$

58.12. $4x^5 + 29x^4 + 68x^3 + 35x^2 - 38x - 30 = 0.$

58.13. $3x^5 - 4x^4 - x^3 + 38x^2 + 48x + 16 = 0.$

58.14. $9x^5 - 7x^4 - 38x^3 - 17x^2 + 7x + 2 = 0.$

58.15. $108x^5 - 396x^4 + 375x^3 + 266x^2 - 113x + 10 = 0.$

58.16. $27x^5 + 99x^4 - 12x^3 - 80x^2 + 16 = 0.$

58.17. $16x^5 + 72x^4 + 137x^3 + 157x^2 - 109x + 15 = 0.$

58.18. $75x^5 + 70x^4 - 437x^3 + 364x^2 - 96x + 8 = 0.$

58.19. $16x^5 - 24x^4 - 167x^3 + 168x^2 + 45x - 54 = 0.$

58.20. $12x^5 - 4x^4 - 5x^3 + 20x^2 + 18x + 4 = 0.$

58.21. $36x^5 + 219x^4 + 487x^3 + 328x^2 + 12x - 32 = 0.$

58.22. $9x^5 - 2x^4 + 18x^3 + 68x^2 + 29x - 10 = 0.$

58.23. $20x^5 - 116x^4 + 241x^3 - 132x^2 + 3x + 8 = 0.$

58.24. $9x^5 - 33x^4 + 25x^3 + 43x^2 - 24x - 20 = 0.$

58.25. $9x^5 + 16x^4 - 76x^3 - 200x^2 - 96x + 32 = 0.$

Приклад 59. Довести, що число $\sqrt[2011]{7}$ – ірраціональне.

Розв'язання. Спосіб I. Дійсне число $\sqrt[2011]{7}$ є коренем многочлена $f(x) = x^{2011} - 7$. Покажемо, що многочлен $f(x)$ раціональних коренів не має. Оскільки старший коефіцієнт многочлена $f(x)$ дорівнює 1, то всі його раціональні корені повинні бути цілими. Водночас, цілі корені нормованого многочлена повинні бути дільниками вільного члена, тобто числа -7. Такими цілими числами є лише ± 1, ± 7. Жодне із цих чисел не є коренем многочлена $f(x)$. Отже, число $\sqrt[2011]{7}$ є ірраціональним.

Спосіб II. Припустимо, що дійсне число $\sqrt[2011]{7}$ є раціональним. Тоді його можна записати у вигляді $\sqrt[2011]{7} = \frac{m}{n}$, де $m \in \mathbb{Z}$, $n \in \mathbb{N}$, $(m, n) = 1$. Піднесемо обидві частини даної рівності до 2011-го степеня і домножимо обидві частини на n^{2011}:

$$7n^{2011} = m^{2011}.$$

Ліва частина даної рівності ділиться на 7, тому $m^{2011} \vdots 7$. Звідси, за властивістю 3 п.1 §3 розд.I [1], $m \vdots 7$. Тоді $m = 7m_1$, $m_1 \in \mathbb{Z}$. Одержимо:

$7n^{2011} = 7^{2011}m^{2011}$, звідки $n^{2011} = 7^{2010}m^{2011}$, а значить, $n^{2011} \vdots 7$. Тоді $n \vdots 7$, і значить, $(n, m) \vdots 7$, що суперечить вибору n і m. Отже, припущення невірне і число $\sqrt[2011]{7}$ є ірраціональним.

Розв'язання в Maple. В Maple визначити, чи є число a раціональним, чи ні, можна за допомогою команди **type(a, rational)**. Якщо $a \in \mathbb{Q}$, то результатом є true, в іншому випадку – false.

```
> type(root[2011](7),rational);
```

false

Тепер визначимо аналогічно, чи є задане число дійсним:

```
> type(root[2011](7),realcons);
```

true

Отже, число $\sqrt[2011]{7}$ не є раціональним, але є дійсним, значить, число $\sqrt[2011]{7}$ – ірраціональне.

Завдання 59. Довести, що число a – ірраціональне, якщо:

59.1. $a = \sqrt[16]{29}$.

59.2. $a = \sqrt[24]{151}$.

59.3. $a = \sqrt[21]{57}$.

59.4. $a = \sqrt[6]{257}$.

59.5. $a = \sqrt[13]{5}$.

59.6. $a = \sqrt[5]{134}$.

59.7. $a = \sqrt[43]{17}$.

59.8. $a = \sqrt[16]{30}$.

59.9. $a = \sqrt[5]{91}$.

59.10. $a = \sqrt[7]{19}$.

59.11. $a = \sqrt[14]{263}$.

59.12. $a = \sqrt[3]{1001}$.

59.13. $a = \sqrt[18]{37}$.

59.14. $a = \sqrt[7]{237}$.

59.15. $a = \sqrt[17]{101}$.

59.16. $a = \sqrt[15]{41}$.

59.17. $a = \sqrt[14]{62}$.

59.18. $a = \sqrt[53]{121}$.

59.19. $a = \sqrt[20]{2}$.

59.20. $a = \sqrt[12]{61}$.

59.21. $a = \sqrt[9]{59}$.

59.22. $a = \sqrt[19]{3}$.

59.23. $a = \sqrt[42]{23}$.

59.24. $a = \sqrt[18]{32}$.

59.25. $a = \sqrt[11]{19}$.

Приклад 60. Довести, що многочлени

$$f(x) = x^6 - 2x^4 + 4x^3 + 2$$

і

$$g(x) = x^4 + 10x^3 + 24x^2 + 25x + 13$$

– незвідні над полем $\mathbb{Q}$ раціональних чисел.

Розв'язання. Застосуємо ознаку Айзенштайна. Оскільки:

1) всі коефіцієнти многочлена $f(x)$, крім старшого, діляться на просте число $p = 2$;

2) вільний член не ділиться на $p^2 = 4$;

3) старший коефіцієнт не ділиться на $p = 2$,

то за ознкою Айзенштайна многочлен є незвідним над полем $\mathbb{Q}$.

До многочлена $g(x)$ безпосередньо застосувати ознаку Айзенштайна не можна. Зробимо заміну: $x = y - 1$. Маємо:

$$h(y) = g(y-1) = (y-1)^4 + 10(y-1)^3 + 24(y-1)^2 + 25(y-1) + 13 = \\ = y^4 + 6y^3 + 3y + 3.$$

1) всі коефіцієнти многочлена $h(y)$, крім старшого, діляться на просте число 3;

2) вільний член не ділиться на 9;

3) старший коефіцієнт не ділиться на 3.

Це означає, що многочлен $h(y)$ є незвідним над полем $\mathbb{Q}$, а тому і многочлен $g(x)$ теж є незвідним над $\mathbb{Q}$.

Розробка процедур. Створимо процедуру **EisensteinsCrit(f)** для перевірки, чи можна до заданого многочлена $f(x)$ застосувати ознаку Айзенштайна. В ході процедури:

1) перевіряємо, чи є коефіцієнти многочлена $f(x)$ цілими числами; якщо ні, з'являється повідомлення про помилку:

```
> if not type(f, polynom(integer)) then
     error "wrong coefficients";
  end if;
```

2) виділяємо коефіцієнти a_i многочлена $f(x)$:

```
> n:=degree(f,x):
  for i from 0 to n do a[i]:=coeff(f,x,i); end do;
```

3) знаходимо множину M всіх простих дільників числа a_0 за допомогою команди **factorset** із пакету **numtheory**:

```
> M:=factorset(a[0]);
```

4) для кожного числа $p \in M$ перевіряємо, чи задовольняє число p умови ознаки Айзенштайна, а саме:

а) перевіряємо, чи кожен із коефіцієнтів a_0, a_1, ...,a_{n-1} ділиться на p (умова 1)):

```
> j:=0;
  while j<=n-1 and irem(a[j],p)=0 do j:=j+1;  end do;
```

б) якщо кожен із коефіцієнтів a_0, a_1, ...,a_{n-1} ділиться на p (тобто в результаті перевірки лічильник j набув значення n), то перевіряємо, чи виконуються умови 2): $a_0 \vdots p^2$ і 3): $a_n \vdots p$. Якщо дані умови виконуються, з'являється повідомлення: "mnogochlen nezvidnyi" і вказується число p; якщо якась із умов 1)-3) не виконується, то лічильник i збільшується на 1, переходимо до розгляду наступного елемента множини M (наступного простого числа):

```
> if j=n and irem(a[0],p^2)<>0 and irem(a[n],p)<>0 then
     return("mnogochlen nezvidnyi, p"=p)
  else i:=i+1;
  end if;
```

6) якщо всі числа множини M досліджено і не знайдено числа p, яке задовольняє умови ознаки Айзенштайна (при цьому лічильник i набуде значення на 1 більшого за кількість елементів множини M), то з'являється повідомлення про те, що ознака Айзенштайна до заданого многочлена незастосовна:

```
> if i=nops(M)+1 then
     return("oznaka Eisenstein nezastosovna‘)
  end if;
```

Код процедури наступний:

```
EisensteinsCrit:=proc(f,x)
uses numtheory:
local n,M,i,j,a,p:
   if not type(f, polynom(integer)) then
      error "wrong coefficients";
   end if;
   n:=degree(f,x):
   for i from 0 to n do a[i]:=coeff(f,x,i); end do;
   M:=factorset(a[0]);
   i:=1:
   while i<=nops(M) do
      p:=M[i];
      j:=0;
      while j<=n-1 and irem(a[j],p )=0 do j:=j+1; end do;
      if j=n and irem(a[0],p^2 )<>0 and irem(a[n],p )<>0 then
         return("mnogochlen nezvidnyi, p-p)
      else i:=i+1;
      end if;
   end do;
   if i=nops(M)+1 then return("oznaka Eisenstein nezastosovna") end if;
end proc:
```

Розв'язання в Maple. Застосовуємо створену процедуру **EisensteinsCrit** до заданих многочленів $f(x)$ і $g(x)$:

```
> f:=x^6-2*x^4+4*x^3+2:
  EisensteinsCrit(f,x);
```

$$\text{"}mnogochlen\ nezvidnyi,\ p\text{"} = 2$$

До многочлена $f(x)$ ознаку Айзенштайна застосувати можна: при $p = 2$ умови 1)-3) виконуються, отже, $f(x)$ – незвідний над $\mathbb{Q}$.

```
> g:=x^4+10*x^3+24*x^2+25*x+13:
  EisensteinsCrit(g,x);
```

$$\text{"}oznaka\ Eisenstein\ nezastosovna\text{"}$$

До многочлена $g(x)$ застосувати ознаку Айзенштайна не можна: простого числа p, яке б задовольняло умови 1)-3), не існує.

Підберемо заміну. Спробуємо спочатку заміну $x = y + 1$:

```
> h1:=expand(subs({x=y+1},g));
```

$$h1 := y^4 + 14\,y^3 + 60\,y^2 + 107\,y + 73$$

Перевіримо, чи можна до многочлена $h_1(y)$ застосувати ознаку Айзенштайна:

```
> EisensteinsCrit(h1,y);
```

$$\text{"}oznaka\ Eisenstein\ nezastosovna\text{"}$$

До отриманого многочлена $h_1(y)$ застосувати ознаку Айзенштайна також не можна – заміна невдала. Спробуємо іншу заміну: $x = y - 1$.

```
> h2:=expand(subs({x=y-1},g));
```

$$h2 := y^4 + 6\,y^3 + 3\,y + 3$$

```
> EisensteinsCrit(h2,y);
```

$$\text{"}mnogochlen\ nezvidnyi,\ p\text{"} = 3$$

Отриманий многочлен $h_2(y)$ – незвідний над полем $\mathbb{Q}$ за ознакою Айзенштайна ($p = 3$), а тому і многочлен $g(x)$ теж є незвідним над $\mathbb{Q}$.

Завдання 60. Довести, що многочлен $f(x)$ – незвідний над полем $\mathbb{Q}$ раціональних чисел:

60.1. $f(x) = x^4 + 2x^3 + 4x^2 + 8x - 1$.

60.2. $f(x) = x^5 + 5x^4 + 7x^3 + x^2 - 4x + 1$.

60.3. $f(x) = x^4 - 2x^3 - 8x^2 - 2x + 5$.

60.4. $f(x) = x^4 - 4x^3 + 12x^2 - 16x + 1$.

60.5. $f(x) = x^4 - 2x^3 - 4x^2 + 14x - 11.$

60.6. $f(x) = x^5 - 9x^4 + 26x^3 - 34x^2 + 21x - 3.$

60.7. $f(x) = x^4 - x^3 - 12x^2 + 23x - 8.$

60.8. $f(x) = x^4 + 8x^3 + 14x^2 + 8x + 3.$

60.9. $f(x) = x^5 + 5x^4 + 10x^3 + x^2 - 13x - 5.$

60.10. $f(x) = x^4 + 8x^3 + 16x^2 + 14x - 1.$

60.11. $f(x) = x^4 - 6x^3 + 16x^2 - 16x - 1.$

60.12. $f(x) = x^5 - 10x^4 + 37x^3 - 62x^2 + 44x - 5.$

60.13. $f(x) = x^4 - 10x^3 + 28x^2 - 26x + 9.$

60.14. $f(x) = x^4 + 4x^3 + 12x^2 + 16x + 1.$

60.15. $f(x) = x^4 + 6x^3 + 8x^2 + 6x + 1.$

60.16. $f(x) = x^5 + x^4 - 6x^3 - 14x^2 - 11x - 1.$

60.17. $f(x) = x^4 - 5x^3 - 3x^2 + 40x - 41.$

60.18. $f(x) = x^4 + 5x^3 - 27x^2 + 35x - 11.$

60.19. $f(x) = x^5 - 5x^4 + 10x^3 - 19x^2 + 23x - 7.$

60.20. $f(x) = x^4 - 8x^2 + 14x - 13.$

60.21. $f(x) = x^4 + 17x^3 + 72x^2 + 116x + 67.$

60.22. $f(x) = x^4 + 2x^3 + 2x^2 + 6x + 3.$

60.23. $f(x) = x^4 - 2x^3 - 9x^2 - 8x + 1.$

60.24. $f(x) = x^4 - 6x^3 + 14x^2 - 10x - 1.$

60.25. $f(x) = x^4 - 10x^3 + 27x^2 - 28x + 13.$

Розділ VII

Теорія груп

1. Група. Підгрупа

ТЕОРЕТИЧНІ ВІДОМОСТІ

Означення (групи)**.** Впорядкована пара $\langle G; * \rangle$, де G – непорожня множина, називається групою, якщо виконуються наступні умови:

1) $*$ – бінарна алгебраїчна операція, задана на множині G;
2) операція $*$ асоціативна на G, тобто для будь-яких елементів a, b, c із G справедливо: $(a * b) * c = a * (b * c)$;
3) в G існує нейтральний відносно $*$ елемент e, тобто такий, що $a * e = e * a = a$ для всіх $a \in G$;
4) для будь-якого елемента $a \in G$ існує симетричний до нього елемент $a' \in G$, тобто такий, що $a * a' = a' * a = e$.

Умови 1)-4) називають **аксіомами** групи. Для позначення групової операції замість знака $*$ використовують частіше більш звичні знаки: $+$ і $\cdot$. Якщо беруть знак $+$, то алгебраїчну операцію називають додаванням, групу відносно цієї операції – адитивною, нейтральний елемент – нульовим або просто нулем, симетричний – протилежним елементом, і таку форму запису називають адитивною. Якщо використовують знак $\cdot$, то алгебраїчну операцію називають множенням, групу відносно цієї операції – мультиплікативною, нейтральний елемент – одиничним або просто одиницею, симетричний – оберненим елементом, і таку форму запису називають мультиплікативною.

Група $\langle G; * \rangle$ називається **комутативною** або **абелевою**, якщо комутативною є операція $*$, тобто якщо для будь-яких елементів a, b із G справедливо: $a * b = b * a$.

Найпростіші властивості групи. Нехай $\langle G; \cdot \rangle$ – група. Тоді:

1) для будь-яких елементів $a, b \in G$ справедливо: $(ab)^{-1} = b^{-1}a^{-1}$.
2) в будь-якій групі G нейтральний елемент єдиний;
3) в групі G для будь-якого елемента a із G існує єдиний симетричний елемент.

Означення (підгрупи)**.** Непорожня підмножина H групи $\langle G; * \rangle$ називається підгрупою цієї групи, якщо вона є групою відносно операції, заданої в G (тобто якщо $\langle H; * \rangle$ – група).

Підгрупа H групи G, відмінна від G і від $\{e\}$, називається власною підгрупою групи G. Якщо H є підгрупою групи G, то пишуть: $H \leqslant G$. Якщо $H \leqslant G$ і $H \neq G$, пишуть: $H < G$. Якщо H не є підгрупою групи G, записують: $H \not\leqslant G$.

Теорема (критерій підгрупи)**.** *Нехай $\langle G; * \rangle$ – група. Для того, щоб непорожня підмножина H групи G була підгрупою цієї групи, необхідно і достатньо, щоб виконувались умови:*

1) операція $*$ була замкненою на H, тобто для довільних $a, b \in H$ виконувалась умова $a * b \in H$;
2) для довільного елемента $a \in H$ симетричний до нього в G елемент a' належав до H.

Якщо деяка непорожня множина T є підмножиною деякої відомої групи $\langle G; * \rangle$, то для того, щоб визначити, чи є $\langle T; * \rangle$ групою, достатньо перевірити (використовуючи критерій підгрупи), чи є T підгрупою групи G. Якщо ж таку „допоміжну" групу G підібрати важко, доводиться перевіряти, чи виконуються в T всі умови 1)-4) означення групи.

В якості „допоміжних" груп найчастіше використовують:

- адитивні групи: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, групу $M_n(P)$ квадратних матриць n-го порядку над полем P;

- мультиплікативні групи: $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \mathbb{R}^* = \mathbb{R}\backslash\{0\}, \mathbb{C}^* = \mathbb{C}\backslash\{0\}$, групу $GL_n(P)$ невироджених квадратних матриць n-го порядку над полем P.

Відмітимо, що при виборі „допоміжної" групи необхідно, щоб виконувались лише дві умови: $\langle G, * \rangle$ – „допоміжна", якщо $G \supseteq T$ і на G задана та ж сама операція $*$, що й на T.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 61.1. Визначити, чи утворює групу відносно операції $*$, заданої наступним чином:

$$(a_1, b_1) * (a_2, b_2) \;=\; (a_1 + a_2, \overline{2}b_1b_2).$$

а) множина M пар (a, b), де $a, b \in \mathbb{Z}_5$;

б) множина M_1 пар (a, b), де $a, b \in \mathbb{Z}_5$, причому $b \neq \overline{0}$.

Якщо так, то чи є ця група абелевою?

Розв'язання. а) Перевіримо, чи виконуються умови 1)-4) означення групи.

1) Нехай (a_1, b_1), (a_2, b_2) – довільні два елементи із M, $a_1, b_1, a_2, b_2 \in \mathbb{Z}_5$. Маємо: $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, \overline{2}b_1b_2) \in M$, оскільки $a_1 + a_2 \in \mathbb{Z}_5$, $\overline{2}b_1b_2 \in \mathbb{Z}_5$. Отже, операція $*$ замкнена на M; крім того, $*$ виконувана і однозначна на M, а значить, є бінарною алгебраїчною на M.

2) Нехай (a_3, b_3) – ще один довільний елемент із M, $a_3, b_3 \in \mathbb{Z}_5$. Тоді:

$$\Big((a_1,b_1)*(a_2,b_2)\Big)*(a_3,b_3)=(a_1+a_2,\overline{2}b_1b_2)*(a_3,b_3)=$$
$$=\Big((a_1+a_2)+a_3,\overline{2}(\overline{2}b_1b_2)b_3\Big)=\Big((a_1+a_2)+a_3,(\overline{4}b_1b_2)b_3\Big);$$
$$(a_1,b_1)*\Big((a_2,b_2)*(a_3,b_3)\Big)=(a_1,b_1)*(a_2+a_3,\overline{2}b_2b_3)=$$
$$=\Big(a_1+(a_2+a_3),\overline{2}b_1(\overline{2}b_2b_3)\Big).$$

Враховуючи асоціативність і комутативність операцій додавання і множення на множині $\mathbb{Z}_5$ (тобто враховуючи, що $(a_1+a_2)+a_3=a_1+(a_2+a_3)$ і $\overline{2}(\overline{2}b_1b_2)b_3=\overline{2}b_1(\overline{2}b_2b_3)$), маємо, що

$$\Big((a_1,b_1)*(a_2,b_2)\Big)*(a_3,b_3)=(a_1,b_1)*\Big((a_2,b_2)*(a_3,b_3)\Big).$$

Отже, операція $*$ є асоціативною на M.

3) В M нейтральним елементом відносно операції $*$ є елемент $(\overline{0},\overline{3})$, оскільки для довільного елемента $(a,b)\in M$ справедливо:

$$(a,b)*(\overline{0},\overline{3})=(a+\overline{0},\overline{2}b\cdot\overline{3})=(a,b)\qquad i$$
$$(\overline{0},\overline{3})*(a,b)=(\overline{0}+a,\overline{2}\cdot\overline{3}b)=(a,b).$$

4) Нехай (a,b) – довільний елемент із M. Покажемо, що симетричний до (a,b) відносно операції $*$ існує не завжди. Дійсно, нехай симетричним до (a,b) елементом є елемент (x,y), тоді

$$\begin{aligned}(a,b)*(x,y)&=(\overline{0},\overline{3})\\(x,y)*(a,b)&=(\overline{0},\overline{3})\end{aligned}$$

тобто

$$\begin{aligned}(a+x,\overline{2}by)&=(\overline{0},\overline{3})\\(x+a,\overline{2}yb)&=(\overline{0},\overline{3}).\end{aligned}$$

З першої рівності маємо: $a+x=\overline{0}$, $\overline{2}by=\overline{3}$. Тоді $x=-a$, $y=\overline{2}^{-1}b^{-1}\cdot\overline{3}=\overline{3}b^{-1}\cdot\overline{3}=\overline{4}b^{-1}$. Елемент $-a$ існує для довільного $a\in\mathbb{Z}_5$, але елемент b^{-1} існує не для кожного $b\in\mathbb{Z}_5$ (а саме: для $b=\overline{0}$ елемента b^{-1} не існує). Значить, і не для кожного елемента (a,b) із M існує симетричний відносно операції $*$ елемент.

Таким чином, множина M не є групою відносно операції $*$.

б) При перевірці умов 1)-3) означення групи для множини M_1 будемо використовувати деякі властивості операції $*$ на множині M (див. п.а)).

1) Операція $*$ на M_1 – виконувана і однозначна, оскільки $*$ є виконуваною і однозначною на M (яка містить M_1). Нехай (a_1, b_1), (a_2, b_2) – довільні два елементи із M_1, $a_1, b_1, a_2, b_2 \in \mathbb{Z}_5$ і $b_1 \neq \overline{0}$, $b_2 \neq \overline{0}$. Тоді $\overline{2}b_1b_2 \neq \overline{0}$, а значить, $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, \overline{2}b_1b_2) \in M_1$. Отже, операція $*$ замкнена на M_1, а значить, і бінарна алгебраїчна на M_1.

2) Операція $*$ на M_1 – асоціативна, оскільки $*$ є асоціативною на множині M.

3) Нейтральним елементом відносно операції $*$ в M_1 є елемент $(\overline{0}, \overline{3})$, оскільки цей елемент є нейтральним відносно $*$ в M.

4) Для довільного $b \in \mathbb{Z}_5$ елемент b^{-1}, обернений до b в $\mathbb{Z}_5$, існує, тому для довільної пари (a, b) існуватиме в M_1 елемент $(-a, \overline{4}b^{-1})$, симетричний до (a, b), оскільки

$$(a, b) * (-a, \overline{4}b^{-1}) = (a - a, \overline{2}b\overline{4}b^{-1}) = (\overline{0}, \overline{3}),$$

$$(-a, \overline{4}b^{-1}) * (a, b) = (-a + a, \overline{24}b^{-1}b) = (\overline{0}, \overline{3}).$$

Умови 1)-4) означення групи виконуються, отже, множина M_1 є групою відносно операції $*$.

Перевіримо, чи є група $\langle M_1; * \rangle$ абелевою.

5) Нехай (a_1, b_1), (a_2, b_2) – довільні два елементи із M_1, $a_1, b_1, a_2, b_2 \in \mathbb{Z}_5$, $b_1 \neq \overline{0}$, $b_2 \neq \overline{0}$. Маємо:

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, \overline{2}b_1b_2);$$

$$(a_2, b_2) * (a_1, b_1) = (a_2 + a_1, \overline{2}b_2b_1).$$

Оскільки операції додавання і множення – комутативні на $\mathbb{Z}_5$, то $a_1 + a_2 = a_2 + a_1$, $b_1b_2 = b_2b_1$, а значить, $(a_1, b_1) * (a_2, b_2) = (a_2, b_2) * (a_1, b_1)$. Отже, $*$ є комутативною на M.

Таким чином, пара $\langle M_1; * \rangle$ є абелевою групою.

Розробка процедур. На основі процедур **isClosed**, **isAssociative**, **Id**, **hasSym**, створених при розв'язанні Прикладу 21.1, можна розробити процедуру для перевірки, чи є непорожня множина M групою відносно операції operation:

```
isGroup:=proc(M,operation)
   if isClosed(M,operation) and isAssociative(M,operation) and
      Id(M,operation)<>false and hasSym(M,operation)<>false then
      return true
   else return false;
   end if;
end proc:
```

Розв'язання в Maple. а) Задаємо множину M і операцію $*$ (див. Приклад 21.1):

```
> M:={seq(seq([a,b],a=0..4),b=0..4)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 5,2*X[2]*Y[2] mod 5]:
```

підключаємо бібліотеку:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> isClosed(M,astra);
```

true

```
> isAssociative(M,astra);
```

true

```
> Id(M,astra);
```

[0, 3]

```
> hasSym(M,astra);
```

false

Умови 1)-3) означення групи виконуються, але умова 4) не виконується, тому пара $\langle M; * \rangle$ не є групою:

```
> isGroup(M,astra);
```

false

б) Задаємо множину M_1 і операцію $*$:

```
> M1:={seq(seq([a,b],a=0..4),b=1..4)}:
> astra:=(X,Y)->[X[1]+Y[1] mod 5,2*X[2]*Y[2] mod 5]:
```

і перевіряємо, чи виконуються умови 1)-4) означення групи:

```
> isClosed(M1,astra);
```

true

```
> isAssociative(M1,astra);
```

true

```
> Id(M1,astra);
```

[0, 3]

```
> hasSym(M1,astra);
```

true

Всі умови означення групи виконуються, отже, пара $\langle M_1; * \rangle$ є групою:

```
> isGroup(M1,astra);
```

true

Перевіримо, чи буде операція $*$ комутативна на M_1.

```
> isCommutative(M1,astra);
```

true

Операція $*$ є комутативною на M_1, тому група $\langle M_1; * \rangle$ – абелева.

Приклад 61.2. Визначити, чи утворює групу множина $M = \mathbb{Z}_7$ відносно операції $*$, заданої наступним чином:

$$a * b = a^2 + b^2.$$

Якщо так, то чи є група $\langle M; * \rangle$ абелевою?

Розв'язання. Перевіримо, чи виконуються умови 1)-4) означення групи.

1) Нехай $a, b \in \mathbb{Z}_7$. Тоді $a*b = a^2+b^2 \in \mathbb{Z}_7$; отже, операція $*$ замкнена на $\mathbb{Z}_7$. Крім того, $*$ завжди виконувана і однозначна на $\mathbb{Z}_7$, значить, $*$ бінарна алгебраїчна на $\mathbb{Z}_7$.

2) Нехай $a, b, c \in \mathbb{Z}_7$. Тоді

$$\begin{aligned} (a * b) * c &= (a^2 + b^2) * c = (a^2 + b^2)^2 + c^2 = a^4 + 2a^2b^2 + b^4 + c^2; \\ a * (b * c) &= a * (b^2 + c^2) = a^2 + (b^2 + c^2)^2 = a^2 + b^4 + 2b^2c^2 + c^4. \end{aligned}$$

Елементи $(a * b) * c$ і $a * (b * c)$ не завжди рівні; наприклад, при $a = b = \overline{1}$, $c = \overline{0}$ маємо: $(a*b)*c = \overline{1}^4 + 2\overline{1}^2\overline{1}^2 + \overline{1}^4 + \overline{0}^2 = \overline{4}$; $a*(b*c) = \overline{1}^2 + (\overline{1}^2 + \overline{1}^2)^2 = \overline{1}^2 + \overline{1}^4 + 2\overline{1}^2\overline{0}^2 + \overline{0}^4 = \overline{2}$. Отже, операція $*$ не є асоціативною на $\mathbb{Z}_7$, а значить, $\langle \mathbb{Z}_7; * \rangle$ не є групою.

Розв'язання в Maple. а) Задаємо множину M і операцію $*$:

```
> M:={seq(a,a=0..6)};
```

$$M := \{0, 1, 2, 3, 4, 5, 6\}$$

```
> astra:=(X,Y)->X^2+Y^2 mod 7:
```

і перевіряємо, чи виконуються умови означення групи:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> isClosed(M,astra);
```

true

```
> isAssociative(M,astra);
```

false

Як бачимо, операція $*$ не є асоціативною на M, тому $\langle M; * \rangle$ не є групою.

Завдання 61. Визначити, чи утворює групу:

61.1. множина M пар (a, b), де $a, b \in \mathbb{Z}_5$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1 b_2 + b_1 a_2, b_1 b_2)$.

61.2. множина $M = \mathbb{Z}_5$ відносно операції $*$, заданої наступним чином: $a * b = ab + \overline{1}$.

61.3. множина $M = \{1, 2, 3, 4, 6, 12\}$ відносно операції знаходження НСД двох цілих чисел.

61.4. множина M пар (a, b), де $a, b \in \mathbb{Z}_7$, $a \neq \overline{0}$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1)$.

61.5. множина $M = \mathbb{Z}_{10}$ відносно операції $*$, заданої наступним чином:

$$a * b = \begin{cases} a, & \text{якщо } a + b \in \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}; \\ b, & \text{якщо } a + b \in \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}\}. \end{cases}$$

61.6. множина $M = \mathbb{Z}_{11}$ відносно операції $*$, заданої наступним чином: $a * b = b$.

61.7. множина M пар (a, b), де $a, b \in \mathbb{Z}_5$, $b \neq 0$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1 + b_1 a_2, b_1 b_2)$.

61.8. множина M квадратних матриць порядку 2 над полем $\mathbb{Z}_5$ відносно операції $*$, заданої наступним чином: для довільних $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ із M $\qquad A * B = \begin{pmatrix} a_1 b_1 & a_2 b_2 \\ a_3 b_3 & a_4 b_4 \end{pmatrix}$.

61.9. множина $M = \mathbb{Z}_5 \backslash \{\overline{0}\}$ відносно операції $\circ$, заданої наступним чином: $a \circ b = a + b + \overline{2}$.

61.10. множина M пар (a, b), де $a, b \in \mathbb{Z}_4$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1, b_2)$.

61.11. множина $M = \mathbb{Z}_7$ відносно операції $*$, заданої наступним чином: $a*b = a^2b^2$.

61.12. множина $M = \mathbb{Z}_5\backslash\{\overline{0}\}$ відносно операції $\circ$, заданої наступним чином: $a \circ b = a + b$.

61.13. множина M пар (a, b), де $a, b \in \mathbb{Z}_4$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1b_2 - b_1a_2, b_1b_2)$.

61.14. множина $M = \mathbb{Z}_7\backslash\{\overline{0}\}$ відносно операції $\circ$, заданої наступним чином: $a \circ b = a + b + \overline{2}$.

61.15. множина $M = \mathbb{Z}_7$ відносно операції $*$, заданої наступним чином: $a*b = a$.

61.16. множина M нескінченних послідовностей (a_1, a_2, a_3), де $a_1, a_2, a_3 \in \mathbb{Z}_8$, відносно операції $*$, заданої наступним чином:

$$(a_1, a_2, a_3) * (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3b_3).$$

61.17. множина M пар (a, b), де $a, b \in \mathbb{Z}_6$ – довільні цілі числа, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1a_2 - \overline{2}b_1b_2, b_1a_2 + a_1b_2)$.

61.18. множина M пар (a, b), де $a, b \in \mathbb{Z}_2$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, \overline{1})$.

61.19. множина $M = \{1, 2, 3, 4, 6, 12\}$ відносно операції знаходження НСК двох цілих чисел.

61.20. множина $M = \mathbb{Z}_{10}$ відносно операції $*$, заданої наступним чином:

$$a * b = \begin{cases} a, & \text{якщо } a + b \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}; \\ b, & \text{якщо } a + b \in \{\overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}. \end{cases}$$

61.21. множина M пар (a, b), де $a, b \in \mathbb{Z}_5$, $b \in \{\overline{1}, \overline{4}\}$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1b_2)$.

61.22. множина $M = \mathbb{Z}_4\backslash\{\overline{0}\}$ відносно операції $\circ$, заданої наступним чином: $a \circ b = ab^{-1}$.

61.23. множина M пар (a, b), де $a, b \in \mathbb{Z}_3$, відносно операції $*$, заданої наступним чином: $(a_1, b_1) * (a_2, b_2) = (a_1b_2, a_2b_1)$.

61.24. множина M квадратних матриць порядку 2 над полем $\mathbb{Z}_5$ відносно операції $*$, заданої наступним чином: для довільних $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ із M $\qquad A * B = \begin{pmatrix} a_1b_1 + a_3b_2 & a_1b_3 + a_3b_4 \\ a_2b_1 + a_4b_2 & a_2b_3 + a_4b_4 \end{pmatrix}$.

61.25. множина M трійок $(a, b, \overline{6})$, де $a, b \in \mathbb{Z}_{10}$, відносно операції $*$, заданої наступним чином: $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1c_2)$.

Приклад 62.1. Визначити, чи є множина M матриць виду $\begin{pmatrix} \overline{1} & a \\ \overline{0} & b \end{pmatrix}$, де $a, b \in \mathbb{Z}_5$, групою відносно:

а) операції додавання матриць;

б) операції множення матриць (за умови $b \neq \overline{0}$).

Розв'язання. а) Помічаємо, що множина $M \neq \varnothing$ є підмножиною адитивної групи $\mathrm{M}_2(\mathbb{Z}_5)$ матриць 2-го порядку над полем $\mathbb{Z}_5$.

Спосіб I. Використаємо критерій підгрупи.

1) Нехай $A_1 = \begin{pmatrix} \overline{1} & a_1 \\ \overline{0} & b_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} \overline{1} & a_2 \\ \overline{0} & b_2 \end{pmatrix}$ – довільні два елементи із M, $a_1, b_1, a_2, b_2 \in \mathbb{Z}_5$. Знайдемо їхню суму:

$$A_1 + A_2 = \begin{pmatrix} \overline{1} & a_1 \\ \overline{0} & b_1 \end{pmatrix} + \begin{pmatrix} \overline{1} & a_2 \\ \overline{0} & b_2 \end{pmatrix} = \begin{pmatrix} \overline{2} & a_1 + a_2 \\ \overline{0} & b_1 + b_2 \end{pmatrix} \notin M,$$

оскільки елемент, що міститься в лівому верхньому куті одержаної матриці відмінний від $\overline{1}$.

Умова 1) критерію підгрупи не виконуються. Отже, M не є підгрупою адитивної групи $\mathrm{M}_2(\mathbb{Z}_5)$, а значить, M не є адитивною групою.

Спосіб II. Кожна підгрупа H групи G обов'язково повинна містити нейтральний елемент групи G. Нейтральним елементом групи $\mathrm{M}_2(\mathbb{Z}_5)$ є матриця $T = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}$. Зрозуміло, що $T \notin M$. Отже, M не є підгрупою групи $\mathrm{M}_2(\mathbb{Z}_5)$, а значить, M не є групою відносно операції додавання матриць.

б) В даному випадку в якості „допоміжної" групи візьмемо групу $GL_2(\mathbb{Z}_5)$ невироджених квадратних матриць 2-го порядку над полем $\mathbb{Z}_5$. Перевіримо умови критерію підгрупи.

Нехай $A_1 = \begin{pmatrix} \overline{1} & a_1 \\ \overline{0} & b_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} \overline{1} & a_2 \\ \overline{0} & b_2 \end{pmatrix}$ – довільні два елементи із M,

$a_1, b_1, a_2, b_2 \in \mathbb{Z}_5$, $b_1 \neq \overline{0}$, $b_2 \neq \overline{0}$. Знайдемо їхній добуток:

$$A_1 A_2 = \begin{pmatrix} \overline{1} & a_1 \\ \overline{0} & b_1 \end{pmatrix} \begin{pmatrix} \overline{1} & a_2 \\ \overline{0} & b_2 \end{pmatrix} = \begin{pmatrix} \overline{1} & a_2 + a_1 b_2 \\ \overline{0} & b_1 b_2 \end{pmatrix} \in M,$$

оскільки $a_2 + a_1 b_2 \in \mathbb{Z}_5$, $b_1 b_2 \in \mathbb{Z}_5$, причому $b_1 b_2 \neq \overline{0}$.

2) Знайдемо обернений до елемента A_1 в $GL_2(\mathbb{Z}_5)$. Маємо:

$$A_1^{-1} = \begin{pmatrix} \overline{1} & a_1 \\ \overline{0} & b_1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{b_1}{|A_1|} & -\frac{a_1}{|A_1|} \\ \overline{0} & \frac{\overline{1}}{|A_1|} \end{pmatrix} = \begin{pmatrix} \frac{b_1}{b_1} & -\frac{a_1}{b_1} \\ \overline{0} & \frac{\overline{1}}{b_1} \end{pmatrix} = \begin{pmatrix} \overline{1} & -a_1 b_1^{-1} \\ \overline{0} & b_1^{-1} \end{pmatrix} \in M.$$

Умови критерію підгрупи виконуються, тому M – підгрупа групи $GL_2(\mathbb{Z}_5)$, а значить, $\langle M; \cdot \rangle$ – група.

Розробка процедур. Для перевірки умов 1)-2) критерію підгрупи використовуємо процедури **isClosed** і **belongsSym**, створені при розв'язанні Прикладів 21.1 і 24.1 відповідно. На основі даних процедур створимо процедуру **isSubgroup**, яка для заданих підмножини M групи G, операції operation і правила пошуку симетричного відносно цієї операції елемента symElement визначатиме, чи є M підгрупою G:

```
isSubgroup:=proc(M,operation,symElement)
   if isClosed(M,operation)=true and belongsSym(M,symElement)=true
      then return true
   else return false
   end if;
end proc:
```

Розв'язання в Maple. а) Задаємо множину M і операцію додавання матриць mplus:

```
> M:={seq(seq([[1,a],[0,b]],a=0..4),b=0..4)}:
> mplus:=(A,B)->[[A[1,1]+B[1,1] mod 5, A[1,2]+B[1,2] mod 5],
                 [A[2,1]+B[2,1] mod 5, A[2,2]+B[2,2] mod 5]]:
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> isClosed(M,mplus);
```

false

Отже, операція додавання матриць не є замкненою на множині M.

б) Задаємо множину M (в даному випадку $b \neq \overline{0}$):

```
> M:={seq(seq([[1,a],[0,b]],a=0..4),b=1..4)}:
```

і операцію множення матриць mmult:

```
> mmult:=(A,B)->[[A[1,1]*B[1,1]+A[1,2]*B[2,1] mod 5,
                  A[1,1]*B[1,2]+A[1,2]*B[2,2] mod 5],
                 [A[2,1]*B[1,1]+A[2,2]*B[2,1] mod 5,
                  A[2,1]*B[1,2]+A[2,2]*B[2,2] mod 5]]:
> isClosed(M,mmult);
```

true

Операція множення матриць на множині M є замкненою.

Тепер задаємо правило пошуку симетричного елемента. Симетричним елементом до матриці $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ відносно операції множення матриць є обернена матриця $A^{-1} = \begin{pmatrix} \frac{a_{22}}{a_{11}a_{22}-a_{21}a_{12}} & -\frac{a_{12}}{a_{11}a_{22}-a_{21}a_{12}} \\ -\frac{a_{21}}{a_{11}a_{22}-a_{21}a_{12}} & \frac{a_{11}}{a_{11}a_{22}-a_{21}a_{12}} \end{pmatrix}$:

```
> im:=A->[[A[2,2]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5,
          -A[1,2]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5],
          [-A[2,1]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5,
           A[1,1]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5]]:
```

Застосовуємо процедуру **belongsSym**:

```
> belongsSym(M,im);
```

true

Отже, і умова 2) критерію підгрупи виконується, значить,

```
> isSubgroup(M,mmult,im);
```

true

Таким чином, $M \leqslant GL_2(\mathbb{Z}_5)$, а значить, $\langle M; \cdot \rangle$ – група.

Приклад 62.2. Визначити, чи є множина $H = \{1, -1, i, -i\}$ мультиплікативною групою.

Розв'язання. Помічаємо, що $H \neq \varnothing$ є підмножиною мультиплікативної групи $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ відмінних від 0 комплексних чисел. Використаємо критерій підгрупи.

1) Покажемо, що добуток довільних двох елементів із H належить до H. В силу комутативності операції множення в $\mathbb{C}^*$, а також враховуючи те, що число 1 є одиничним елементом в $\mathbb{C}^*$ (а значить, є одиничним і в H) достатньо перевірити лише такі добутки: $(-1)\cdot(-1)$, $(-1)\cdot i$, $(-1)\cdot(-i)$, $i\cdot i$, $i\cdot(-i)$, $(-i)\cdot(-i)$. Маємо:

$$(-1)\cdot(-1) = 1 \in H, \qquad (-1)\cdot(-i) = i \in H, \qquad i\cdot(-i) = 1 \in H,$$
$$(-1)\cdot i = -i \in H, \qquad i\cdot i = -1 \in H, \qquad (-i)\cdot(-i) = -1 \in H.$$

Таким чином, операція множення – алгебраїчна на H.

2) Покажемо, що разом із кожним своїм елементом множина H містить і обернений до нього. Маємо:

$$1^{-1} = 1 \in H, \qquad (-1)^{-1} = -1 \in H, \qquad i^{-1} = -i \in H, \qquad (-i)^{-1} = i \in H.$$

Умови 1) і 2) критерію підгрупи виконуються, отже, H є підгрупою мультиплікативної групи $\mathbb{C}^*$, а це означає, що H сама є мультиплікативною групою.

Для перевірки умов критерію підгрупи у випадку скінченної множини G з невеликою кількістю елементів досить зручно використовувати таблицю Келі (див. §4 розд.III). Операція $*$ замкнена на G, якщо в таблиці Келі всі клітинки заповнені лише елементами із G (тобто в результаті операції $*$ над довільними елементами із G отримуємо знову елемент із G). Для елемента a існує елемент, симетричний справа відносно операції $*$, якщо в рядку, який відповідає елементу a є нейтральний елемент e; причому якщо e знаходиться в стовпці, який відповідає елементу b, то b – елемент, симетричний до a справа.

$*$	$\dots$	$\dots$	b	$\dots$	$\dots$
$\vdots$			$\uparrow$		
$\vdots$			$\mid$		
a			e		
$\vdots$					

Аналогічно до елемента a існує симетричний зліва, якщо в стовпці, який відповідає елементу a є елемент e.

Тому для перевірки існування симетричного елемента перевіряють:

а) чи в кожному рядку і стовпці є нейтральний елемент e;

б) чи однаковими для елемента a є симетричний справа і симетричний зліва елементи. Якщо операція $*$ комутативна на G (в такому випадку таблиця симетрична відносно діагоналі, що виходить з лівого верхнього кута), то достатньо перевірити лише умову а).

Для множини H і операції $\cdot$ маємо:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Всі клітинки таблиці заповнено елементами із H, тому операція $\cdot$ замкнена на H. Оскільки таблиця – симетрична відносно діагоналі, що виходить з лівого верхнього кута, то операція $\cdot$ комутативна на H і достатньо перевірити лише умову а). Як бачимо, в кожному рядку є нейтральний елемент 1, тому для кожного елемента a із H в H міститься і обернений до a в $\mathbb{C}$. Умови критерію підгрупи виконуються, тому $H \leqslant \langle \mathbb{C}; \cdot \rangle$, а значить, H сама є мультиплікативною групою.

Розв'язання в Maple. Задаємо множину H, операцію множення mult:

```
> H:={1,-1,I,-I}:
> mult:=(a,b)->a*b:
```

і використовуємо процедури **isClosed** і **belongsSym**:

```
> isClosed(H,mult);
```

$$true$$

Отже, операція $\cdot$ замкнена на H.

Задаємо правило пошуку елемента, симетричного відносно операції $\cdot$ (тобто оберненого) до елемента a в $\mathbb{C}$:

```
> obern:=a->a^(-1);
```

$$obern := a \to \frac{1}{a}$$

```
> belongsSym(H,obern);
```

$$true$$

Для кожного елемента із H обернений до нього в $\mathbb{C}$ належить до H. Тому $H \leqslant \mathbb{C}$:

```
> isSubgroup(H,mult,obern);
```

$$true$$

Для побудови таблиці Келі використовуємо процедуру **cayleyTable**, створену при розв'язанні Прикладу 23.1.

```
> cayleyTable(H,mult);
```

$$\begin{bmatrix} 1 & -1 & I & -I \\ -1 & 1 & -I & I \\ I & -I & -1 & 1 \\ -I & I & 1 & -1 \end{bmatrix}$$

Завдання 62. Визначити, чи утворює групу:

62.1. множина M всіх діагональних матриць порядку 2 над полем $\mathbb{Z}_2$ відносно: а) операції додавання матриць; б) операції множення матриць.

62.2. множина $M = \{1, \sqrt{2}, \sqrt{2}+1, \sqrt{2}-1\}$ відносно операції множення.

62.3. множина M матриць виду $\begin{pmatrix} \overline{0} & a & b \\ c & \overline{0} & d \\ f & g & \overline{0} \end{pmatrix}$, де $a, b, c, d, f, g \in \mathbb{Z}_3$, відносно операції множення матриць.

62.4. множина $M = \{0, 1, 2, -1, -2\}$ відносно: а) операції додавання; б) операції множення.

62.5. множина $M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ відносно: а) операції додавання матриць; б) операції множення матриць.

62.6. множина $M = \{1, -1, \frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i\}$ відносно операції множення.

62.7. множина $M = \left\{ \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \right\}$, де $\overline{0}, \overline{1} \in \mathbb{Z}_2$ відносно операції додавання матриць.

62.8. множина $M = \{0, 1, \sqrt{2}, \sqrt{2}+1, \sqrt{2}-1\}$ відносно операції додавання.

62.9. множина M всіх комплексних чисел z виду $z = \cos\frac{\pi k}{5} + i\sin\frac{\pi k}{5}$, де $k \in \overline{0,9}$, відносно операції множення.

62.10. множина всіх квадратних матриць 2-го порядку над полем $\mathbb{Z}_7$, визначник яких дорівнює $\overline{1}$, відносно операції множення матриць.

62.11. множина всіх матриць виду $\begin{pmatrix} a & \overline{0} & \overline{0} \\ \overline{0} & b & \overline{0} \\ c & \overline{0} & d \end{pmatrix}$, де $a, b, c \in \mathbb{Z}_3 \backslash \{\overline{0}\}$, відносно операції множення матриць.

62.12. множина всіх комплексних чисел z, що задовольняють умову $z^5 = 1$, відносно: а) операції додавання; б) операції множення.

62.13. множина M матриць виду $\begin{pmatrix} a & b & c \\ \overline{0} & d & f \\ \overline{0} & \overline{0} & g \end{pmatrix}$, де $a, b, c, d, f, g \in \mathbb{Z}_3 \backslash \{\overline{0}\}$, відносно операції множення матриць.

62.14. множина $M = \{-1, 0, 1\}$ відносно: а) операції додавання; б) операції множення.

62.15. множина M всіх невироджених симетричних матриць 2-го порядку над полем $\overline{Z}_5$ відносно операції множення матриць.

62.16. множина M всіх матриць виду $\begin{pmatrix} \overline{0} & c \\ -c & \overline{0} \end{pmatrix}$, де $c \in \mathbb{Z}_7$, відносно операції додавання матриць.

62.17. множина $M = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$ відносно операції множення матриць.

62.18. множина M всіх кососиметричних матриць 3-го порядку над полем $\mathbb{Z}_3$, тобто матриць виду $\begin{pmatrix} \overline{0} & a & b \\ -a & \overline{0} & c \\ -b & -c & \overline{0} \end{pmatrix}$, де $a, b, c \in \mathbb{Z}_3\}$, відносно операції додавання матриць.

62.19. множина M всіх матриць виду $\begin{pmatrix} a & \overline{0} \\ b & \overline{1} \end{pmatrix}$, де $b \in \mathbb{Z}_5$, $a \in \{\overline{1}, \overline{4}\}$, відносно операції множення матриць.

62.20. множина $M = \{1, -1, i, -i, \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\}$ відносно операції множення.

62.21. множина матриць виду $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, де $a, b \in \mathbb{Z}_5$ такі, що $a^2 + b^2 = \overline{1}$, відносно операції множення матриць.

62.22. множина $M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$ відносно операції множення матриць.

62.23. множина M всіх комплексних чисел z виду $z = \cos\frac{\pi k}{10} + i \sin\frac{\pi k}{10}$, де $k \in \overline{0, 9}$, відносно операції множення.

62.24. множина M матриць виду $\begin{pmatrix} a & \overline{0} & \overline{0} \\ b & c & \overline{0} \\ d & f & g \end{pmatrix}$, де $a, b, c, d, f, g \in \mathbb{Z}_3$, причому $acg \neq \overline{0}$.

62.25. множина M всіх невироджених матриць виду $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, де $c \in \mathbb{Z}_5$, відносно операції множення матриць.

2. Групи підстановок. Циклічні групи

ТЕОРЕТИЧНІ ВІДОМОСТІ

Порядком $|G|$ групи G називають кількість її елементів. Якщо в групі G скінченна кількість елементів, то G називається **скінченною** (пишуть $|G| < \infty$); якщо нескінченна кількість, то **нескінченною** (пишуть $|G| = \infty$).

Симетрична група підстановок S_n

Нехай $M_n = \{1, 2, ..., n\}$ – множина перших n натуральних чисел. Позначимо через S_n множину всіх взаємно однозначних відображень множини M_n на себе. Ці відображення назвемо підстановками:

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix}, \dots, \gamma = \begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_1 & \gamma_2 & \dots & \gamma_n \end{pmatrix},$$

де $\alpha_i, \beta_i, \gamma_i \in M_n$, $1 \leqslant i \leqslant n, \alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$, $\gamma_i \neq \gamma_j$, при $i \neq j$, $1 \leqslant j \leqslant n$.

На множині S_n всіх підстановок степеня n задамо операцію множення. Під множенням підстановок α і β будемо розуміти послідовне виконання відображень α і β:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \delta_1 & \delta_2 & \dots & \delta_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \delta_1 & \delta_2 & \dots & \delta_n \end{pmatrix} = \delta.$$

Множина S_n відносно операції множення підстановок є неабелевою групою, $|S_n| = n!$. Її називають симетричною групою підстановок n-го степеня.

Множина A_n всіх парних підстановок із S_n є підгрупою групи S_n, $|A_n| = \frac{n!}{2}$. Її називають знакозмінною групою підстановок n-го степеня.

Циклічні групи

Нехай $\langle G; * \rangle$ – група, a – довільний її елемент. Підгрупа H групи G називається циклічною, якщо в G існує такий елемент a, що кожен елемент $h \in H$ можна записати у вигляді $h = \underbrace{a * a * a * ... * a}_{k}$ або $h = \underbrace{a' * a' * a' * ... * a'}_{k}$, де a' – елемент, симетричний до a відносно операції $*$, для деякого $k \in \mathbb{N} \cup \{0\}$.

У випадку мультиплікативної групи G підгрупа H групи G називається циклічною, якщо всі її елементи є степенями деякого фіксованого її елемента a, тобто якщо $H = \langle a \rangle = \{a^k | k \in \mathbb{Z}\}$. Зокрема, група G називається циклічною, якщо всі її елементи є степенями деякого фіксованого її елемента g, тобто якщо $G = \langle g \rangle = \{g^k | k \in \mathbb{Z}\}$. Елемент g при цьому називається породжуючим (або твірним) елементом групи G.

У випадку адитивної групи G підгрупа H групи G називається циклічною, якщо всі її елементи є кратними деякого фіксованого її елемента a, тобто якщо $H = \langle a \rangle = \{ka | k \in \mathbb{Z}\}$. Зокрема, група G називається циклічною, якщо всі її елементи є кратними деякого фіксованого її елемента g, тобто якщо $G = \langle g \rangle = \{kg | k \in \mathbb{Z}\}$.

Порядком $|a|$ елемента a групи $\langle G; * \rangle$ називається таке найменше натуральне число n, що $\underbrace{a * a * ... * a}_{n} = e$, де e – одиничний елемент групи G. Якщо такого натурального числа n не існує, то говорять, що елемент a має нескінченний порядок, і записують: $|a| = \infty$.

Нехай G – мультиплікативна група.

1. Якщо $|a| = n$, то $a^k = e$ тоді і лише тоді, коли $k \vdots n$.
2. $|\langle a\rangle| = |a|$.
3. Будь-яка підгрупа циклічної групи є циклічною.
4. Нехай $G = \langle a\rangle$, $|G| = n$. Тоді:

4.1 елемент a^k є твірним елементом групи G тоді і лише тоді, коли $(k, n) = 1$.
4.2 для кожного дільника m числа n в G існує і причому єдина підгрупа порядку m, твірним елементом якої є $a^{\frac{n}{m}}$

5. Всі скінченні циклічні групи одного й того самого порядку m ізоморфні між собою і ізоморфні адитивній групі $\mathbb{Z}_m$. Всі нескінченні циклічні групи ізоморфні між собою і ізоморфні адитивній групі $\mathbb{Z}$ цілих чисел.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 63.1. Нехай G – циклічна група порядку 10, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^6;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^8\rangle$ в G;
д) підгрупу $K = \langle a^5\rangle \cap \langle a^6\rangle$.

Розв'язання. а) За твердженням 4.1, елемент a^k циклічної групи $G = \langle a\rangle$, $|G| = 10$, буде її твірним елементом тоді і лише тоді, коли $(k, 10) = 1$. Кількість таких натуральних k дорівнює $\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4$; ними є: $k = 1$, $k = 3$, $k = 7$, $k = 9$. Отже, твірними елементами групи є елементи: a, a^3, a^7 і a^9.

б) Знайдемо таке найменше натуральне число n, що $(a^6)^n = e$, де e – одиничний елемент групи G.

Маємо:

$$(a^6)^2 = a^{12} = a^{10} \cdot a^2 = e \cdot a^2 = a^2 \neq e;$$
$$(a^6)^3 = (a^6)^2 \cdot a^6 = a^2 \cdot a^6 = a^8 \neq e;$$
$$(a^6)^4 = (a^6)^3 \cdot a^6 = a^8 \cdot a^6 = a^{14} = a^{10} \cdot a^4 = a^4 \neq e;$$
$$(a^6)^5 = (a^6)^4 \cdot a^6 = a^4 \cdot a^6 = a^{10} = e.$$

Отже, $\left|a^6\right| = 5$.

в) *Спосіб I.* Оскільки G – циклічна, то, в силу твердження 3, її підгрупи теж є циклічними. Тоді в G знайдеться такий елемент a^s, $0 \leqslant s \leqslant 9$, що $H = \langle a^s\rangle$.

Якщо $s = 0$, то $H_1 = \langle a^0 \rangle = \{e\}$ – одинична підгрупа.

Якщо $s \in \{1, 3, 7, 9\}$, то, як показано в п.б), $\langle a^s \rangle = G$, значить, $H_2 = G$.

Нехай $s = 2$, тоді $H_3 = \langle a^2 \rangle =$
$= \left\{a^2, (a^2)^2 = a^4, (a^2)^3 = a^6, (a^2)^4 = a^8, (a^2)^5 = e\right\} = \left\{a^2, a^4, a^6, a^8, e\right\}$.

Нехай $s = 4$. Тоді $H = \langle a^4 \rangle =$
$= \left\{a^4, (a^4)^2 = a^8, (a^4)^3 = a^2, (a^4)^4 = (a^4)^3 \cdot a^4 = a^2 \cdot a^4 = a^6, (a^4)^5 = e\right\} = \left\{a^4, a^8, a^2, a^6, e\right\} = H_3$.

Аналогічно показуємо, що $\langle a^6 \rangle = H_3$ і $\langle a^8 \rangle = H_3$.

Нехай $s = 5$. Тоді $H_4 = \langle a^5 \rangle = \left\{a^5, (a^5)^2 = a^{10} = e\right\} = \left\{a^5, e\right\}$.

Отже, в групі G є лише такі підгрупи:

$$
\begin{aligned}
&H_1 = \{e\} - \text{ одинична підгрупа;}\\
&H_2 = G - \text{ сама група } G;\\
&H_3 = \langle a^2 \rangle = \langle a^4 \rangle = \langle a^6 \rangle = \langle a^8 \rangle = \left\{a^2, a^4, a^6, a^8, e\right\};\\
&H_4 = \left\{a^5, e\right\}.
\end{aligned}
$$

Зауваження 1. Оскільки порядок підгрупи H_3 дорівнює 5 (тобто простий), в H_3 кожний елемент є твірним. Тому, знайшовши підгрупу H_3 і знаючи її елементи, можна було окремо не шукати $\langle a^4 \rangle$, $\langle a^6 \rangle$, $\langle a^8 \rangle$, а одразу записати $\langle a^4 \rangle = \langle a^6 \rangle = \langle a^8 \rangle = H_3$.

Спосіб II. В силу властивості 4.2, група G порядку 10 має $\tau(10) = \tau(2 \cdot 5) = 4$ підгрупи. Ними є:

$$
\begin{aligned}
&\langle a^{\frac{10}{1}} \rangle = \langle a^{10} \rangle = \langle e \rangle = \{e\};\\
&\langle a^{\frac{10}{2}} \rangle = \langle a^5 \rangle = \{a^5, e\};\\
&\langle a^{\frac{10}{5}} \rangle = \langle a^2 \rangle = \{a^2, a^4, a^6, a^8, e\};\\
&\langle a^{\frac{10}{10}} \rangle = \langle a \rangle = G.
\end{aligned}
$$

г) Порядок $|\langle a^8 \rangle|$ підгрупи $\langle a^8 \rangle = H_3$ (див. в)) дорівнює 5. За наслідком із теореми Лагранжа (див. §9)

$$|G : \langle a^8 \rangle| = \frac{|G|}{|\langle a^8 \rangle|} = \frac{10}{5} = 2.$$

д) Елементами підгрупи $K = \langle a^5 \rangle \cap \langle a^6 \rangle$ є ті і лише ті елементи, що одночасно належать як до $\langle a^5 \rangle$, так і до $\langle a^6 \rangle$. Таким елементом є лише елемент e. Отже, $K = \langle a^5 \rangle \cap \langle a^6 \rangle = \{e\}$.

Розробка процедур. В Maple є можливість працювати із двома типами груп: симетричними групами підстановок та групами, заданими за допомогою

твірних елементів та визначальних співвідношень. При цьому під заданням групи за допомогою твірних елементів та визначальних співвідношень розуміють наступне. Підгрупою групи G, породженою даною підмножиною M, називається підгрупа $\langle M\rangle$, що складається із всіх елементів $g \in G$ виду $g = a_1^{k_1}a_2^{k_2}...a_s^{k_s}$, де $a_i \in M$, $s \in \mathbb{N}$, $c_i \in \mathbb{Z}$ для $i \in \overline{1,s}$. Зокрема, говорять, що група G породжується множиною M, якщо $G = \langle M\rangle$. Виділити серед всіх груп із породжуючою множиною M конкретну групу можна, задаючи для елементів множини M певні співвідношення. Наприклад, циклічну групу $G = \langle a\rangle$ порядку n можна розглядати як групу із породжуючою множиною $M = \{a\}$ і визначальним співвідношенням $a^n = e$, де e – одиничний елемент групи G. Для розв'язування даного завдання такий підхід не зовсім зручний, однак в подальшому він знадобиться (див. Приклад 66.2). Тут використаємо наступне.

Як відомо (див. властивість 5), скінченна група $G = \langle a\rangle$ порядку n ізоморфна адитивній групі $\mathbb{Z}_n$ класів лишків за модулем n: $\mathbb{Z}_n = \{\overline{0},\overline{1},...,\overline{n-1}\}$, при цьому в якості ізоморфізму можна взяти відображення $\varphi : G \to \mathbb{Z}_n$ за правилом $\varphi(a^k) = \overline{k}$. Досліджуватимемо в Maple саме властивості групи $\mathbb{Z}_n$ і всі процедури створимо для дослідження властивостей саме цієї групи.

а) Для пошуку множини всіх твірних елементів групи $\mathbb{Z}_n$ використаємо властивість 4.1: елемент $\overline{a}$ є твірним елементом групи $\mathbb{Z}_n$ тоді і лише тоді, коли $(a,n) = 1$. Процедура матиме наступний код:

```
generators:=proc(n)
local M,i;
   M:={};
   for i from 1 to n-1 do
      if igcd(i,n)=1 then M:=M union {i}; end if;
   end do;
   return(M);
end proc:
```

б) Для розробки процедури пошуку порядку деякого елемента циклічної групи використаємо наступні міркування. Нехай m – порядок елемента $\overline{a}^s$ циклічної групи $G = \langle a\rangle$ порядку n. Тоді m – найменше натуральне число таке, що

$$(a^s)^m = e, \tag{VII.1}$$

де e – одиничний елемент групи G. В групі $\mathbb{Z}_n$ рівності (VII.1) відповідатиме умова $sm \equiv 0 \pmod n$. Розв'язуючи дану конгруенцію, знаходимо число m. Однак зауважимо, що використовувати для розв'язання конгруенції

команду **msolve** із пакету **numtheory** не досить зручно: її результатом є множина класів лишків, а нам потрібне найменше натуральне число m, яке задовольняє дану конгруенцію. Тому шукатимемо число m, випробовуючи послідовно числа множини $\overline{1, n-1}$. Як тільки число m таке, що $sm \equiv 0 \pmod{n}$, знайдене, робота циклу завершується.

Процедура пошуку порядку m елемента $\overline{s}$ в групі $\mathbb{Z}_n$ матиме вигляд:

```
OrdZ:=proc(s,n)
local m;
   m:=1;
   while (m<=n-1) and (m*s mod n<>0) do m:=m+1; end do;
   return(m);
end proc:
```

в) За властивістю 4.2, підгрупи групи $\overline{Z}_n$ всі є циклічними і мають вигляд $\langle\overline{\frac{n}{m}}\rangle$, де m – натуральний дільник числа n.

Створимо спочатку процедуру побудови циклічної підгрупи групи $\mathbb{Z}_n$, породженої деяким її елементом $\overline{x}$. Підгрупа $H = \langle\overline{x}\rangle$ групи $\mathbb{Z}_n$ складається із елементів $\underbrace{\overline{x} + \overline{x} + ... + \overline{x}}_{m} = m \cdot \overline{x}$, де $k \in \overline{0, n-1}$. На початку задаємо $H = \{x\}$. В ході циклу до множини H поступово додаємо елементи $2\overline{x} = x + x \bmod n$, $3\overline{x}$, $4\overline{x}$,... поки не отримаємо нульовий елемент $\overline{0}$.

```
cyclicSubZ:=proc(x,n)
local b,H,z,m;
   z:=x;
   m:=1;
   H:={x};
   while z<>0 do z:=z+x mod n; m:=m+1; H:=H union {z}; end do;
   return(H);
end proc:
```

Наприклад, для елемента $\overline{2}$ групи $\mathbb{Z}_{10}$ матимемо:

```
> cyclicSubZ(2,10);
```

$$\{0,\ 2,\ 4,\ 6,\ 8\}$$

тобто $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$

Використаємо процедуру **cyclicSubZ** для побудови процедури відшукання всіх підгруп групи $\mathbb{Z}_n$. В ході процедури:

1) знаходимо всі можливі натуральні дільники числа n:

```
> M:=divisors(n);
```

2) для кожного із дільників $M[i]$ числа n знаходимо підгрупу порядку $M[i]$: її твірним елементом є елемент $\langle\overline{\frac{n}{M[i]}}\rangle$:

```
> for i from 1 to nops(M) do
  if M[i]<>1 then s:=cyclicSubZ(n/M[i],n) else
     s:=cyclicSubZ(n/M[i] mod n,n); end if;
```

Процедура матиме наступний код:

```
subgroups:=proc(n)
uses numtheory:
local M,i,gen,s;
   gen:=generators(n)[1];
   M:=divisors(n);
   for i from 1 to nops(M) do
      if M[i]<>1 then s:=cyclicSubZ(n/M[i],n)
      else s:=cyclicSubZ(n/M[i] mod n,n);
      end if;
   print(s);
   end do;
end proc:
```

4) Для відшукання індексу підгрупи H в групі G (за формулою $[G : H] = \frac{|G|}{|H|}$) введемо функцію **indexG**:

```
> indexG:=(H,G)-> nops(G)/nops(H):
```

Розв'язання в Maple. Застосовуємо створені процедури для дослідження властивостей групи $\mathbb{Z}_{10}$, ізоморфної групі $G = \langle a \rangle$ 10-го порядку.

```
> Z10:={$0..9}:
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

а) Шукаємо твірні елементи:

```
> generators(10);
```

$$\{1,\ 3,\ 7,\ 9\}$$

Твірними елементами групи $\mathbb{Z}_{10}$ є елементи $\overline{1}, \overline{3}, \overline{7}, \overline{9}$. Тоді твірними елементами заданої групи G є елементи a^1, a^3, a^7, a^9.

б) Знаходимо порядок елемента $\overline{6}$ в групі $\mathbb{Z}_{10}$:

```
> OrdZ(6,10);
```

$$5$$

Отже, порядок елемента $\overline{6}$ в групі $\mathbb{Z}_{10}$ дорівнює 5, відповідно порядок елемента a^6 в групі $G = \langle a \rangle$ також дорівнює 5.

в) Знаходимо підгрупи групи $\mathbb{Z}_{10}$:

```
> subgroups(10);
```

$$\{0\}$$
$$\{0,\ 5\}$$

$$\{0,\ 2,\ 4,\ 6,\ 8\}$$
$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$

Таким чином, група Z_{10} має всього 4 підгрупи: $\{\overline{0}\}$, $\{\overline{0},\overline{5}\}$, $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8}\}$, $\mathbb{Z}_{10}$. Відповідно задана група $G=\langle a\rangle$ має також лише 4 підгрупи, а саме: $\{e\}$, $\{e,a^5\}=\langle a^5\rangle$, $\langle e,a^2,a^4,a^6,a^8\rangle=\langle a^2\rangle$, G.

г) Шукаємо індекс підгрупи $H_3=\langle\overline{8}\rangle$ в групі Z_{10}.

```
> H3:=cyclicSubZ(8,10);
```
$$H3 := \{0,\ 2,\ 4,\ 6,\ 8\}$$
```
> indexG(H3,Z10);
```
$$2$$

Отже, $[\mathbb{Z}_{10}:H_3]=2$, тоді відповідно $[G:\langle a^8\rangle]=2$.

д) Знаходимо підгрупи $K_1=\langle\overline{5}\rangle$ та $K_2=\langle\overline{6}\rangle$ групи $\mathbb{Z}_{10}$:

```
> K1:=cyclicSubZ(5,10);
```
$$K := \{0,\ 5\}$$
```
> K2:=cyclicSubZ(6,10);
```
$$L := \{0,\ 2,\ 4,\ 6,\ 8\}$$

та їхній перетин:

```
> K1 intersect K2;
```
$$\{0\}$$

Отже, $K_1\cap K_2=\overline{0}$, тоді і $K=\langle a^5\rangle\cap\langle a^6\rangle=\{a^0\}=\{e\}$.

Приклад 63.2. Нехай $G=\langle z\rangle$, де $z=\cos\frac{\pi}{9}+i\sin\frac{\pi}{9}$. Знайти:

а) порядок групи G;
б) всі твірні елементи групи G;
в) всі підгрупи групи G;
г) порядок елемента z^8;
д) індекс підгрупи $\langle z^8\rangle$ в G;
е) підгрупу $K=\langle z^6\rangle\cap\langle z^8\rangle$.

Розв'язання. а) Група G є підгрупою, наприклад, мультиплікативної групи $\mathbb{C}^*$ відмінних від нуля комплексних чисел, тому її одиничним елементом є комплексне число 1. Оскільки порядок циклічної групи дорівнює порядку її твірного елемента, знаходимо таке натуральне найменше число n, що $z^n=1$. За формулою Муавра

$$z^n=\left(\cos\frac{\pi}{9}+i\sin\frac{\pi}{9}\right)^n=\cos\frac{n\pi}{9}+i\sin\frac{n\pi}{9}.$$

Тому $\cos\frac{n\pi}{9}+i\sin\frac{n\pi}{9}=1$. З умови рівності двох комплексних чисел випливає, що

$$\begin{cases}\cos\frac{n\pi}{9}=1,\\ \sin\frac{n\pi}{9}=0;\end{cases}\quad\text{звідки}\quad\begin{cases}\frac{n\pi}{9}=2\pi m,\quad m\in\mathbb{Z},\\ \frac{n\pi}{9}=\pi t,\quad t\in\mathbb{Z}.\end{cases}$$

Тоді $\begin{cases}n=18m,\\ n=9t,\quad m,t\in\mathbb{Z}.\end{cases}$ Найменше натуральне число, кратне 9 і 18 одночасно, – це число 18. Отже, $|z|=18$, а значить, і $|G|=18$.

б) За твердженням 4.1 елемент z^k циклічної групи $G=\langle z\rangle$, $|G|=18$, буде її твірним елементом тоді і лише тоді, коли $(k,18)=1$. Таких натуральних чисел k всього є $\varphi(18)=\varphi(2)\varphi(3^2)=1\cdot 3^2\left(1-\frac{1}{3}\right)=6$; а саме: $k=1$, $k=5$, $k=7$, $k=11$, $k=13$, $k=17$. Отже, твірними елементами групи G є елементи: z, z^5, z^7, z^{11}, z^{13} і z^{17}.

в) *Спосіб I.* Див. приклад 63.1 в).

Спосіб II. В силу твердження 4.2, в групі G для кожного дільника m порядку групи G існує і лише одна, підгрупа порядку m. Дільниками числа 18 є числа: 1, 2, 3, 6, 9, 18. Отже, група G має лише 6 різних підгруп порядків 1, 2, 3, 6, 9, 18 відповідно. Знайдемо їх. Оскільки G – циклічна, то і всі її підгрупи H теж є циклічними. Нехай $H=\langle z^s\rangle$, $0\leqslant s\leqslant 17$. Порядок m підгрупи H дорівнює порядку її твірного елемента. Таким чином, питання пошуку всіх підгруп в циклічній групі еквівалентне питанню пошуку для кожного дільника m числа $|G|$ такого елемента групи, що має порядок m. Нехай:

1) $m=1$, тоді, очевидно, $H_1=\langle 1\rangle$ – одинична підгрупа.

2) $m=2$. Тоді $H_2=\langle z^{\frac{18}{2}}\rangle=\langle z^9\rangle=\{z^9,1\}$ – підгрупа порядку 2.

3) $m=3$. Тоді $H_3=\langle z^{\frac{18}{3}}\rangle=\langle z^6\rangle=\{z^6,z^{12},1\}$ – підгрупа порядку 3.

4) $m=6$. Тоді $H_4=\langle z^{\frac{18}{6}}\rangle=\langle z^3\rangle=\{z^3,z^6,z^9,z^{12},z^{15},1\}$ – підгрупа порядку 6.

5) $m=9$. Тоді $H_5=\langle z^{\frac{18}{9}}\rangle=\langle z^2\rangle=\{z^2,z^4,z^6,z^8,z^{10},z^{12},z^{14},z^{16},1\}$ – підгрупа порядку 9.

6) $m=18=|G|$. Тоді $H_6=G$.

Таким чином, в групі $G=\langle a\rangle$ порядку 18 є такі підгрупи:

$$H_1=\langle 1\rangle,\ H_2=\langle z^9\rangle,\ H_3=\langle z^6\rangle,\ H_4=\langle z^3\rangle,\ H_5=\langle z^2\rangle,\ H_6=G.$$

г) *Спосіб I.* Див. приклад 63.1 б).

Спосіб II. Порядок елемента z^8 дорівнює порядку циклічної групи $\langle z^8\rangle$, яку він породжує. В G є лише підгрупи H_1, H_2, H_3, H_4, H_5, H_6 із в). Елемент z^8 належить лише до підгруп H_5 і H_6. Оскільки z^8 не є твірним елементом групи G, то $\langle z^8\rangle\neq H_6$. Значить, $\langle z^8\rangle=H_5$, а значить, $|\langle z^8\rangle|=|H_5|=9$.

д) Індекс підгрупи $H_5 = \langle z^8 \rangle$ в G за наслідком 2 із теореми Лагранжа дорівнює

$$|G : H_5| = \frac{|G|}{|H_5|} = \frac{18}{9} = 2.$$

е) Елементами підгрупи $K = \langle z^6 \rangle \cap \langle z^8 \rangle$ є ті і лише ті елементи, що одночасно належать як до $\langle z^6 \rangle$, так і до $\langle z^8 \rangle = H_5$. Такими елементами є елементи $z^6, z^{12}, 1$. Отже, $K = \langle z^6 \rangle \cap \langle z^8 \rangle = \{z^6, z^{12}, 1\}$.

Розробка процедур. Створимо процедуру для відшукання порядку n елемента a довільної групи $\langle G; * \rangle$. В ході процедури послідовно знаходитимемо елементи $a * a$, $a * a * a$, $a * a * a * a$, ..., доки в результаті не отримаємо нейтральний елемент e. Елемент a може мати і нескінченний порядок, тоді натурального числа n такого, що $\underbrace{a * a * ... * a}_{n} = e$, не існує. Тому пошук числа n обмежуємо певним діапазоном $1..m$, де m – параметр процедури, який задає довільним чином користувач (наприклад, 1..100). В результаті якщо $|a| \leqslant m$, то процедура поверне значення $n = |a|$. Якщо ж всі числа від 1 до m перебрано і потрібного не знайдено, отримаємо: FAIL. В даному випадку FAIL означатиме, що або порядок елемента a більший за m, або нескінченний, тоді можна спробувати розширити діапазон для пошуку числа n (задавши більше значення параметра m), або перевірити, чи не є порядок нескінченним.

Процедура матиме наступний код:

```
OrdG:=proc(a,e,operation,m)
local b,n;
   b:=a;
   n:=1;
   while (b<>e) and (n<=m) do b:=operation(b,a); n:=n+1; end do;
   if n=m+1 then return(FAIL) else return(n); end if;
end proc:
```

Розв'язання в Maple. а) Для пошуку порядку елемента z застосовуємо процедуру **OrdG**. Оскільки група G є підгрупою мультиплікативної групи $\mathbb{C}^*$ відмінних від нуля комплексних чисел, то її одиничним елементом є комплексне число 1. Задаємо число z і операцію множення:

```
> z:=cos(Pi/9)+I*sin(Pi/9);
  mult:=(x,y)->simplify(x*y):
```

Зауважимо, що при заданні операції mult використано також команду **simplify**, яка буде спрощувати отриманий результат. Без цієї додаткової команди відбуватиметься наступне:

```
> z*z;
```

$$(\cos(\frac{\pi}{9}) + \sin(\frac{\pi}{9})\, I)^2$$

```
> z*z*z;
```

$$(\cos(\frac{\pi}{9}) + \sin(\frac{\pi}{9})\, I)^3$$

Знаходимо порядок елемента z (обмежуючи діапазон пошуку числом $m = 100$):

```
> read(‘e:/atchlib.m‘); with(atchlib):
> OrdG(z,1,mult,100);
```

18

Отже, $|z| = 18$. Тоді і порядок групи $G = \langle z \rangle$ дорівнює 18.

б)-е) аналогічно до Прикладу 63.1. Для групи $\mathbb{Z}_{18}$:

```
> Z18:={$0..17}:
```

яка ізоморфна групі G, маємо:

```
> generators(18);
```

{1, 5, 7, 11, 13, 17}

Твірними елементами групи $\mathbb{Z}_{18}$ є: $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}$, відповідно твірними елементами групи G є: $z, z^5, z^7, z^{11}, z^{13}, z^{17}$.

```
> OrdZ(8,18);
```

5

Порядок елемента $\overline{8}$ в $\mathbb{Z}_{18}$ дорівнює 9, відповідно порядок елемента z^8 в G також дорівнює 9.

```
> subgroups(18);
```

{0}

{0, 9}

{0, 6, 12}

{0, 3, 6, 9, 12, 15}

{0, 2, 4, 6, 8, 10, 12, 14, 16}

{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17}

Підгрупами групи $\mathbb{Z}_{18}$ є: $\{\overline{0}\}$, $\{\overline{0}, \overline{9}\} = \langle \overline{9} \rangle$, $\{\overline{0}, \overline{6}, \overline{12}\} = \langle \overline{6} \rangle$. $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\} = \langle \overline{3} \rangle$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}\} = \langle \overline{2} \rangle$, $\mathbb{Z}_{18}$. Відповідно маємо наступні підгрупи групи G: $\{1\}$, $\langle z^9 \rangle$, $\langle z^6 \rangle$, $\langle z^3 \rangle$, $\langle z^2 \rangle$, G.

Задаємо підгрупу $H_3 = \langle \overline{8} \rangle$ групи $\mathbb{Z}_{18}$ і знаходимо її індекс в $\mathbb{Z}_{18}$:

```
> H3:=cyclicSubZ(8,18);
```

$H3 :=$ {0, 2, 4, 6, 8, 10, 12, 14, 16}

```
> indexG(H3,Z18);
```

2

Отже, $[\mathbb{Z}_{18} : \langle\overline{8}\rangle] = 2$, тоді і $[G : \langle z^8\rangle] = 2$.

Тепер задаємо підгрупи $K_1 = \langle\overline{6}\rangle$ і $K_2 = \langle\overline{8}\rangle$ групи $\mathbb{Z}_{18}$ і знаходимо їхній перетин:

```
> K1:=cyclicSubZ(6,18);
```

$$K := \{0,\ 6,\ 12\}$$

```
> K2:=cyclicSubZ(8,18);
```

$$L := \{0,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14,\ 16\}$$

```
> K1 intersect K2;
```

$$\{0,\ 6,\ 12\}$$

Отже, $K_1 \cap K_2 = \{\overline{0}, \overline{6}, \overline{12}\} = \langle\overline{6}\rangle$, тоді і $\langle z^6\rangle \cap \langle z^8\rangle = \langle z^6\rangle$.

Приклад 63.3. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ невироджених квадратних матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \end{pmatrix}$;

б) всі твірні елементи групи $T = \langle A\rangle$;

в) всі підгрупи групи T;

г) порядок елемента A^6;

д) індекс підгрупи $\langle A^4\rangle$ в T;

е) підгрупу $K = \langle A^6\rangle \cap \langle A^4\rangle$.

Розв'язання. В групі $\mathrm{GL}_2(\mathbb{C})$ одиничним елементом є матриця $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Знаходимо таке найменше натуральне число n, що $A^n = E$.

Спосіб I. Маємо:

$$
\begin{aligned}
A &= \begin{pmatrix} \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix} \neq E;\\
A^2 &= A\cdot A = \begin{pmatrix} \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix} =\\
&= \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \neq E;\\
A^3 &= A^2\cdot A = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix} =\\
&= \begin{pmatrix} -\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & -\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix} \neq E;\\
A^4 &= A^3\cdot A = \begin{pmatrix} -\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & -\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i \end{pmatrix} =\\
&= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq E;\\
A^5 &= A^4\cdot A = \begin{pmatrix} -\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i & 0 \\ 0 & -\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i \end{pmatrix} \neq E;\\
A^6 &= A^5\cdot A = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \neq E;\\
A^7 &= A^6\cdot A = \begin{pmatrix} \frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i & 0 \\ 0 & \frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i \end{pmatrix} \neq E;\\
A^8 &= A^8\cdot A = E.
\end{aligned}
$$

Отже, порядок елемента A дорівнює 8.

Спосіб II. Нехай $\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i = z$. Покажемо, що $A^n = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}^n = \begin{pmatrix} z^n & 0 \\ 0 & z^n \end{pmatrix}$, використовуючи метод математичної індукції. При $n=1$ твердження очевидне. Припустимо, що твердження справедливе при $n-1$. Тоді $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}^n = \begin{pmatrix} z^{n-1} & 0 \\ 0 & z^{n-1} \end{pmatrix}\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} = \begin{pmatrix} z^n & 0 \\ 0 & z^n \end{pmatrix}$. В силу принципу математичної індукції, твердження справедливе для довільного $n \in \mathbb{N}$.

Нехай $|A| = n$. Тоді n – таке найменше натуральне число, що $A^n =$

E. Значить, $\begin{pmatrix} z^n & 0 \\ 0 & z^n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Звідси, $z^n = 1$. Запишемо число z в тригонометричній формі: $z = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$. Тоді, за формулою Муавра, $\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$. З умови рівності двох комплексних чисел отримуємо:

$$\begin{cases} \cos\frac{n\pi}{4} = 1, \\ \sin\frac{n\pi}{4} = 0; \end{cases} \quad \text{звідки} \quad \begin{cases} \frac{n\pi}{4} = 2\pi m, \quad m \in \mathbb{Z}, \\ \frac{n\pi}{4} = \pi t, \quad t \in \mathbb{Z}. \end{cases}$$

Тоді $\begin{cases} n = 8m, \\ n = 4t, \quad m, t \in \mathbb{Z}. \end{cases}$ Найменше натуральне число, кратне 8 і 4 одночасно, – це число 8. Отже, порядок елемента A дорівнює 8.

б) За твердженням 4.1 елемент A^k циклічної групи $T = \langle A\rangle$, $|T| = 8$, буде її твірним елементом тоді і лише тоді, коли $(k, 8) = 1$. Кількість таких натуральних k дорівнює $\varphi(8) = 2^3 - 2^2 = 4$; ними є: $k = 1$, $k = 3$, $k = 5$, $k = 7$. Отже, твірними елементами групи T є елементи: A, A^3, A^5 і A^7.

в) В силу властивості 4.2, група T має $\tau(8) = 4$ підгрупи. Ними є:

$$\begin{aligned} &\langle A^{\frac{8}{1}}\rangle = \langle A^8\rangle = \langle E\rangle = \{E\}; \\ &\langle A^{\frac{8}{2}}\rangle = \langle A^4\rangle = \{A^4, E\}; \\ &\langle A^{\frac{8}{4}}\rangle = \langle A^2\rangle = \{A^2, A^4, A^6, E\}; \\ &\langle A^{\frac{8}{8}}\rangle = \langle A\rangle = T. \end{aligned}$$

г) Знайдемо таке найменше натуральне число n, що $(A^6)^n = E$. Маємо:

$$\begin{aligned} &(A^6)^2 = A^{12} = A^8 \cdot A^4 = E \cdot A^4 = A^4 \neq E; \\ &(A^6)^3 = A^{18} = (A^8)^2 \cdot A^2 = A^2 \neq E; \\ &(A^6)^4 = A^{24} = (A^8)^3 = E. \end{aligned}$$

Отже, порядок елемента A^6 дорівнює 4.

д) Порядок підгрупи $\langle A^4\rangle = H_3$ дорівнює 2. За наслідком 2 із теореми Лагранжа,

$$|G : \langle A^4\rangle| = \frac{|T|}{|\langle A^4\rangle|} = \frac{8}{2} = 4.$$

е) Елементами підгрупи $K = \langle A^6\rangle \cap \langle A^4\rangle$ є ті і лише ті елементи, що одночасно належать як до $\langle A^6\rangle = \{A^2, A^4, A^6, E\}$ (див. п.г)), так і до $\langle A^4\rangle$. Такими елементами є елементи A^4, E. Отже, $K = \{A^4, E\}$.

Розробка процедур. Для відшукання порядку елемента групи матриць можна використати загальну процедуру **OrdG** (відшукання порядку довільної групи), створену при розв'язанні Прикладу 63.2.

А можна створити окрему процедуру **OrdM**, застосовну лише до елементів мультиплікативної групи матриць $GL_2(\mathbb{C})$. Для цього дещо модифікуємо процедуру **OrdG**.

В такому випадку параметр *e* не потрібний (оскільки одиничним елементом завжди виступатиме одинична матриця). Водночас, одиничну матрицю не будемо задавати і в тілі процедури, а замість умови b<>e процедури **OrdG** введемо умову IsMatrixShape(b, identity)<>true. Команда **IsMatrixShape(b, identity)** здійснює перевірку, чи є матриця *b* одиничною, чи ні. Поки матриця не є одиничною, відбувається множення матриць *b.a* (операція множення об'єктів Matrix в Maple позначається крапкою).

```
OrdM:=proc(a,m)
uses LinearAlgebra;
local b,n;
   b:=a; n:=1;
   while (IsMatrixShape(b, identity)<>true) and (n<=m) do
      b:=simplify(b.a); n:=n+1;
   end do;
   if n=m+1 then return(FAIL) else return(n); end if;
end proc:
```

Розв'язання в Maple. а) Спосіб I: Використовуємо загальну команду **OrdG**, створену при розв'язуванні Прикладу 63.2. Матриці задаємо за допомогою об'єктів типу Lists (див. Приклад 21.1), операцію множення матриць задаємо безпосередньо:

```
> A:=[[1/sqrt(2)+1/sqrt(2)*I,0],[0,1/sqrt(2)+1/sqrt(2)*I]]:
  E:=[[1,0],[0,1]]:
  mmult:=(A,B)->simplify([[A[1,1]*B[1,1]+A[1,2]*B[2,1],
                           A[1,1]*B[1,2]+A[1,2]*B[2,2]],
                          [A[2,1]*B[1,1]+A[2,2]*B[2,1],
                           A[2,1]*B[1,2]+A[2,2]*B[2,2]]]):
```

Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

```
> OrdG(A,E,mmult,100);
```

8

Спосіб II (зручніший): застосовуємо процедуру **OrdM**. Тут для задання матриць використовуватимемо об'єкти типу Matrix:

```
> A:=Matrix([[1/sqrt(2)+1/sqrt(2)*I,0],[0,1/sqrt(2)
  +1/sqrt(2)*I]]);
```

$$A := \begin{bmatrix} \frac{\sqrt{2}}{2} + \frac{1}{2} I \sqrt{2} & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{1}{2} I \sqrt{2} \end{bmatrix}$$

Для заданої матриці A матимемо:

```
> n:=OrdM(A,100);
```

$$n := 8$$

Отже, порядок елемента A дорівнює 8. Для перевірки правильності відшукання степенів $A^2, A^3, \ldots$ елемента A можна використати команду **trace**:

```
> trace(OrdM); n:=OrdM(A,100);
```

OrdM

```
{--> enter OrdM, args = Matrix(2, 2, [[...],[...]], datatype =
anything), 100
```

$$b := \begin{bmatrix} \frac{\sqrt{2}}{2} + \frac{1}{2} I \sqrt{2} & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{1}{2} I \sqrt{2} \end{bmatrix}$$

$$n := 1$$

$$b := \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

$$n := 2$$

$$b := \begin{bmatrix} (\frac{-1}{2} + \frac{1}{2} I) \sqrt{2} & 0 \\ 0 & (\frac{-1}{2} + \frac{1}{2} I) \sqrt{2} \end{bmatrix}$$

$$n := 3$$

$$b := \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$n := 4$$

$$b := \begin{bmatrix} -\frac{\sqrt{2}}{2} - \frac{1}{2} I \sqrt{2} & 0 \\ 0 & -\frac{\sqrt{2}}{2} - \frac{1}{2} I \sqrt{2} \end{bmatrix}$$

$$n := 5$$

$$b := \begin{bmatrix} -I & 0 \\ 0 & -I \end{bmatrix}$$

$$n := 6$$

$$b := \begin{bmatrix} (\frac{1}{2} - \frac{1}{2}\,I)\sqrt{2} & 0 \\ 0 & (\frac{1}{2} - \frac{1}{2}\,I)\sqrt{2} \end{bmatrix}$$

$$n := 7$$

$$b := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

```
> n := 8;
```

```
<-- exit OrdM (now at top level) = 8}
```

$$n := 8$$

б)-е) аналогічно до Прикладів 63.1 і 63.2. Група $T = \langle A \rangle$ ізоморфна групі $\mathbb{Z}_8$. Маємо:

```
> Z8:={$0..7}:
```

```
> generators(8);
```

$$\{1,\ 3,\ 5,\ 7\}$$

Твірними елементами групи $\mathbb{Z}_8$ є: $\overline{1}, \overline{3}, \overline{5}, \overline{7}$, відповідно твірними елементами групи T є: A, A^3, A^5, A^7.

```
> OrdZ(6,8);
```

$$4$$

Порядок елемента $\overline{6}$ в $\mathbb{Z}_8$ дорівнює 4, відповідно порядок елемента A^6 в T також дорівнює 4.

```
> subgroups(8);
```

$$\{0\}$$

$$\{0,\ 4\}$$

$$\{0,\ 2,\ 4,\ 6\}$$

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7\}$$

Підгрупами групи $\mathbb{Z}_8$ є: $\{\overline{0}\}$, $\{\overline{0}, \overline{4}\} = \langle \overline{4} \rangle$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\} = \langle \overline{2} \rangle$, $\mathbb{Z}_8$. Відповідно маємо підгрупи групи T: $\{E\}$, $\langle A^4 \rangle$, $\langle A^2 \rangle$, T.

Задаємо підгрупу $H_3 = \langle \overline{4} \rangle$ групи Z_8:

```
> H3:=cyclicSubZ(4,8);
```

$$H3 := \{0,\ 4\}$$

і знаходимо її індекс в Z_8:

```
> indexG(H3,Z8);
```

$$2$$

Отже, $[\mathbb{Z}_8 : \langle\overline{4}\rangle] = 4$, тоді і $[T : \langle A^4\rangle] = 4$.

Тепер задаємо підгрупи $K_1 = \langle\overline{6}\rangle$ і $K_2 = \langle\overline{4}\rangle$ групи $\mathbb{Z}_8$ і знаходимо їхній перетин:

```
> K1:=cyclicSubZ(6,8);
```

$$K := \{0,\ 2,\ 4,\ 6\}$$

```
> K2:=cyclicSubZ(4,8);
```

$$K2 := \{0,\ 4\}$$

```
> K1 intersect K2;
```

$$\{0,\ 4\}$$

Отже, $K_1 \cap K_2 = \{\overline{0}, \overline{4}\}$, тоді і $\langle A^6\rangle \cap \langle A^4\rangle = \{A^4, E\} = \langle A^4\rangle$.

Завдання 63.

63.1. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ невироджених квадратних матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$;

б) всі твірні елементи групи $T = \langle A\rangle$;

в) всі підгрупи групи T;

г) порядок елемента A^3;

д) індекс підгрупи $\langle A^4\rangle$ в T;

е) підгрупу $K = \langle A^2\rangle \cap \langle A^4\rangle$.

63.2. Нехай G – циклічна група порядку 14, породжена елементом a. Знайти:

а) всі твірні елементи групи G;

б) порядок елемента a^4;

в) всі підгрупи групи G;

г) індекс підгрупи $\langle a^3\rangle$ в G;

д) підгрупу $K = \langle a^4\rangle \cap \langle a^3\rangle$.

63.3. В мультиплікативній групі $G = \langle z\rangle$, де $z = \cos\frac{\pi}{8} + i\sin\frac{\pi}{8}$, знайти:

а) порядок групи G;

б) всі твірні елементи групи G;

в) всі підгрупи групи G;

г) порядок елемента z^6;
д) індекс підгрупи $\langle z^6\rangle$ в G;
е) підгрупу $K = \langle z^2\rangle \cap \langle z^4\rangle$.

63.4. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} -i & 1 \\ 0 & 1 \end{pmatrix}$;
б) всі твірні елементи групи $T = \langle A\rangle$;
в) всі підгрупи групи T;
г) порядок елемента A^3;
д) індекс підгрупи $\langle A^3\rangle$ в T;
е) підгрупу $K = \langle A^2\rangle \cap \langle A^3\rangle$.

63.5. Нехай G – циклічна група порядку 10, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^2;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^6\rangle$ в G;
д) підгрупу $K = \langle a^8\rangle \cap \langle a^5\rangle$.

63.6. В мультиплікативній групі $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ відмінних від 0 комплексних чисел знайти:

а) порядок підгрупи $G = \langle z\rangle$, де $z = \frac{1}{2} - \frac{\sqrt{3}}{2}i$;
б) всі твірні елементи групи G;
в) всі підгрупи групи G;
г) порядок елемента z^4;
д) індекс підгрупи $\langle z^6\rangle$ в G;
е) підгрупу $K = \langle z^2\rangle \cap \langle z^6\rangle$.

63.7. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} -i & \frac{1}{2} \\ 0 & i \end{pmatrix}$;
б) всі твірні елементи групи $T = \langle A\rangle$;
в) всі підгрупи групи T;

г) порядок елемента A^2;
д) індекс підгрупи $\langle A^2\rangle$ в T;
е) підгрупу $K = \langle A^2\rangle \cap \langle A^3\rangle$.

63.8. В адитивній групі $\mathbb{Z}_{20}$ знайти:

а) всі твірні елементи групи $\mathbb{Z}_{20}$;
б) порядок елемента $\overline{4}$;
в) всі підгрупи групи $\mathbb{Z}_{20}$;
г) індекс підгрупи $\langle\overline{6}\rangle$ в $\mathbb{Z}_{20}$;
д) підгрупу $K = \langle\overline{4}\rangle \cap \langle\overline{6}\rangle$.

63.9. Нехай G – циклічна група порядку 25, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^5;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^1 0\rangle$ в G;
д) підгрупу $K = \langle a^5\rangle \cap \langle a^1 0\rangle$.

63.10. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i & -2 \\ 0 & i \end{pmatrix}$;
б) всі твірні елементи групи $T = \langle A\rangle$;
в) всі підгрупи групи T;
г) порядок елемента A^6;
д) індекс підгрупи $\langle A^5\rangle$ в T;
е) підгрупу $K = \langle A^2\rangle \cap \langle A^6\rangle$.

63.11. В мультиплікативній групі $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ відмінних від 0 комплексних чисел знайти:

а) порядок підгрупи $G = \langle z\rangle$, де $z = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$;
б) всі твірні елементи групи G;
в) всі підгрупи групи G;
г) порядок елемента z^6;
д) індекс підгрупи $\langle z^7\rangle$ в G;
е) підгрупу $K = \langle z^6\rangle \cap \langle z^7\rangle$.

63.12. Нехай G – циклічна група порядку 16, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^3;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^2\rangle$ в G;
д) підгрупу $K = \langle a^{10}\rangle \cap \langle a^7\rangle$.

63.13. В мультиплікативній групі $G = \langle z\rangle$, де $z = \cos 15^\circ + i \sin 15^\circ$, знайти:

а) порядок групи G;
б) всі твірні елементи групи G;
в) всі підгрупи групи G;
г) порядок елемента z^4;
д) індекс підгрупи $\langle z^3\rangle$ в G;
е) підгрупу $K = \langle z^3\rangle \cap \langle z^6\rangle$.

63.14. Нехай G – циклічна група порядку 24, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^8;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^{15}\rangle$ в G;
д) підгрупу $K = \langle a^{20}\rangle \cap \langle a^{15}\rangle$.

63.15. В адитивній групі $\mathbb{Z}_{12}$ знайти:

а) всі твірні елементи групи $\mathbb{Z}_{12}$;
б) порядок елемента $\overline{9}$;
в) всі підгрупи групи $\mathbb{Z}_{12}$;
г) індекс підгрупи $\langle\overline{3}\rangle$ в $\mathbb{Z}_{12}$;
д) підгрупу $K = \langle\overline{6}\rangle \cap \langle\overline{8}\rangle$.

63.16. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ невироджених квадратних матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$;
б) всі твірні елементи групи $T = \langle A\rangle$;

в) всі підгрупи групи T;
г) порядок елемента A^2;
д) індекс підгрупи $\langle A^2\rangle$ в T;
е) підгрупу $K = \langle A^2\rangle \cap \langle A^4\rangle$.

63.17. В мультиплікативній групі $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ відмінних від 0 комплексних чисел знайти:

а) порядок елемента $z = \cos\frac{\pi}{15} + i\sin\frac{\pi}{15}$;
б) всі твірні елементи групи $T = \langle z\rangle$;
в) всі підгрупи групи T;
г) порядок елемента z^3;
д) індекс підгрупи $\langle z^3\rangle$ в T;
е) підгрупу $K = \langle z^3\rangle \cap \langle z^9\rangle$.

63.18. В адитивній групі $\mathbb{Z}_{13}$ знайти:

а) всі твірні елементи групи $\mathbb{Z}_{13}$;
б) порядок елемента $\overline{4}$;
в) всі підгрупи групи $\mathbb{Z}_{13}$;
г) індекс підгрупи $\langle\overline{2}\rangle$ в $\mathbb{Z}_{13}$;
д) підгрупу $K = \langle\overline{6}\rangle \cap \langle\overline{4}\rangle$.

63.19. Нехай G – циклічна група порядку 21, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^{14};
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^1 0\rangle$ в G;
д) підгрупу $K = \langle a^4\rangle \cap \langle a^{14}\rangle$.

63.20. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{C})$ матриць 2-го порядку над полем $\mathbb{C}$ комплексних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} 1 & 13 \\ 0 & -\frac{\sqrt{3}}{2} + \frac{1}{2}i \end{pmatrix}$;
б) всі твірні елементи групи $T = \langle A\rangle$;
в) всі підгрупи групи T;
г) порядок елемента A^6;

д) індекс підгрупи $\langle A^4\rangle$ в T;
е) підгрупу $K = \langle A^6\rangle \cap \langle A^4\rangle$.

63.21. Нехай G – циклічна група порядку 12, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^6;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^2\rangle$ в G;
д) підгрупу $K = \langle a^2\rangle \cap \langle a^6\rangle$.

63.22. В адитивній групі $\mathbb{Z}_{14}$ знайти:

а) всі твірні елементи групи $\mathbb{Z}_{14}$;
б) порядок елемента $\overline{12}$;
в) всі підгрупи групи $\mathbb{Z}_{14}$;
г) індекс підгрупи $\langle\overline{5}\rangle$ в $\mathbb{Z}_{14}$;
д) підгрупу $K = \langle\overline{5}\rangle \cap \langle\overline{14}\rangle$.

63.23. В мультиплікативній групі $G = \langle z\rangle$, де $z = \frac{-\sqrt{3}}{2} + \frac{1}{2}i$, знайти:

а) порядок групи G;
б) всі твірні елементи групи G;
в) всі підгрупи групи G;
г) порядок елемента z^2;
д) індекс підгрупи $\langle z^6\rangle$ в G;
е) підгрупу $K = \langle z^2\rangle \cap \langle z^4\rangle$.

63.24. Нехай G – циклічна група порядку 9, породжена елементом a. Знайти:

а) всі твірні елементи групи G;
б) порядок елемента a^5;
в) всі підгрупи групи G;
г) індекс підгрупи $\langle a^2\rangle$ в G;
д) підгрупу $K = \langle a^5\rangle \cap \langle a^3\rangle$.

63.25. В мультиплікативній групі $\mathrm{GL}_2(\mathbb{R})$ невироджених квадратних матриць 2-го порядку над полем $\mathbb{R}$ дійсних чисел знайти:

а) порядок елемента $A = \begin{pmatrix} -\frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix}$;

б) всі твірні елементи групи $T = \langle A \rangle$;
в) всі підгрупи групи T;
г) порядок елемента A^2;
д) індекс підгрупи $\langle A^3 \rangle$ в T;
е) підгрупу $K = \langle A^3 \rangle \cap \langle A^2 \rangle$.

Приклад 64. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$;
б) елемент a^{-1};
в) елемент a^{2010};
г) підгрупу $\langle a^2 \rangle$ та її індекс в S_4;
д) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$;
е) множину $C_{S_4}(a)$ всіх елементів групи S_4, які переставні із елементом a (таку множину $C_G(a) = \{x \in G | xa = ax\}$ називають централізатором елемента a в групі G, причому $C_G(a) \leqslant G$).

Розв'язання. а) Одиничним елементом групи S_4 є елемент $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$.
Знайдемо таке найменше натуральне число n, що $a^n = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.
Маємо:

$$a^2 = aa = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix};$$

$$a^3 = a^2 a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix};$$

$$a^4 = a^3 a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e.$$

Отже, $|a| = 4$.

б) *Спосіб I.* Елемент a^{-1} будемо шукати у вигляді $a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ x & y & z & u \end{pmatrix}$. За означенням оберненого елемента

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ x & y & z & u \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Перемноживши підстановки в лівій частині рівності, отримуємо:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ y & z & u & x \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Звідси $y = 1$, $z = 2$, $u = 3$, $x = 4$. Отже, $a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

Спосіб II. Для того, щоб знайти елемент a^{-1}, обернений до a, міняємо місцями 1-ий і 2-ий рядочки підстановки a:

$$a^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

в) Врахуємо, що $|a| = 4$ (див. а)), тобто $a^4 = e$. За теоремою про ділення з остачею, маємо: $2010 = 4 \cdot 502 + 2$. Отже,

$$a^{2010} = (a^4)^{502} \cdot a^2 = a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

г) Підгрупа $\langle a^2 \rangle$ складається з усіх можливих різних степенів елемента a^2. Знайдемо ці степені:

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

$$(a^2)^2 = a^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e.$$

Отже, $\langle a^2 \rangle = \{a^2, e\}$. За наслідком 2 із теореми Лагранжа,

$$|S_4 : \langle a^2 \rangle| = \frac{|S_4|}{|\langle a^2 \rangle|} = \frac{4!}{2} = 12.$$

д) Знаходимо порядок елемента c:

$$\begin{aligned} c &\neq e; \\ c^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \neq e; \\ c^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e. \end{aligned}$$

Отже, $|c| = 3$, тоді і $|\langle c\rangle| = 3$, одночасно знайдено і саму підгрупу F:

$$F = \{c, c^2, e\} = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}\}.$$

До підгрупи L належать елементи, спільні для множин $H = \langle a\rangle$ і F:

$$L = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}\} = \{e\}.$$

е) Якщо $x \in C_{S_4}(a)$, то $xa = ax$. Нехай $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$. Маємо:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

тоді

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ x_3 & x_1 & x_2 & x_4 \end{pmatrix}.$$

Домножимо обидві частини даної рівності зліва на x^{-1}:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 2 & 3 & 4 \\ x_3 & x_1 & x_2 & x_4 \end{pmatrix},$$

тобто

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ 1 & 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ x_3 & x_1 & x_2 & x_4 \end{pmatrix},$$

значить,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_1 & x_2 & x_4 \end{pmatrix},$$

Очевидно, $x_4 = 4$. Далі можливі випадки: а) $x_1 = 1$, б) $x_1 = 2$, в) $x_1 = 3$.

Якщо $x_1 = 1$, то $x_3 = 3$, звідки $x_2 = 2$;

якщо $x_1 = 2$, то $x_3 = 1$, звідки $x_2 = 3$;

якщо $x_1 = 3$, то $x_3 = 2$, звідки $x_2 = 1$.

Таким чином, є лише три підстановки, переставні із підстановкою a, а саме: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = a$. Отже,

$$C_{S_4}(a) = \left\{e, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, a\right\}.$$

Розробка процедур. Створимо процедуру для відшукання степеня x^k підстановки x. В ході даної процедури за допомогою циклу **for** послідовно знаходимо добутки xx, xxx, $xxxx$,...,$\underbrace{xx...x}_{k}$ (для множення підстановок a і b в Maple є команда **mulperms(a,b)** із пакету **group**):

```
permPower:=proc(x,k)
uses group;
local h,m,f,s,i:
   f:=x:
   for i from 1 to k-1 do f:=mulperms(f, x); end do;
   return(f);
end proc:
```

Крім того, створимо процедуру для відшукання індексу підгрупи в групі підстановок (створену при розв'язанні Прикладу 63.1 (функцію **indexG** використати не можна через специфічне задання груп підстановок в Maple). Для відшукання порядку групи підстановок в пакеті **group** є спеціальна команда **grouporder**. Код процедури матиме вигляд:

```
indexP:=proc(H,G)
uses group;
   grouporder(G)/grouporder(H);
end proc:
```

Розв'язання в Maple. Для задання групи підстановок G використовується команда **permgroup(n, gens)** із пакету **group**, де n – степінь групи підстановок, **gens** – множина підстановок, які породжують групу G. Підстановки в Maple записують за допомогою циклів. При цьому під циклом (довжини k) в алгебрі розуміють підстановку виду

$$\begin{pmatrix} \alpha_1 & \alpha_2 & ... & \alpha_k & \beta_1 & \beta_2 & ... & \beta_{n-k} \\ \alpha_2 & \alpha_3 & ... & \alpha_1 & \beta_1 & \beta_2 & ... & \beta_{n-k} \end{pmatrix} \in S_n. \qquad \text{(VII.2)}$$

Так, наприклад, підстановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 5 & 4 & 6 & 2 & 3 \end{pmatrix}$ є циклом довжини 5, оскільки її можна записати у вигляді $\begin{pmatrix} 2 & 7 & 3 & 5 & 6 & 1 & 4 \\ 7 & 3 & 5 & 6 & 2 & 1 & 4 \end{pmatrix}$. До числа циклів належать і транспозиції. За аналогією із використовуваним скороченим записом транспозицій, для циклів використовується наступний запис: символи, які переходять в інші символи, записують в круглих дужках один за одним в тому порядку, в якому вони один в одний переходять: починається запис із будь-якого символа, і вважають, що останній символ переходить в перший; символи, які переходять самі в себе, не запи-

сують. Підстановку (VII.2) записують у вигляді $(\alpha_1\alpha_2...\alpha_k)$ або у будь-якому вигляді $(\alpha_i\alpha_{i+1}...\alpha_k\alpha_1...\alpha_{i-1})$. Для наведеного вище прикладу такий запис має вигляд: (27356). Два цикли $(\alpha_1\alpha_2...\alpha_k)$ і $(\beta_1\beta_2...\beta_l)$ називають незалежними, якщо вони не мають спільних символів (тобто множини $\{\alpha_1, \alpha_2, ..., \alpha_k\}$ і $\{\beta_1, \beta_2, ..., \beta_l\}$ перетинаються). Кожну підстановку можна записати у вигляді добутку попарно незалежних циклів, наприклад: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = (132)(45)$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 7 & 6 & 8 & 4 & 5 \end{pmatrix} = (13)(47)(568)$.

В Maple підстановку $(l_1l_2...l_s)(k_1k_2...k_t)$, де l_i і k_j – попарно різні (подану у вигляді добутку незалежних циклів), записують наступним чином: $[[l_1, l_2, ..., l_s][k_1, k_2, ..., k_t]]$, одиничну підстановку подають у вигляді порожнього списку [].

Наведемо задання груп підстановок S_n і A_n за допомогою твірних елементів:

$$S_n = \langle (12), (13), (14), ..., (1n) \rangle = \langle (12), (123...n) \rangle;$$

$$A_n = \langle (ijk) | i, j, k - \text{ попарно різні числа із множини } \overline{1, n} \rangle$$

(тобто група A_n породжується всіма можливими потрійними циклами).

Задаємо групу $S_4 = \langle (12), (1234) \rangle$:

```
> with(group):
  S4:=permgroup(4, {[[1,2]], [[1,2,3,4]]}):
```

а) Для того, щоб знайти порядок елемента симетричної групи підстановок S_4, використаємо той факт, що порядок елемента a дорівнює порядку циклічної підгрупи $H = \langle a \rangle$, яку він породжує. Для відшукання порядку групи використаємо команду **grouporder**. Задаємо елемент a і підгрупу $H = \langle a \rangle$:

```
> a:=[[1,2,3,4]]:
  H:=permgroup(4, {a}):
> grouporder(H);
```

4

Отже, $|a| = 4$.

б) Підстановку, обернену до даної підстановки a, знаходять за допомогою команди **invperm(a)**.

```
> invperm(a);
```

[[1, 4, 3, 2]]

Отже, $a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

в) Для відшукання степеня x^k підстановки x використовуємо створену процедуру **permPower**:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> permPower(a,2010);
```

[[1, 3], [2, 4]]

Отже, $a^{2010} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

г) Нехай $b = a^2$:

```
> b:=permPower(a, 2);
```

$b :=$ [[1, 3], [2, 4]]

Задаємо підгрупу $K = \langle b \rangle$:

```
> K:=permgroup(4, {b}):
```

Елементами підгрупи K є:

```
> elements(K);
```

{[], [[1, 3], [2, 4]]}

Отже, $K = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\}$.

Індекс підгрупи K в S_4 шукаємо за допомогою процедури **indexP**:

```
> indexP(K,S4);
```

12

Таким чином, $[S_4 : \langle a^2 \rangle] = 12$.

д) Задаємо елемент c і підгрупу $F = \langle c \rangle$:

```
> c:=[[1,2,3]]: F:=permgroup(4, {c}):
```

і знаходимо перетин L підгруп H і F:

```
> L:=inter(H,F):
> elements(L);
```

{[]}

Отже, $L = \{e\}$.

д) Для пошуку централізатора елемента (або деякої множини M елементів) заданої групи підстановок G використовується команда **centralizer(G,M)** із пакету **group**. (У випадку, коли M складається більше ніж з одного елемента, дана команда знаходить множину всіх елементів групи G, які переставні з кожним елементом множини M.) Маємо:

```
> C:=centralizer(S4,{c}):
> elements(C);
```

{[], [[1, 2, 3]], [[1, 3, 2]]}

Таким чином, $C_{S_4}(a) = \left\{e, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = a\right\}$.

Завдання 64.

64.1. В симетричній групі підстановок S_5 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$;
б) елементи a^{-1}, a^{2012};
в) підгрупу $\langle a^3 \rangle$ та її індекс в S_5;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$;
д) централізатор $C_{S_5}(a)$ елемента a в групі S_5.

64.2. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$;
б) елементи a^{-1}, a^{2011};
в) підгрупу $\langle a^2 \rangle$ та її індекс в S_4;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;
д) централізатор $C_{S_4}(a)$ елемента a в групі S_4.

64.3. В симетричній групі підстановок S_6 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$;
б) елементи a^{-1}, a^{2013};
в) підгрупу $\langle a^2 \rangle$ та її індекс в S_6;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 2 & 6 & 5 \end{pmatrix}$;
д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.4. В симетричній групі підстановок S_7 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 7 & 2 & 4 & 6 \end{pmatrix}$;
б) елементи a^{-1}, a^{2012};
в) підгрупу $\langle a^5 \rangle$ та її індекс в S_7;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$;

д) централізатор $C_{S_7}(a)$ елемента a в групі S_7.

64.5. В симетричній групі підстановок S_6 знайти:

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

б) елементи a^{-1}, a^{2009};

в) підгрупу $\langle a^3 \rangle$ та її індекс в S_6;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 1 & 6 \end{pmatrix}$;

д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.6. В симетричній групі підстановок S_5 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$;

б) елементи a^{-1}, a^{2012};

в) підгрупу $\langle a^2 \rangle$ та її індекс в S_5;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix}$;

д) централізатор $C_{S_5}(a)$ елемента a в групі S_5.

64.7. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;

б) елементи a^{-1}, a^{2010};

в) підгрупу $\langle a^3 \rangle$ та її індекс в S_4;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$;

д) централізатор $C_{S_4}(a)$ елемента a в групі S_4.

64.8. В симетричній групі підстановок S_7 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$;

б) елементи a^{-1}, a^{2011};

в) підгрупу $\langle a^3 \rangle$ та її індекс в S_7;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$;

д) централізатор $C_{S_7}(a)$ елемента a в групі S_7.

64.9. В симетричній групі підстановок S_6 знайти:

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

б) елементи a^{-1}, a^{2009};
в) підгрупу $\langle a^3\rangle$ та її індекс в S_6;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 5 & 6 & 3 \end{pmatrix}$;
д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.10. В симетричній групі підстановок S_5 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$;
б) елементи a^{-1}, a^{2011};
в) підгрупу $\langle a^2\rangle$ та її індекс в S_5;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$;
д) централізатор $C_{S_5}(a)$ елемента a в групі S_5.

64.11. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$;
б) елементи a^{-1}, a^{2011};
в) підгрупу $\langle a^3\rangle$ та її індекс в S_4;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$;
д) централізатор $C_{S_4}(a)$ елемента a в групі S_4.

64.12. В симетричній групі підстановок S_6 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}$;
б) елементи a^{-1}, a^{2012};
в) підгрупу $\langle a^5\rangle$ та її індекс в S_6;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 5 & 2 & 3 \end{pmatrix}$;
д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.13. В симетричній групі підстановок S_7 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 3 & 2 & 1 & 7 & 6 \end{pmatrix}$;
б) елементи a^{-1}, a^{2011};
в) підгрупу $\langle a^2\rangle$ та її індекс в S_7;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 3 & 2 & 1 & 6 & 7 \end{pmatrix}$;

д) централізатор $C_{S_7}(a)$ елемента a в групі S_7.

64.14. В симетричній групі підстановок S_8 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 3 & 8 & 7 & 5 & 4 & 2 \end{pmatrix}$;

б) елементи a^{-1}, a^{2011};

в) підгрупу $\langle a^4 \rangle$ та її індекс в S_8;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 4 & 3 & 7 & 5 & 8 & 2 \end{pmatrix}$;

д) централізатор $C_{S_8}(a)$ елемента a в групі S_8.

64.15. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$;

б) елементи a^{-1}, a^{2010};

в) підгрупу $\langle a^3 \rangle$ та її індекс в S_4;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$;

д) централізатор $C_{S_4}(a)$ елемента a в групі S_4.

64.16. В симетричній групі підстановок S_5 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$;

б) елементи a^{-1}, a^{2011};

в) підгрупу $\langle a^2 \rangle$ та її індекс в S_5;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$;

д) централізатор $C_{S_5}(a)$ елемента a в групі S_5.

64.17. В симетричній групі підстановок S_6 знайти:

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

б) елементи a^{-1}, a^{2010};

в) підгрупу $\langle a^3 \rangle$ та її індекс в S_6;

г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$;

д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.18. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$;

б) елементи a^{-1}, a^{2013};
в) підгрупу $\langle a^2\rangle$ та її індекс в S_4;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$;
д) централізатор $C_{S_4}(a)$ елемента a в групі S_4.

64.19. В симетричній групі підстановок S_6 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix}$;
б) елементи a^{-1}, a^{2010};
в) підгрупу $\langle a^4\rangle$ та її індекс в S_6;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 2 & 6 \end{pmatrix}$;
д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.20. В симетричній групі підстановок S_5 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$;
б) елементи a^{-1}, a^{2012};
в) підгрупу $\langle a^4\rangle$ та її індекс в S_5;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$;
д) централізатор $C_{S_5}(a)$ елемента a в групі S_5.

64.21. В симетричній групі підстановок S_4 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$;
б) елементи a^{-1}, a^{2011};
в) підгрупу $\langle a^3\rangle$ та її індекс в S_4;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$;
д) централізатор $C_{S_4}(a)$ елемента a в групі S_4.

64.22. В симетричній групі підстановок S_6 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 3 & 2 \end{pmatrix}$;
б) елементи a^{-1}, a^{2011};
в) підгрупу $\langle a^2\rangle$ та її індекс в S_6;
г) підгрупу $L = \langle a\rangle \cap \langle c\rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$;

д) централізатор $C_{S_6}(a)$ елемента a в групі S_6.

64.23. В симетричній групі підстановок S_7 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 6 & 5 & 4 \end{pmatrix}$;
б) елементи a^{-1}, a^{2012};
в) підгрупу $\langle a^3 \rangle$ та її індекс в S_7;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$;
д) централізатор $C_{S_7}(a)$ елемента a в групі S_7.

64.24. В симетричній групі підстановок S_5 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$;
б) елементи a^{-1}, a^{2013};
в) підгрупу $\langle a^2 \rangle$ та її індекс в S_5;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$;
д) централізатор $C_{S_5}(a)$ елемента a в групі S_5.

64.25. В симетричній групі підстановок S_9 знайти:

а) порядок елемента $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 1 & 7 & 8 & 6 & 5 & 3 & 2 \end{pmatrix}$;
б) елементи a^{-1}, a^{2012};
в) підгрупу $\langle a^3 \rangle$ та її індекс в S_9;
г) підгрупу $L = \langle a \rangle \cap \langle c \rangle$, де $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 1 & 4 & 7 & 6 & 5 & 3 & 9 \end{pmatrix}$;
д) централізатор $C_{S_9}(a)$ елемента a в групі S_9.

Приклад 65. Знайти мультиплікативну групу $\mathbb{Z}_m^*$ кільця $\mathbb{Z}_m$ класів лишків за модулем m. Визначити, чи є вона циклічною, якщо:
а) $m = 15$; б) $m = 10$.

Розв'язання. Спосіб I. а) Мультиплікативна група $\mathbb{Z}_{15}^*$ кільця $\mathbb{Z}_{15}$ складається з усіх дільників одиниці цього кільця. Знайдемо їх. Маємо:

$$\mathbb{Z}_{15} = \left\{ K_0^{(15)}, K_1^{(15)}, \ldots, K_{14}^{(15)} \right\},$$

де $K_1^{(15)} = e$ – одиничний елемент кільця $\mathbb{Z}_{15}$. В силу наслідку 1 із теореми 1 п.2 §2 розд.III [1], клас $K_a^{(15)}$ є дільником одиниці тоді і тільки тоді, коли

$(a, 15) = 1$. Таких чисел a, $0 \leqslant a \leqslant 14$, є всього $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$, а саме: $a = 1, 2, 4, 7, 8, 11, 13, 14$. Отже, дільниками одиниці кільця $\mathbb{Z}_{15}$ є: $K_1^{(15)}$, $K_2^{(15)}$, $K_4^{(15)}$, $K_7^{(15)}$, $K_8^{(15)}$, $K_{11}^{(15)}$, $K_{13}^{(15)}$, $K_{14}^{(15)}$. Значить,

$$\mathbb{Z}_{15}^* = \left\{K_1^{(15)}, K_2^{(15)}, K_4^{(15)}, K_7^{(15)}, K_8^{(15)}, K_{11}^{(15)}, K_{13}^{(15)}, K_{14}^{(15)}\right\}.$$

Припустимо, що група $\mathbb{Z}_{15}^*$ – циклічна. Тоді в $\mathbb{Z}_{15}^*$ знайдеться елемент $K_x^{(15)}$, порядок якого дорівнює порядку групи $\mathbb{Z}_{15}^*$ (тобто 8). Іншими словами елемент $K_x^{(15)}$ повинен задовольняти 2 умови:

$$\left(K_x^{(15)}\right)^8 = K_1^{(15)}$$

$$\text{і} \qquad \left(K_x^{(15)}\right)^s \neq K_1^{(15)} \quad \text{при} \quad 1 \leqslant s < 8. \tag{VII.3}$$

Проте:

$$\left(K_2^{(15)}\right)^4 = K_{16}^{(15)} = K_1^{(15)} = e;$$

$$\left(K_4^{(15)}\right)^2 = K_{16}^{(15)} = K_1^{(15)} = e;$$

$$\left(K_7^{(15)}\right)^4 = \left(K_{49}^{(15)}\right)^2 = \left(K_{19}^{(15)}\right)^2 = K_1^{(15)} = e;$$

$$\left(K_8^{(15)}\right)^4 = \left(K_2^{(15)} K_4^{(15)}\right)^4 = K_{16}^{(15)} = K_1^{(15)} = e;$$

$$\left(K_{11}^{(15)}\right)^2 = K_1^{(15)} = e;$$

$$\left(K_{13}^{(15)}\right)^4 = \left(K_{169}^{(15)}\right)^2 = \left(K_{19}^{(15)}\right)^2 = K_1^{(15)} = e;$$

$$\left(K_{14}^{(15)}\right)^2 = K_1^{(15)} = e.$$

Отже, такого елемента, що задовольняє умову (VII.3), в $\mathbb{Z}_{15}^*$ немає. Значить, припущення невірне – група $\mathbb{Z}_{15}^*$ не є циклічною.

б) Знаходимо $\mathbb{Z}_{10}^*$. Порядок групи $\mathbb{Z}_{10}^*$ дорівнює $\varphi(10) = \varphi(2)\varphi(5) = 4$. Маємо:

$$\mathbb{Z}_{10}^* = \left\{K_a^{(10)} | (a, 10) = 1\right\} = \left\{K_1^{(10)}, K_3^{(10)}, K_7^{(10)}, K_9^{(10)}\right\}.$$

Знайдемо порядки її елементів. Оскільки порядок елемента є дільником порядку групи (тобто числа 4), то його слід шукати серед чисел 1, 2, 4. Одиничним елементом групи $\mathbb{Z}_{10}^*$ є елемент $e = K_1^{(10)}$. Маємо: $(K_2^{(10)})^2 \neq e$, але тоді обов'язково порядок елемента $K_2^{(10)}$ дорівнює 4. Таким чином, в $\mathbb{Z}_{10}^*$ існує елемент, порядок якого дорівнює порядку групи, значить, $\mathbb{Z}_{10}^* = K_2^{(10)}$ – циклічна.

Спосіб II. Покажемо, що порядок елемента $\overline{a} = K_a^{(m)}$ мультиплікативної групи $\mathbb{Z}_m^*$ – це порядок $P_m(a)$ числа a за модулем m. Дійсно, нехай $|\overline{a}| = m$, тоді m – найменше натуральне число, що задовольняє умову $\overline{a}^m = \overline{1}$. Дана рівність еквівалентна конгруенції $a \equiv 1 \pmod{m}$. Але тоді $m = P_m(a)$.

Елемент $\overline{a}$ є твірним елементом групи $\mathbb{Z}_m^*$ тоді і лише тоді, коли його порядок дорівнює $|\mathbb{Z}_m^*| = \varphi(m)$. Але тоді $P_m(a) = \varphi(m)$, тобто a – первісний корінь за модулем m. Первісні корені, як відомо, існують лише для модулів $m \in \{p^\alpha, 2p^\alpha\}$, де p – непарне просте число, $\alpha \in \mathbb{N}$, та $m = 2^\alpha$, де $\alpha \in \overline{0,2}$. Для числа $m = 15$ первісного кореня не існує, тому група $\mathbb{Z}_{15}^*$ не є циклічною. Для числа $m = 10 = 2 \cdot 5$ первісний корінь існує, тому група $\mathbb{Z}_{10}^*$ є циклічною.

Розробка процедур. Задамо функцію для пошуку елемента мультиплікативної групи $\mathbb{Z}_m^*$ кільця $\mathbb{Z}_m$. Ця група складається із усіх дільників одиниці цього кільця $\mathbb{Z}_m$. Знайдемо їх, вибираючи з чисел множини $\{0, 1, .., m-1\}$ взаємно прості із числом m:

```
> U:=m->select(i->evalb(igcd(i,m)=1),{$0..m-1}):
```

Тепер створимо процедуру для перевірки, чи є мультиплікативна група $\mathbb{Z}_m^*$ циклічною. Для того, щоб скінченна група порядку m була циклічною, необхідно і достатньо, щоб знайшовся елемент, порядок якого дорівнює числу m. Порядок групи $\mathbb{Z}_m^*$ дорівнює числу $\varphi(m)$, тому в ході процедури **isCyclic(G,m)** для кожного елемента групи $G = \mathbb{Z}_m^*$ перевіряємо, чи дорівнює його порядок числу $\varphi(m)$. (При розв'язанні даного Прикладу способом II було показано, що порядок елемента $\overline{a}$ мультиплікативної групи $\mathbb{Z}_m^*$ – це порядок $P_m(a)$ числа a за модулем m, який можна знайти за допомогою команди **order(a,m)** із пакету **numtheory**.) Якщо такий елемент знайдено, перевірка закінчується.

```
isCyclic:=proc(G,m)
uses numtheory:
local j:
   for j from 1 to nops(G) do
   if order(G[j],m)=phi(m) then return(true); break; end if;
      j:=j+1; end do;
   if j=nops(G)+1 then return(false); end if;
      end proc:
```

Розв'язання в Maple. За допомогою функції **U** знаходимо елементи групи $\mathbb{Z}_{15}^*$:

```
> read(‘e:/atchlib.m‘); with(atchlib):
```

```
> U(15);
```

$$\{1, 2, 4, 7, 8, 11, 13, 14\}$$

Перевіряємо, чи є група $\mathbb{Z}_{15}^*$ циклічною:

```
> isCyclic(U(15),15);
```

false

Таким чином, група $\mathbb{Z}_{15}^*$ не є циклічною. Аналогічно можна легко перевірити, чи є група $\mathbb{Z}_{10}^*$ циклічною:

```
> U(10);
```

$$\{1, 3, 7, 9\}$$

```
> isCyclic(U(10),10);
```

true

Група $\mathbb{Z}_{10}^*$ – циклічна.

Для перевірки можна також використати спосіб II аналітичного розв'язання. За допомогою команди **primroot(m)** із пакету **numtheory** можна не лише визначити, чи існує первісний корінь за модулем m, але навіть і знайти цей корінь.

```
> with(numtheory):
  primroot(15);
```

FAIL

Первісний корінь за модулем 15 не існує, тому група $\mathbb{Z}_{15}^*$ не є циклічною.

```
> primroot(10);
```

3

За модулем 10 первісний корінь існує, тому група $\mathbb{Z}_{10}^*$ є циклічною. більше того, $\mathbb{Z}_{10}^* = \langle\overline{3}\rangle$.

Завдання 65. Знайти мультиплікативну групу $\mathbb{Z}_m^*$ кільця $\mathbb{Z}_m$ класів лишків за модулем m. Визначити, чи є вона циклічною, якщо:

65.1. $m = 30$.
65.2. $m = 25$.
65.3. $m = 42$.
65.4. $m = 20$.
65.5. $m = 12$.
65.6. $m = 24$.
65.7. $m = 32$.
65.8. $m = 17$.
65.9. $m = 40$.
65.10. $m = 21$.
65.11. $m = 16$.
65.12. $m = 18$.
65.13. $m = 22$.
65.14. $m = 26$.
65.15. $m = 36$.
65.16. $m = 27$.
65.17. $m = 29$.
65.18. $m = 13$.
65.19. $m = 35$.
65.20. $m = 11$.
65.21. $m = 28$.
65.22. $m = 19$.
65.23. $m = 23$.
65.24. $m = 14$.
65.25. $m = 33$.

3. Суміжні класи групи за підгрупою

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай G – група, $H \leqslant G$. Для довільного $a \in G$ множина $aH = \{ah_1, ah_2, ...|h_1, h_2, ... \in H\}$ називається **лівостороннім суміжним класом** групи G за підгрупою H із представником a. Аналогічно, **правостороннім суміжним класом** групи G за підгрупою H із представником a називають множину $Ha = \{h_1a, h_2a, ...|h_1, h_2, ... \in H\}$.

Властивості лівосторонніх суміжних класів:

1°. Якщо $a \in H$, то $aH = H$.

2°. Суміжний клас aH групи G є підгрупою цієї групи тоді і лише тоді, коли $a \in H$.

3°. $|aH| = |Ha| = |H|$.

4°. Будь-який елемент суміжного класу можна взяти за його представник: якщо $b \in aH$, то $bH = aH$.

5°. Будь-які два суміжні класи aH і bH або збігаються, або не мають спільних елементів.

6°. Об'єднання всіх різних суміжних класів групи G за підгрупою H співпадає з групою G: $\bigcup\limits_{i \in I} a_iH = G$.

Властивості правосторонніх суміжних класів аналогічні.

Лівосторонні (правосторонні) суміжні класи групи G за підгрупою H утворюють розбиття групи G. **Лівостороннім розкладом** скінченної групи G за підгрупою H називається представлення групи G у вигляді: $G = x_1H \cup x_2H \cup ... \cup x_tH$, де $x_iH \cap x_jH = \varnothing$ при $i \neq j$. **Правостороннім розкладом** скінченної групи G за підгрупою H називається представлення групи G у вигляді: $G = Hy_1 \cup Hy_2 \cup ... \cup Hy_t$, де $Hy_i \cap Hy_j = \varnothing$ при $i \neq j$.

Теорема (Лагранжа)**.** *Порядок $|H|$ підгрупи H скінченної групи G є дільником порядку $|G|$ цієї групи.*

Наслідки:

1. Число правосторонніх і лівосторонніх суміжних класів групи G за підгрупою H однакове. Його називають **індексом** підгрупи H в групі G і позначають символом $|G : H|$
2. Якщо група G – скінченна, то $|H| \cdot |G : H| = |G|$.
3. Група G простого порядку є циклічною.
4. Порядок кожного елемента скінченної групи G є дільником порядку групи G.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 66.1. Знайти лівосторонній і правосторонній розклади на суміжні класи симетричної групи підстановок S_3 за її підгрупою $\langle a_3 \rangle$, де $a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Чи однакові ці розклади?

Розв'язання. Знайдемо спочатку підгрупу $H = \langle a_3 \rangle$. Маємо:

$$a_3^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = a_0.$$

Отже, $H = \langle a_3 \rangle = \{a_3, a_0\}$.

а) В якості першого лівостороннього суміжного класу можна взяти суміжний клас із представником a_0:

$$a_0 H = a_0\{a_3, a_0\} = \{a_3, a_0\} = H.$$

Візьмемо будь-який елемент із S_3, що не ввійшов до лівостороннього суміжного класу $a_0 H$, наприклад елемент a_1, і помножимо його на елементи підгрупи H:

$$a_1 H = a_1\{a_3, a_0\} = \{a_1 a_3, a_1 a_0\} = \{a_4, a_1\},$$

оскільки $a_1 a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = a_4$. Отримаємо другий лівосторонній суміжний клас $a_1 H = \{a_4, a_1\}$.

Далі знову візьмемо із групи S_3 елемент, що не ввійшов до жодного із двох побудованих вже лівосторонніх суміжних класів $a_0 H$ і $a_1 H$, наприклад елемент a_2. Отримаємо третій лівосторонній суміжний клас:

$$a_2 H = a_2\{a_3, a_0\} = \{a_2 a_3, a_2 a_0\} = \{a_5, a_2\},$$

оскільки $a_2 a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a_5$. Враховуючи те, що в побудовані класи ввійшли всі елементи групи (оскільки $H \cup a_1 H \cup a_2 H = \{a_3, a_0\} \cup \{a_4, a_1\} \cup \{a_5, a_2\} = S_3$) і ці класи попарно не перетинаються, розклад

$$S_3 = H \cup a_1 H \cup a_2 H$$

є лівостороннім розкладом групи S_3 за підгрупою H.

б) Знайдемо тепер правосторонній розклад групи S_3 за підгрупою H. Перший правосторонній суміжний клас – це суміжний клас із представником a_0:

$$H a_0 = \{a_3, a_0\} a_0 = \{a_3, a_0\} = H;$$

другий правосторонній суміжний клас – клас

$$H a_1 = \{a_3, a_0\} a_1 = \{a_3 a_1, a_0 a_1\} = \{a_5, a_1\},$$

оскільки $a_3 a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a_5.$

Далі беремо довільний елемент групи S_3, що не ввійшов до Ha_0 і Ha_1, наприклад елемент a_2. Отримаємо третій правосторонній суміжний клас:

$$Ha_2 = \{a_3, a_0\}a_2 = \{a_3a_2, a_0a_2\} = \{a_4, a_2\},$$

оскільки $a_3a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = a_4$. Оскільки ці класи попарно не перетинаються і $H \cup Ha_1 \cup Ha_2 = \{a_3, a_0\} \cup \{a_5, a_1\} \cup \{a_4, a_2\} = S_3$, то розклад

$$S_3 = H \cup Ha_1 \cup Ha_2$$

є правостороннім розкладом групи S_3 за підгрупою H.

в) Оскільки, наприклад, $a_1H = \{a_4, a_1\} \neq \{a_5, a_1\} = Ha_1$, то лівосторонній і правосторонній розклади групи S_3 за підгрупою H не однакові.

Розробка процедур. В Maple є команда **cosets(G,H)**, яка знаходить набір представників всіх різних правосторонніх суміжних класів групи G за підгрупою H. Однак для пошуку множини представників лівосторонніх суміжних класів окремої команди немає. Тому створимо відповідну процедуру. Зауважимо, що вона буде застосовна лише до груп підстановок.

Спочатку розглянемо алгоритм пошуку лівосторонніх суміжних класів.

I. Першим суміжним класом групи G за підгрупою H є сама підгрупа H (суміжний клас із представником e, де e – одиничний елемент групи G).

II. Наступним суміжним класом є клас a_1H, де $a_1 \in G \backslash H$.

III. Далі, суміжним класом є клас a_2H, де $a_2 \in (G \backslash H) \backslash a_1H$ і т.д. до a_sH (якщо кількість суміжних класів – скінченна) такий, що $((((G \backslash H) \backslash a_1H) \backslash a_2H) \backslash ...) \backslash a_sH = \varnothing$.

Реалізуємо даний алгоритм в Maple.

Оскільки результатом команди **permgroup**, за допомогою якої задаються групи підстановок G і H, є не множина елементів (дана команда лише перевіряє, чи існує група підстановок для введених аргументів, і декларує G і H як групи підстановок), то необхідно спочатку знайти множини EG і EH елементів груп G і H за допомогою команди **elements**:

```
> EG:=elements(G);
  EH:=elements(H);
```

До множини GS всіх представників лівосторонніх суміжних класів додаємо елемент – одиничну підстановку (представник класу H):

```
> FG:={[]};
```

Наступний представник шукаємо серед елементів множини $G\backslash H$:

```
> GS:=EG minus EH;
```

Тепер доти, доки в множині GS є елементи:

```
> while GS<>{} do ... end do;
```

поступово вибираємо довільний елемент із GS (команда **Generate(choose(GS))** із пакету **RandomTools**):

```
> a:=Generate(choose(GS));
```

додаємо його в якості представника суміжного класу до множини FG і вилучаємо із множини GS елементи класу $K = aH$:

```
> K:={};
  for i from 1 to nops(EH) do
      K:=K union {mulperms(a,EH[i])};
  end do;
  GS:=GS minus K;
```

Процедура матиме наступний код:

```
cosetsL:=proc(G,H)
local EG,EH,FG,GS,K,a,i;
uses group, RandomTools;
   EG:=elements(G);
   EH:=elements(H);
   FG:={[]};
   GS:=EG minus EH;
   while GS<>{} do
      a:=Generate(choose(GS));
      FG:=FG union {a};
      for i from 1 to nops(EH) do
         K:={}; K:=K union {mulperms(a,EH[i])};
      end do;
      GS:=GS minus K;
   end do;
   return(FG);
end proc:
```

Аналогічно можна створити процедуру пошуку представників правосторонніх суміжних класів групи підстановок:

```
cosetsR:=proc(G,H)
local EG,EH,FG,GS,K,a,i;
uses group, RandomTools;
   EG:=elements(G);
   EH:=elements(H);
   FG:={[]};
   GS:=EG minus EH;
   while GS<>{} do
      a:=Generate(choose(GS));
      FG:=FG union {a};
      for i from 1 to nops(EH) do
         K:={}; K:=K union {mulperms(EH[i],a)};
      end do;
      GS:=GS minus K;
   end do;
   return(FG);
end proc:
```

Розв'язання в Maple. Для відшукання лівостороннього розкладу використовуємо створену процедуру **cosetsL**. Зауважимо, що результат даної процедури не єдиний, оскільки в якості представника лівостороннього суміжного класу aH можна взяти будь-який елемент цього класу. Тому щоб побачити саме ті представники суміжних класів, які було знайдено аналітично, інколи треба декілька разів застосувати процедуру. Маємо:

```
> S3:=permgroup(3, {[[1,2]], [[1,2,3]]}):
  H:=permgroup(3, {[[1,2]]}):
  read(‘e:/atchlib.m‘); with(atchlib):
```

```
> cosetsL(S3,H);
```

$$\{[],\ [[2,\ 3]],\ [[1,\ 3,\ 2]]\}$$

```
> cosetsL(S3,H);
```

$$\{[],\ [[1,\ 2,\ 3]],\ [[1,\ 3,\ 2]]\}$$

```
> cosetsL(S3,H);
```

$$\{[],\ [[1,\ 3]],\ [[2,\ 3]]\}$$

Отримали бажаний результат: $S_3 = H \cup a_2H \cup a_1H$.

Правосторонній розклад групи S_3 можемо знаходити або за допомогою процедури **cosets** із пакету **group**, або за допомогою створеної процедури **cosetsR**:

```
> with(group):
  cosets(S3,H);
```

$$\{[],\ [[2,\ 3]],\ [[1,\ 2,\ 3]]\}$$

Оскільки $(23) = a_1$, $(123) = a_4$, то правосторонній розклад групи S_3 за

підгрупою H має вигляд:

$$S_3 = H \cup Ha_1 \cup Ha_4.$$

Враховуючи, що $a_4 \in Ha_2$, а значить, $Ha_4 = Ha_2$, даний результат збігається із отриманим аналітично. Команда **cosetsR** дає, в свою чергу, наступне:

```
> cosetsR(S3,H);
```

{[], [[1, 3]], [[1, 3, 2]]}

Отже, правосторонній розклад на суміжні класи групи S_3 за підгрупою H має вигляд: $S_3 = H \cup Ha_2 \cup Ha_5$. Оскільки $a_5 \in Ha_1$, то $Ha_5 = Ha_1$, і отриманий результат збігається із розв'язком, отриманим вище.

Приклад 66.2. Знайти лівосторонній і правосторонній розклади на суміжні класи циклічної групи $G = \langle b \rangle$ порядку 20 за її підгрупою $H = \langle b^8 \rangle$.

Розв'язання. Оскільки група G – комутативна, то кожний її лівосторонній суміжний клас xH співпадає із відповідним правостороннім суміжним класом Hx, $x \in G$, а значить, співпадають лівосторонній і правосторонній розклади групи G за підгрупою H.

Спосіб I. Одним із суміжних класів є сама підгрупа $H = \langle b^8 \rangle = \{b^8, b^{16}, b^4, e\} = \{e, b^4, b^8, b^{12}, b^{16}\}$, де e – одиничний елемент групи G.

Візьмемо будь-який елемент із G, що не ввійшов до суміжного класу H, наприклад елемент b, і помножимо його на елементи підгрупи H:

$$bH = b\{e, b^4, b^8, b^{12}, b^{16}\} = \{b, b^5, b^9, b^{13}, b^{17}\}.$$

Отримали другий суміжний клас.

Далі знову візьмемо із групи G елемент, що не ввійшов до жодного із двох побудованих вже суміжних класів H і bH, наприклад елемент b^2. Отримаємо третій суміжний клас:

$$b^2H = b^2\{e, b^4, b^8, b^{12}, b^{16}\} = \{b^2, b^6, b^{10}, b^{14}, b^{18}\}.$$

В групі G ще залишились елементи, які не ввійшли до жодного із побудованих вище класів. Вибираємо будь-який із них, наприклад b^3. Отримуємо наступний суміжний клас.

$$b^3H = b^3\{e, b^4, b^8, b^{12}, b^{16}\} = \{b^3, b^7, b^{11}, b^{15}, b^{19}\}.$$

Оскільки в класи H, bH, b^2H, b^3H ввійшли всі елементи групи, тобто

$$H \cup bH \cup b^2H \cup b^3H = \{e, b^4, b^8, b^{12}, b^{16}\} \cup \{b, b^5, b^9, b^{13}, b^{17}\} \cup \\ \cup \{b^2, b^6, b^{10}, b^{14}, b^{18}\} \cup \{b^3, b^7, b^{11}, b^{15}, b^{19}\} = G,$$

і ці класи попарно не перетинаються, то розклад

$$G = H \cup bH \cup b^2H \cup b^3H$$

є розкладом на суміжні класи групи G за підгрупою H.

Спосіб II.

Перш за все відмітимо, що $|H| = 5$, значить, $H = \langle b^4 \rangle$ (властивість 4.2 попереднього пункту). За наслідком із теореми Лагранжа, $[G : H] = 4$, тобто різних суміжних класів є 4. Нехай b^s – довільний елемент групи G, $s \in \overline{0, 19}$. Знайдемо суміжний клас $\overline{b^s} = b^sH$, представником якого є b^s.

За теоремою про ділення з остачею існує, причому єдина, пара цілих чисел q і r таких, що $s = 4q + r$, де $r = 0, 1, 2, 3$. Тоді

$$b^sH = b^s\langle b^4 \rangle = b^{4q+r}\langle b^4 \rangle = b^{4q} \cdot b^r \cdot \langle b^4 \rangle = b^r \cdot b^{4q} \cdot \langle b^4 \rangle = b^r \cdot \langle b^4 \rangle = b^rH,$$

де $r \in \{0, 1, 2, 3\}$. Отже, всього є 4 суміжних класів групи G за підгрупою H, а саме:

$$b^0H = H = \langle b^4 \rangle = \{b^{4k} | k \in \mathbb{Z}\};$$
$$b^1H = b\{b^{4k} | k \in \mathbb{Z}\} = \{b^{4k+1} | k \in \mathbb{Z}\};$$
$$b^2H = b^2\{b^{4k} | k \in \mathbb{Z}\} = \{b^{4k+2} | k \in \mathbb{Z}\};$$
$$b^3H = b^3\{b^{4k} | k \in \mathbb{Z}\} = \{b^{4k+3} | k \in \mathbb{Z}\}.$$

Ці класи попарно не перетинаються і

$$G = H \cup bH \cup b^2H \cup b^3H, \tag{VII.4}$$

отже, розклад (VII.4) є розкладом на суміжні класи групи G за підгрупою H.

Розв'язання в Maple. Як було сказано при розв'язанні Прикладу 63.1, циклічну групу $G = \langle b \rangle$ порядку n можна задати за допомогою твірного елемента і визначального співвідношення $b^n = e$. В Maple для задання групи G за допомогою твірних елементів і визначальних співвідношень використовується команда **grelgroup(gens, rels)**, де gens – множина твірних елементів, rels – множина визначальних співвідношень. Визначальне

співвідношення записують у вигляді списку, елементами якого є елементи множини gens. Запис $[a_1, a_2, a_3, ..., a_k]$ означає, що $a_1a_2a_3...a_k = e$, де e – одиничний елемент групи G. Якщо у визначальному співвідношенні зустрічається елемент, обернений до деякого твірного g, його позначають $1/g$. Для запису натурального степеня g^l елемента цей елемент повторюють l разів [g, g, ..., g], або пишуть [g$l].

Задаємо групу $G = \langle b \rangle$, де $b^{20} = e$:

```
> with(group):
  G:=grelgroup({b}, {[b$20]}):
```

Підгрупа H групи G задається за допомогою команди **subgrel(gensH, G)**, де gensH – множина твірних елементів підгрупи H. Відмітимо, що множину твірних елементів підгрупи підгрупи необхідно записувати у вигляді {символ=[твірний елемент]}:

```
> H:=subgrel({x=[b$8]}, G):
```

Оскільки група G – комутативна (а значить, лівосторонній і правосторонній розклади на суміжні класи збігаються), то для відшукання розкладу групи G можемо використати команду **cosets** із пакету **group**.

```
> cosets(H);
```

$$\{[], [b], [b, b], [b, b, b]\}$$

Це означає, що розклад групи G за підгрупою H має вигляд:

$$G = H \cup bH \cup b^2H \cup b^3H.$$

Завдання 66. Знайти розклад(и) на суміжні класи:

66.1. знакозмінної групи підстановок A_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

66.2. симетричної групи підстановок S_3 за її підгрупою $\langle a_1 \rangle$, де $a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

66.3. циклічної групи 8-го порядку за її підгрупою 4-го порядку.

66.4. мультиплікативної групи коренів 6-го степеня з одиниці за її підгрупою коренів 2-го степеня з одиниці.

66.5. симетричної групи підстановок S_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

66.6. циклічної групи $G = \langle a \rangle$ порядку 10 за її підгрупою $H = \langle a^4 \rangle$.

66.7. мультиплікативної групи коренів 12-го степеня з одиниці за її підгрупою коренів 3-го степеня з одиниці.

66.8. циклічної групи $G = \langle a \rangle$ порядку 18 за її підгрупою $H = \langle a^8 \rangle$.

66.9. мультиплікативної групи коренів 12-го степеня з одиниці за її підгрупою коренів 4-го степеня з одиниці.

66.10. циклічної групи 25-го порядку за її підгрупою 5-го порядку.

66.11. симетричної групи підстановок S_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$.

66.12. знакозмінної групи підстановок A_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

66.13. циклічної групи порядку 14 за всіма її підгрупами.

66.14. симетричної групи підстановок S_3 за її підгрупою $\langle a_5 \rangle$, де $a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

66.15. знакозмінної групи підстановок A_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

66.16. циклічної групи $G = \langle a \rangle$ порядку 15 за її підгрупою $H = \langle a^9 \rangle$.

66.17. мультиплікативної групи коренів 10-го степеня з одиниці за її підгрупою коренів квадратних з одиниці.

66.18. симетричної групи підстановок S_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$.

66.19. знакозмінної групи підстановок A_4 за її підгрупою $\langle a \rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

66.20. циклічної групи 16-го порядку за її підгрупою 4-го порядку.

66.21. симетричної групи підстановок S_4 за її підгрупою $\langle a\rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

66.22. циклічної групи порядку 9 за всіма її підгрупами.

66.23. знакозмінної групи підстановок A_4 за її підгрупою $\langle a\rangle$, де $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

66.24. циклічної групи $G = \langle a\rangle$ порядку 20 за її підгрупою порядку 5.

66.25. симетричної групи підстановок S_3 за її підгрупою $\langle a_2\rangle$, де $a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

4. Нормальні підгрупи. Фактор-група

ТЕОРЕТИЧНІ ВІДОМОСТІ

Означення. Підгрупа H групи G називається нормальною підгрупою (або нормальним дільником) групи G (пишуть: $H \trianglelefteq G$), якщо для будь-якого елемента x із G лівосторонній суміжний клас xH збігається із правостороннім суміжним класом Hx: $xH = Hx$.

Теорема (критерій нормальної підгрупи)**.** *Непорожня підмножина H групи $\langle G; \cdot\rangle$ є нормальною підгрупою групи G тоді і лише тоді, коли виконуються умови:*

1) для довільних $a, b \in H$ справедливо, що $ab \in H$;
2) для довільного $a \in H$ обернений до нього в G елемент a^{-1} належить до H;
3) для довільних $a \in H$ і $x \in G$ справедливо, що $x^{-1}ax \in H$.

Елемент $x^{-1}ax$ називається **спряженим** до елемента a за допомогою елемента $x \in G$. Умову 3) критерію нормальної підгрупи можна сформулювати наступним чином: множина H разом із кожним своїм елементом a містить всі до нього спряжені елементи $x^{-1}ax$, де $x \in G$.

Якщо H – підгрупа групи G індексу 2, то $H \triangleleft G$. Перетин довільного числа нормальних підгруп групи G є нормальною підгрупою цієї групи.

Нехай x – довільний елемент групи G, $H \trianglelefteq G$. Суміжний клас xH позначимо $\overline{x}$. Множина $G/H = \overline{G} = \left\{\overline{x}, \overline{y}, \overline{z}, ...\right\}$ всіх різних суміжних класів групи G за підгрупою H відносно операції множення: $\overline{x} \cdot \overline{y} = \overline{xy}$ для довільних $\overline{x}, \overline{y} \in \overline{G}$ утворює групу. Її називають **фактор-групою** групи G за нормальною підгрупою H.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 67.1. Визначити, чи є нормальною підгрупою симетричної групи підстановок S_3 підгрупа $H = \langle a_2 \rangle$, де $a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Розв'язання. Спосіб I. Використаємо означення нормальної підгрупи. Покажемо, що існує елемент x із S_3 такий, що $xH \neq Hx$.

Знайдемо a_4H і Ha_4:

$$a_4H = a_4\langle a_2 \rangle = a_4\{a_2, a_0\} = \{a_4a_2, a_4a_0\} = \{a_3, a_4\},$$
$$Ha_4 = \langle a_2 \rangle a_4 = \{a_2, a_0\}a_4 = \{a_2a_4, a_0a_4\} = \{a_1, a_4\}.$$

Оскільки $\{a_3, a_4\} \neq \{a_1, a_4\}$, то $a_4H \neq Ha_4$. Отже, $H \not\trianglelefteq S_3$.

Спосіб II. Використаємо критерій нормальної підгрупи. Маємо: $H = \langle a_2 \rangle = \{a_2, a_0\}$; помічаємо, що $a_2 \in H$, але $a_4^{-1}a_2a_4 = a_3 \notin H$. Отже, підгрупа H разом із своїм елементом a_2 не містить спряжений до нього елемент $a_4^{-1}a_2a_4$. Не виконується умова 3) критерію нормальної підгрупи, тому $H \not\trianglelefteq S_3$.

Розробка процедур. Створимо процедуру для перевірки умови 3) критерію нормальної підгрупи. Щоб дану процедуру можна було використовувати для довільних груп, в якості параметрів введемо не групи G і H, а множини елементів цих груп setG і setH.

Нехай $t = |H|$, $m = |G|$:

```
> t:=nops(setH);
  m:=nops(setG);
```

Для кожного із m елементів $x = setG[i]$ групи G знаходимо симетричний до нього в G елемент $xsym = symElement(x)$, де symElement – це правило відшукання симетричного елемента (яке користувач задає в якості параметра) і розглядаємо всі можливі добутки $conj = xsym \cdot a_j \cdot x$:

```
> for i from 1 to m do
     x:=setG[i];
     xsym:=symElement(x);
     for j from 1 to t do
       a:=setH[j];
       conj:=operation(operation(xsym,a),x);
  ... end do; end do;
```

Якщо елемент conj належить до H, то збільшуємо лічильник s на одиницю:

```
> if member(conj,setH)=true then s:=s+1; else break; end if;
```

і переходимо до дослідження наступного добутку $xsym \cdot a_j \cdot x = conj$. Якщо всі спряжені елементи conj містяться в H, то в результаті виконання циклу лічильник s має набути значення mt. Тому перевіряємо, чи виконується умова $s = mt$:

```
> evalb(s=m*t);
```

Процедура матиме наступний код:

```
belongsConj:=proc(setH,setG,operation,symElement)
local i,s,t,m,j,x,xsym,conj,a;
   t:=nops(setH);
   m:=nops(setG);
   s:=0;
   for i from 1 to m do
      x:=setG[i];
      xsym:=symElement(x);
      for j from 1 to t do
         a:=setH[j]; conj:=operation(operation(xsym,a),x);
         if member(conj,setH)=true then s:=s+1; else break; end if;
      end do;
   end do;
   evalb(s=m*t);
end proc:
```

Розв'язання в Maple. В пакеті **group** є команда **isnormal**, за допомогою якої визначають, чи є деяка множина H нормальною підгрупою заданої групи G. Формат **isnormal(G,H)** даної команди використовується для групи підстановок G; в цьому випадку визначається, чи є множина H нормальною підгрупою групи HG (зверніть увагу: не групи G! тому спершу необхідно перевірити, чи є взагалі H підгрупою групи G). Для групи G, заданої за допомогою твірних елементів і визначальних співвідношень, команда має формат **isnormal(H)**; в такому випадку визначається, чи є задана множина H нормальною підгрупою групи G

Задаємо групу S_3 та групу H:

```
> with(group):
  S3:=permgroup(3, {[[1,2]], [[1,2,3]]}):
  H:=permgroup(3, {[[1,3]]}):
```

Визначаємо, чи є H підгрупою групи S_3:

```
> issubgroup(H,S3);
```

$$true$$

Отже, $H \leqslant S_3$.

```
> isnormal(S3,H);
```

false

Таким чином, $H \not\trianglelefteq S_3$.

Покрокова перевірка аналітичного розв'язання матиме наступний вигляд. Спочатку перевіряємо, чи є множина H (позначено через setH) підмножиною множини S_3 (setS3):

```
> setS3:=elements(S3);
```

$$setS3 := \{[], [[1, 2]], [[1, 3]], [[2, 3]], [[1, 2, 3]], [[1, 3, 2]]\}$$

```
> setH:=elements(H);
```

$$setH := \{[], [[1, 3]]\}$$

```
> setH subset setS3;
```

true

Отже, $H \subseteq S_3$. Далі перевіряємо умови 1)-3) критерію нормальної підгрупи. Умову 1) перевіряємо за допомогою процедури **isClosed**, створеної при розв'язанні Прикладу 21.1:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> isClosed(setH, mulperms);
```

true

Отже, умова 1) критерію нормальної підгрупи виконується.

Для перевірки умови 2) критерію використовуємо процедуру **belongsSym**, створену при розв'язанні Прикладу 24.1. Відмітимо, що в якості першого параметра даної процедури має виступати множина елементів групи, а не сама група!

У випадку групи підстановок G елемент, симетричний до елемента $a \in G$, – це обернена підстановка **invperm(a)**.

```
> belongsSym(setH,invperm);
```

true

Таким чином, разом із кожним своїм елементом $setH[i]$ множина H містить і обернений до нього елемент.

Для перевірки умови 3) критерію використовуємо створену процедуру:

```
> belongsConj(setH,setS3,mulperms,invperm);
```

false

Отже, умова 3) критерію нормальної підгрупи не виконується, $H \not\trianglelefteq S_3$.

Приклад 67.2. Визначити, чи є множина $\mathfrak{M}$ матриць 2-го порядку над полем $\mathbb{Z}_5$, визначник кожної з яких рівний $\overline{1}$, нормальною підгрупою мульти-

плікативної групи $GL_2(\mathbb{Z}_5)$ невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$.

Розв'язання. а) Покажемо спочатку, що $\mathfrak{M}$ є підгрупою групи $GL_2(\mathbb{Z}_5)$. Очевидно, $\varnothing \neq \mathfrak{M} \subseteq GL_2(\mathbb{Z}_5)$. Використаємо критерій нормальної підгрупи.

1) Нехай A, B – довільні два елементи із $\mathfrak{M}$. Тоді $|A| = |B| = \overline{1}$. Знайдемо визначник $|AB|$ добутку матриць A і B: $|AB| = |A||B| = \overline{1}$, значить, $AB \in \mathfrak{M}$.

2) Для довільної матриці A із $\mathfrak{M}$ визначник оберненої до неї в $GL_2(\mathbb{Q})$ матриці A^{-1} дорівнює теж $\overline{1}$ (дійсно, $|A^{-1}| = \frac{\overline{1}}{|A|} = \frac{\overline{1}}{\overline{1}} = \overline{1}$), а значить, $A^{-1} \in \mathfrak{M}$.

3) Нехай A – довільний елемент із $\mathfrak{M}$. Тоді для довільного $X \in GL_2(\mathbb{Z}_5)$

$$|X^{-1}AX| = |X^{-1}||A||X| = \frac{1}{|X|}|A||X| = |A| = \overline{1},$$

значить, $X^{-1}AX \in \mathfrak{M}$. Отже, підгрупа $\mathfrak{M}$ разом із кожним своїм елементом A містить і кожний спряжений до нього елемент $X^{-1}AX$.

В силу критерію нормальної підгрупи, $\mathfrak{M} \trianglelefteq GL_2(\mathbb{Z}_5)$.

Розв'язання в Maple. Задаємо множину $GL_2(\mathbb{Z}_5)$ в наступний спосіб: серед множини T всіх матриць над полем $\mathbb{Z}_5$ вибираємо (функція **select**) ті матриці A, визначник яких відмінний від $\overline{0}$:

```
> T:={seq(seq(seq(seq([[x,y],[z,t]],x=0..4),y=0..4),z=0..4),t=0..4)}:
> GL2:=select(A->evalb(A[1,1]*A[2,2]-A[1,2]*A[2,1] mod 5<>0),T):
```

і аналогічно задаємо множину $H = \mathfrak{M}$ (вибираючи матриці, визначник яких дорівнює $\overline{1}$):

```
> H:=select(A->evalb(A[1,1]*A[2,2]-A[1,2]*A[2,1] mod 5=1),T):
```

Далі задаємо групову операцію (операцію множення матриць):

```
> mmult:=(A,B)->[[A[1,1]*B[1,1]+A[1,2]*B[2,1] mod 5,
                  A[1,1]*B[1,2]+A[1,2]*B[2,2] mod 5],
                 [A[2,1]*B[1,1]+A[2,2]*B[2,1] mod 5,
                  A[2,1]*B[1,2]+A[2,2]*B[2,2] mod 5]]:
```

і діємо за алгоритмом розв'язання Прикладу 67.1. Перевіряємо, чи є множина H підмножиною множини $GL_2(\mathbb{Z}_5)$.

```
> H subset GL2;
```

true

Отже, $H \subseteq GL_2(\mathbb{Z}_5)$. Далі перевіряємо, чи виконуються умови 1)-3) критерію нормальної підгрупи.

```
> isClosed(H,mmult);
```

true

Операція множення матриць замкнена на H.

Задаємо правило invmatr для відшукання матриці A^{-1}, оберненої до матриці $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Матриця A^{-1} має вигляд: $A^{-1} = \begin{pmatrix} \frac{a_{22}}{a_{11}a_{22}-a_{21}a_{12}} & -\frac{a_{12}}{a_{11}a_{22}-a_{21}a_{12}} \\ -\frac{a_{21}}{a_{11}a_{22}-a_{21}a_{12}} & \frac{a_{11}}{a_{11}a_{22}-a_{21}a_{12}} \end{pmatrix}$:

```
> invmatr:=A->[[A[2,2]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5,
               -A[1,2]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5],
               [-A[2,1]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5,
                A[1,1]/(A[1,1]*A[2,2]-A[2,1]*A[1,2]) mod 5]]:
```

і перевіряємо, чи для кожного елемента $A \in H$ обернений до нього в $GL_2(\mathbb{Z}_5)$ належить до H:

```
> belongsSym(H,invmatr);
```

true

Таким чином, умова 2) виконується. Залишається перевірити, чи містить множина H разом із елементом A і кожний спряжений до нього:

```
> belongsConj(H,GL2,mmult,invmatr);
```

true

Умова 3) також виконується. В силу критерію нормальної підгрупи, $H \trianglelefteq GL_2(\mathbb{Z}_5)$.

Завдання 67. Визначити, чи є підмножина H групи G її нормальною підгрупою, якщо:

67.1. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – множина матриць виду $\begin{pmatrix} a & b \\ \overline{0} & c \end{pmatrix}$, де $a, b, c \in \mathbb{Z}_5$, $ac \neq \overline{0}$.

67.2. G – симетрична група підстановок S_4;
$H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$.

67.3. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;

H – множина матриць виду $\begin{pmatrix} a & \overline{0} \\ b & \overline{1} \end{pmatrix}$, $a, b, c \in \mathbb{Z}_5$, $a \neq \overline{0}$.

67.4. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – множина всіх матриць із G, визначник яких дорівнює $\overline{4}$.

67.5. G – група трійок (a, b, ε), де $a, b \in \mathbb{Z}_5$, $\varepsilon \in \{\overline{1}, \overline{4}\}$, відносно операції $*$, заданої рівністю: $(a_1, b_1, \varepsilon_1) * (a_2, b_2, \varepsilon_2) = (a_1 + a_2, b_1 + b_2, \varepsilon_1\varepsilon_2)$;
H – циклічна підгрупа, породжена елементом $(\overline{1}, \overline{0}, \overline{1})$.

67.6. G – мультиплікативна група матриць виду $\begin{pmatrix} a & b \\ \overline{0} & c \end{pmatrix}$, a,b,$c \in \mathbb{Z}_7$, $ac \neq \overline{0}$;
H – множина всіх матриць виду $\begin{pmatrix} \overline{1} & m \\ 0 & \overline{1} \end{pmatrix}$, де $m \in \mathbb{Z}_7$.

67.7. $G = GL_2(\mathbb{Z}_7)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_7$;
H – множина всіх матриць із G, визначник яких дорівнює $\overline{2}$.

67.8. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$ комплексних чисел;
H – множина матриць A із G таких, що $A \cdot A^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, де A^T – матриця, транспонована до матриці A.

67.9. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 3-го порядку над полем $\mathbb{Z}_5$;
H – множина матриць $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}_5$, таких, що $a^2 + b^2 = c^2 + d^2 = \overline{1}$, $ac + bd = \overline{0}$.

67.10. G – симетрична група підстановок S_4;
H – симетрична група підстановок S_3.

67.11. G – група пар (a, ε), де $a \in \mathbb{Z}_7^*$, $\varepsilon = \pm 1$, відносно операції $*$, заданої рівністю: $(a_1, \varepsilon_1) * (a_2, \varepsilon_2) = (a_1^{\varepsilon_2} a_2, \varepsilon_1\varepsilon_2)$;
H – множина всіх пар виду $(h, 1)$, де $h \in \mathbb{Z}_7^*$.

67.12. G – симетрична група підстановок S_4;
$H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \right\}$.

67.13. $G = SL_2(\mathbb{Z}_7)$ – мультиплікативна група невироджених матриць 2-го порядку із визначником рівним 1 над полем $\mathbb{Z}_7$;
H – множина всіх матриць виду $\begin{pmatrix} \overline{1} & 0 \\ x & \overline{1} \end{pmatrix}$, де $x, y, z \in \mathbb{Z}_7$.

67.14. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – множина всіх матриць із G, визначник яких дорівнює $\overline{3}$.

67.15. G – група пар (a, b), де $a, b \in \mathbb{Z}_7$, відносно операції $*$, заданої рівністю: $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, a_2 b_1 + b_2)$;
H – множина всіх пар виду $(\overline{0}, c)$, де $c \in \mathbb{Z}_7$.

67.16. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – циклічна підгрупа, породжена елементом $\begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix}$.

67.17. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – множина матриць виду $\begin{pmatrix} a & \overline{0} \\ \overline{0} & b \end{pmatrix}$, де $a, b \in \mathbb{Z}_5$, $ab \neq \overline{0}$.

67.18. G – симетрична група підстановок S_4;
$H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \right\}$.

67.19. G – група пар (a, b), де $a, b \in \mathbb{Z}_5$, $a \neq \overline{0}$, відносно операції $*$, заданої рівністю: $(a, b) * (c, d) = (ac, bd + c)$;
$H = \{(k, \overline{1}) | k \in \mathbb{Z}_7, k \neq \overline{0}\}$.

67.20. $G = GL_2(\mathbb{Z}_7)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_7$;
H – циклічна підгрупа, породжена елементом $\begin{pmatrix} \overline{1} & \overline{5} \\ \overline{0} & \overline{6} \end{pmatrix}$.

67.21. G – симетрична група підстановок S_4;
H – знакозмінна група підстановок A_3.

67.22. $G = GL_2(\mathbb{Z}_5)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – множина всіх матриць із G, визначник яких відмінний від $\overline{1}$.

67.23. G – група трійок (a, b, c), де $a, b, c \in \mathbb{Z}_4$, відносно операції $*$, заданої рівністю: $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$;
H – множина всіх трійок виду $(k, \overline{0}, \overline{0})$, де $k \in \mathbb{Z}_4$.

67.24. $G = GL_2(\mathbb{Z}_7)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_7$;
H – множина всіх нескалярних матриць із G.

67.25. $G = GL_2(\mathbb{Z}_3)$ – мультиплікативна група невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$;
H – множина всіх матриць виду $\begin{pmatrix} a & \overline{0} \\ \overline{0} & b \end{pmatrix}$, де $a, b \in \mathbb{Z}_5$, $ab \neq \overline{0}$, $a+b = \overline{0}$.

Приклад 68.1. Побудувати фактор-групу G/H циклічної групи G 20-го порядку за її підгрупою H 5-го порядку.

Розв'язання. Суміжні класи групи G за підгрупою H було знайдено при розв'язанні Прикладу 66.2. Ними є: $\overline{e} = eH = H$, $\overline{a} = aH$, $\overline{a^2} = a^2H$, $\overline{a^3} = a^3H$. Фактор-група G/H має вигляд: $G/H = \{\overline{a^0}, \overline{a}, \overline{a^2}, \overline{a^3}\}$.

Операція множення $\cdot$ на множині G/H задається наступним чином: для довільних $\overline{a}, \overline{b} \in G/H$

$$\overline{a} \cdot \overline{b} = \overline{ab},$$

в даному випадку матимемо: для довільних $\overline{a^s}, \overline{a^t} \in G/H$

$$\overline{a^s} \cdot \overline{a^t} = \overline{a^s a^t} = \overline{a^{s+t}} = \overline{a^{s+t \pmod 4}}.$$

Побудуємо таблицю Келі для даної операції:

	$\overline{a^0}$	$\overline{a^1}$	$\overline{a^2}$	$\overline{a^3}$
$\overline{a^0}$	$\overline{a^0}$	$\overline{a^1}$	$\overline{a^2}$	$\overline{a^3}$
$\overline{a^1}$	$\overline{a^1}$	$\overline{a^2}$	$\overline{a^3}$	$\overline{a^0}$
$\overline{a^2}$	$\overline{a^2}$	$\overline{a^3}$	$\overline{a^0}$	$\overline{a^1}$
$\overline{a^3}$	$\overline{a^3}$	$\overline{a^0}$	$\overline{a^1}$	$\overline{a^2}$

Розв'язання в Maple. Для побудови таблиці Келі використовуємо процедуру **cayleyTable**, створену при розв'язанні Прикладу 27.1. Задаємо фактор-групу G/H:

```
> FG:={a^0, a, a^2, a^3};
```

$$FG := \{1,\, a,\, a^2,\, a^3\}$$

і операцію mult множення елементів фактор-групи:

```
> mult:=(x,y)->a^(degree(x,a)+degree(y,a) mod 4):
```

(Елементам x і y ставимо у відповідність елемент $a^{\deg x+\deg y \pmod 4}$.)

Будуємо таблицю Келі:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> cayleyTable(FG,mult);
```

$$\begin{bmatrix} 1 & a & a^2 & a^3 \\ a & a^2 & a^3 & 1 \\ a^2 & a^3 & 1 & a \\ a^3 & 1 & a & a^2 \end{bmatrix}$$

Приклад 68.2. Побудувати фактор-групу K/H мультиплікативної групи K коренів 15-го степеня з одиниці за її підгрупою коренів 5-го степеня з одиниці. Скласти таблицю Келі для K/H.

Розв'язання. Нехай

$$K = \langle \varepsilon_1 \rangle = \left\{ \varepsilon_0, \varepsilon_1, \varepsilon_1^2, ..., \varepsilon_1^{14} \right\},\ \text{де}\ \varepsilon_1 = \cos\frac{2\pi}{15} + i\sin\frac{2\pi}{15}.$$

Тоді $\left|\varepsilon_1^3\right| = 5$, значить, $\left|\left\langle \varepsilon_1^3 \right\rangle\right| = 5$ і $H = \left\langle \varepsilon_1^3 \right\rangle = \left\{ \varepsilon_1^3, \varepsilon_1^6, \varepsilon_1^9, \varepsilon_1^{12}, \varepsilon_0 \right\}$. Знайдемо суміжні класи групи K за підгрупою H. З теореми Лагранжа випливає, що всього суміжних класів є $|K : H| = \frac{|K|}{|H|} = \frac{15}{5} = 3$. Одним із суміжних класів є сама підгрупа $H = \left\langle \varepsilon_1^3 \right\rangle$.

Нехай ε_1^k, $k = 0, 1, \ldots, 14$, – довільний елемент із K. Знайдемо суміжний клас $\overline{\varepsilon_1^k} = \varepsilon_1^k H$, представником якого є ε_1^k. Поділимо число k з остачею на 3. Маємо: $k = 3q + r$, де $r = 0, 1, 2$. Тоді

$$\overline{\varepsilon_1^k} = \varepsilon_1^k \left\langle \varepsilon_1^3 \right\rangle = \varepsilon_1^{3q+r} \left\langle \varepsilon_1^3 \right\rangle = \varepsilon_1^{3q} \cdot \varepsilon_1^r \cdot \left\langle \varepsilon_1^3 \right\rangle = \varepsilon_1^r \cdot \varepsilon_1^{3q} \cdot \left\langle \varepsilon_1^3 \right\rangle = \varepsilon_1^r \cdot \left\langle \varepsilon_1^3 \right\rangle = \overline{\varepsilon_1^r},$$

де $r = 0, 1, 2$. Отже, суміжними класами групи за підгрупою є:

$$\overline{\varepsilon_1^0} = \varepsilon_1^0 \cdot \left\langle \varepsilon_1^3 \right\rangle = \left\{ \varepsilon_0, \varepsilon_1^3, \varepsilon_1^6, \varepsilon_1^9, \varepsilon_1^{12} \right\};$$
$$\overline{\varepsilon_1^1} = \varepsilon_1^1 \cdot \left\langle \varepsilon_1^3 \right\rangle = \varepsilon_1^1 \cdot \left\{ \varepsilon_0, \varepsilon_1^3, \varepsilon_1^6, \varepsilon_1^9, \varepsilon_1^{12} \right\} = \left\{ \varepsilon_1^1, \varepsilon_1^4, \varepsilon_1^7, \varepsilon_1^{10}, \varepsilon_1^{13} \right\};$$
$$\overline{\varepsilon_1^2} = \varepsilon_1^2 \cdot \left\langle \varepsilon_1^3 \right\rangle = \varepsilon_1^2 \cdot \left\{ \varepsilon_0, \varepsilon_1^3, \varepsilon_1^6, \varepsilon_1^9, \varepsilon_1^{12} \right\} = \left\{ \varepsilon_1^2, \varepsilon_1^5, \varepsilon_1^8, \varepsilon_1^{11}, \varepsilon_1^{14} \right\}.$$

Фактор-група K/H має вигляд: $K/H = \left\{ \overline{\varepsilon_0}, \overline{\varepsilon_1}, \overline{\varepsilon_1^2} \right\}$.

Складемо таблицю Келі (пам'ятаючи, що операція множення суміжних класів $\overline{\varepsilon_1^i}$ зводиться до операції множення їхніх представників ε_1^i, $i = 0, 1, 2$):

	$\overline{\varepsilon_0}$	$\overline{\varepsilon_1}$	$\overline{\varepsilon_1^2}$
$\overline{\varepsilon_0}$	$\overline{\varepsilon_0}$	$\overline{\varepsilon_1}$	$\overline{\varepsilon_1^2}$
$\overline{\varepsilon_1}$	$\overline{\varepsilon_1}$	$\overline{\varepsilon_1^2}$	$\overline{\varepsilon_0}$
$\overline{\varepsilon_1^2}$	$\overline{\varepsilon_1^2}$	$\overline{\varepsilon_0}$	$\overline{\varepsilon_1}$

Розв'язання в Maple. Спочатку знаходимо суміжні класи групи K за підгрупою H за допомогою команди **cosets** (див. Приклад 66.2):

```
> with(group):
  K:=grelgroup({epsilon},{[epsilon$15]}):
> H:=subgrel({x=[epsilon$3]},K):
> cosets(H);
```

$$\{[], [\varepsilon], [\varepsilon, \varepsilon]\}$$

Отже, $K/H = \left\{\overline{\varepsilon_0}, \overline{\varepsilon_1}, \overline{\varepsilon_1^2}\right\}$. Щоб простіше було задавати операцію, запишемо фактор-групу K/H в іншому вигляді:

```
> FG:={seq(epsilon^i,i=0..2)};
```

$$FG := \{1, \varepsilon, \varepsilon^2\}$$

Операція множення суміжних класів матиме вигляд:

```
> mult:=(x,y)->
    epsilon^(degree(x,epsilon)+degree(y,epsilon) mod 3):
```

Застосовуємо процедуру **cayleyTable**:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> cayleyTable(FG,mult);
```

$$\begin{bmatrix} 1 & \varepsilon & \varepsilon^2 \\ \varepsilon & \varepsilon^2 & 1 \\ \varepsilon^2 & 1 & \varepsilon \end{bmatrix}$$

Приклад 68.3. Побудувати фактор-групу адитивної групи $\mathbb{Z}_{30}$ за її підгрупою $H = \langle\overline{3}\rangle$. Побудувати таблицю Келі для даної фактор-групи.

Розв'язання. Знаходимо підгрупу: $H = \langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}$. Порядок підгрупи H дорівнює 10. Тому порядок шуканої фактор-групи $\mathbb{Z}_{30}/H$ дорівнює $|\mathbb{Z}_{30} : H| = \frac{|\mathbb{Z}_{30}|}{|H|} = \frac{30}{10} = 3$.

В якості першого суміжного класу беремо саму підгрупу $H = \overline{0} + H$. Представником наступного суміжного класу виберемо довільний елемент, який не ввійшов у перший суміжний клас, наприклад $\overline{1}$. Отримаємо суміжний клас

$$\overline{1}+H = \overline{1}+\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12},\overline{15},\overline{18},\overline{21},\overline{24},\overline{27}\} = \{\overline{1},\overline{4},\overline{7},\overline{10},\overline{13},\overline{16},\overline{19},\overline{22},\overline{25},\overline{28}\}.$$

До третього суміжного класу ввійдуть всі елементи групи, які не ввійшли до класів H та $1 + H$; його утворюємо за допомогою елемента $\overline{2}$:

$$\overline{2}+H = \overline{2}+\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12},\overline{15},\overline{18},\overline{21},\overline{24},\overline{27}\} = \{\overline{2},\overline{5},\overline{8},\overline{11},\overline{14},\overline{17},\overline{20},\overline{23},\overline{26},\overline{29}\}.$$

Таким чином, $\mathbb{Z}_{30}/H = \{H, \overline{1}+H, \overline{2}+H\}$. Операція для елементів групи $\mathbb{Z}_{30}/H$ задається наступним чином: для довільних $a + H, b + H \in \mathbb{Z}_{30}/H$ справедливо: $(a+H)+(b+H) = (a+b)+H$. Побудуємо таблицю Келі для даної операції:

	H	$\overline{1}+H$	$\overline{2}+H$
H	H	$\overline{1}+H$	$\overline{2}+H$
$\overline{1}+H$	$\overline{1}+H$	$\overline{2}+H$	H
$\overline{2}+H$	$\overline{2}+H$	H	$\overline{1}+H$

Розв'язання в Maple. Задаємо фактор-групу і операцію на ній (команда **coeff(X,H,0)** використовується для виокремлення числа a з виразу $a + H$ (як коефіцієнта при H^0)):

```
> FG:={H,1+H,2+H};
```

$$FG := \{H,\ 1+H,\ 2+H\}$$

```
> plus:=(X,Y)-> coeff(X,H,0)+coeff(Y,H,0) mod 3+H:
```

Застосовуємо процедуру **cayleyTable**:

```
> read(‘e:/atchlib.m‘);  with(atchlib):
> cayleyTable(FG,plus);
```

$$\begin{bmatrix} H & 1+H & 2+H \\ 1+H & 2+H & H \\ 2+H & H & 1+H \end{bmatrix}$$

Приклад 68.4. Побудувати фактор-групу A_4/V знакозмінної групи A_4 за її нормальною підгрупою

$$V = \left\{ e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \right.$$
$$\left. b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}.$$

Побудувати таблицю Келі для фактор-групи A_4/V.

Розв'язання. Порядок групи A_4 дорівнює $\frac{4!}{2} = 12$. Для зручності випишемо всі її елементи (парні підстановки степеня 4):

$$A_4 = \{e, a, b, c, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}\}.$$

Порядок шуканої фактор-групи A_4/V дорівнює

$$|A_4/V| = [A_4 : V] = \frac{|A_4|}{|V|} = \frac{12}{4} = 3.$$

Знаходимо її елементи (суміжні класи групи A_4 за підгрупою V). В якості першого суміжного класу беремо саму підгрупу $V = eV$. Для побудови наступного суміжного класу візьмемо будь-який елемент, який не ввійшов до класу eV, наприклад $m = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. Отримуємо наступний суміжний клас

$$mV = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} V =$$
$$= \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} e, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} a, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} b, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} c\} =$$
$$= \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}\}.$$

Третій суміжний клас отримаємо, вибравши в якості його представника будь-який елемент, який не ввійшов до класів eV і mV, наприклад $n =$

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

$$nV = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} V =$$

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

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

Елементи фактор-групи A_4/V знайдено. Отже,

$$A_4/V = \{eV, mV, nV\}.$$

Будуємо таблицю Келі для фактор-групи A_4/V. Рядочок і стовпчик, які відповідають елементу eV легко заповнити:

$\cdot$	eV	mV	nV
eV	eV	mV	nV
mV	mV		
nV	nV		

Тепер знаходимо добуток елементів mV і mV:

$$mV \cdot mV = m^2V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} V.$$

Оскільки підстановка $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ належить до класу nV, то $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} V = nV$, результат заносимо до таблиці Келі.

Далі знаходимо добуток елементів mV і nV:

$$mV \cdot nV = mnV = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} V.$$

Оскільки підстановка $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ належить до класу $eV = V$, то $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} V = eV$, результат знову заносимо до таблиці Келі.

Далі аналогічно знаходимо решту добутків:

$\cdot$	eV	mV	nV
eV	eV	mV	nV
mV	mV	nV	eV
nV	nV	eV	mV

Зауваження. Оскільки кожна група простого порядку є циклічною, а значить, і абелевою, то таблиця Келі для фактор-групи A_4/V повинна бути симетричною. Це дозволяє не обчислювати добуток $nVmV$, а одразу написати результат: $nVmV = mVnV = eV$. Крім того, можна врахувати, що таблиця Келі, яка задає групу, в кожному рядочку і стовпчику має містити нейтральний елемент; крім того, в рядочку елементи повторюватись не можуть (аналогічно для стовпчиків). Це може спростити побудову таблиці Келі.

Розв'язання в Maple. Задаємо групу A_4. При розв'язуванні Прикладу 64 було зазначено, що твірними елементами даної групи є всі можливі потрійні цикли. Маємо:

```
> A4:=permgroup(4, {[[1,2,3]], [[1,2,4]], [[1,3,2]], [[1,3,4]],
[[1,4,2]], [[1,4,3]], [[2,3,4]], [[2,4,3]]}):
```

Тепер задаємо підгрупу V:

```
> V:=permgroup(4, {[[1,2],[3,4]],[[1,3],[2,4]],[[1,4],[2,3]]}):
```

Оскільки $V \trianglelefteq A_4$, то кожен лівосторонній суміжний клас xV групи A_4 за підгрупою V збігається із відповідним правостороннім Vx. Тому для пошуку елементів фактор-групи A_4/V можна використати вбудовану команду **cosets**:

```
> FG:=cosets(A4,V);
```

$$FG := \{[],\ [[2,\ 3,\ 4]],\ [[2,\ 4,\ 3]]\}$$

Застосовуємо команду **cayleyTable**:

```
> read(‘e:/atchlib.m‘); with(atchlib):
> cayleyTable(FG,mulperms);
```

$$\begin{bmatrix} [\,] & [[2,3,4]] & [[2,\ 4,\ 3]] \\ [[2,\ 3,\ 4]] & [[2,\ 4,\ 3]] & [\,] \\ [[2,\ 4,\ 3]] & [\,] & [[2,\ 3,\ 4]] \end{bmatrix}$$

Підстановка $(234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ належить до суміжного класу nV, тому $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} V = nV$; підстановка $(243) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ належить до класу mV, тому $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} V = mV$. Тоді таблиця Келі, отримана в Maple, фактично, має вигляд:

$\cdot$	eV	nV	mV
eV	eV	nV	mV
nV	nV	mV	eV
mV	mV	eV	nV

Даний результат збігається із отриманим аналітично.

Завдання 68. Побудувати фактор-групу G/H групи G за її підгрупою H. Скласти таблицю Келі для G/H.

68.1. G – мультиплікативна група коренів 6-го степеня з одиниці;
H – її підгрупа коренів 2-го степеня з одиниці.

68.2. G – циклічна група 18-го порядку;
H – її підгрупа порядку 3.

68.3. $G = S_4$ – симетрична група підстановок степеня 4;
$H = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\}$.

68.4. G – циклічна група 16-го порядку;
H – її підгрупа порядку 4.

68.5. $G = \mathbb{Z}_{28}$ – адитивна група класів лишків за модулем 28;
$H = \langle\overline{8}\rangle$.

68.6. G – мультиплікативна група коренів 18-го степеня з одиниці;
H – її підгрупа коренів 6-го степеня з одиниці.

68.7. $G = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix},$
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}\}$;
$H = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}\}$.

68.8. $G = \mathbb{Z}_{18}$ – адитивна група класів лишків за модулем 28;
H – її підгрупа порядку 6.

68.9. G – циклічна група 15-го порядку;
H – її підгрупа порядку 3.

68.10. G – мультиплікативна група коренів 16-го степеня з одиниці;
H – її підгрупа коренів 4-го степеня з одиниці.

68.11. $G = \mathbb{Z}_{16}$ – адитивна група класів лишків за модулем 16;
$H = \langle\overline{10}\rangle$.

68.12. G – циклічна група 14-го порядку;
H – її підгрупа порядку 7.

68.13. G – мультиплікативна група коренів 20-го степеня з одиниці;
H – її підгрупа коренів 4-го степеня з одиниці.

68.14. G – циклічна група 24-го порядку;
H – її підгрупа порядку 4.

68.15. $G = \mathbb{Z}_{12}$ – адитивна група класів лишків за модулем 12;
H – її підгрупа порядку 2.

68.16. G – мультиплікативна група коренів 10-го степеня з одиниці;
H – її підгрупа коренів 2-го степеня з одиниці.

68.17. $G = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}\}$;
$H = \{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}\}$.

68.18. G – циклічна група 24-го порядку;
H – її підгрупа порядку 8.

68.19. $G = \mathbb{Z}_{18}$ – адитивна група класів лишків за модулем 18;
$H = \langle\overline{12}\rangle$.

68.20. G – мультиплікативна група коренів 20-го степеня з одиниці;
H – її підгрупа коренів 5-го степеня з одиниці.

68.21. G – циклічна група 18-го порядку;
H – її підгрупа порядку 6.

68.22. $G = \{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix},$

$$\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\4&3&2&1&5\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\5&4&3&2&1\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4&5\\1&5&4&3&2\end{pmatrix}\};$$
$$H=\{\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix}\}.$$

68.23. $G=\mathbb{Z}_{24}$ – адитивна група класів лишків за модулем 24;
$H=\langle\overline{4}\rangle$.

68.24. G – мультиплікативна група коренів 16-го степеня з одиниці;
H – її підгрупа коренів 8-го степеня з одиниці.

68.25. G – циклічна група 21-го порядку;
H – її підгрупа порядку 7.

5. Гомоморфізми груп

ТЕОРЕТИЧНІ ВІДОМОСТІ

Група $\langle G;*\rangle$ називається **гомоморфною** групі $\langle T;\circ\rangle$, якщо існує таке відображення φ групи G на групу T, при якому зберігається групова операція, тобто виконуються наступні умови:

1) для довільного $a\in G$ існує в T єдиний елемент t такий, що $\varphi(a)=t$;
2) для довільного $t_1\in T$ існує в G елемент a_1 такий, що $\varphi(a_1)=t_1$;
3) $\varphi(a_1*a_2)=\varphi(a_1)\circ\varphi(a_2)$ для будь-яких $a_1,a_2\in G$.

Якщо група G гомоморфна групі T, то пишуть: $G\simeq T$.

Властивості гомоморфізму груп:

1. Якщо φ – гомоморфізм групи $\langle G;*\rangle$ на групу $\langle T;\circ\rangle$, то:

1) образом нейтрального елемента e групи G є нейтральний елемент e_1 групи T, тобто $\varphi(e)=e_1$;
2) образом елемента a^{-1}, симетричного до елемента a групи G, є елемент $[\varphi(a)]^{-1}$, симетричний до образа $\varphi(a)$ елемента a.

2. Гомоморфний образ $\varphi(G)$ групи G є групою. Якщо G – абелева, то $\varphi(G)$ – також абелева.

Група $\langle G;*\rangle$ називається **ізоморфною** групі $\langle T;\circ\rangle$, якщо можна задати таке взаємно однозначне відображення φ групи G на групу T, при якому зберігається групова операція, тобто виконуються наступні умови:

1) для довільного $a \in G$ існує елемент $t \in T$ такий, що $\varphi(a) = t$;
2) для довільного $t' \in T$ існує елемент $a' \in G$ такий, що $\varphi(a') = t'$;
3) для будь-яких елементів $a_1, a_2 \in G \quad \varphi(a_1 * a_2) = \varphi(a_1) \circ \varphi(a_2)$;
4) для довільних $a, b \in G$ таких, що $a \neq b$, справедливо: $\varphi(a) \neq \varphi(b)$.

Якщо група G ізоморфна групі T, пишуть: $G \cong T$. Ізоморфне відображення групи G на групу T називають **ізоморфізмом** групи G на групу T. Таким чином, ізоморфізм G на T – це взаємно однозначний гомоморфізм G на T.

Ядром гомоморфізму φ групи G на групу T називається множина $K = \operatorname{Ker}\varphi$ елементів групи G, що відображаються на одиничний елемент e' групи T, тобто $\operatorname{Ker}\varphi = \{x \in G | \varphi(x) = e'\}$.

Ядро $\operatorname{Ker}\varphi$ гомоморфізму φ групи G на групу T є нормальною підгрупою групи G. Гомоморфізм φ групи G на групу T є ізоморфізмом цих груп тоді і лише тоді, коли $\operatorname{Ker}\varphi = \{e\}$, де e – одиничний елемент групи G.

Теорема (основна теорема гомоморфізму двох груп)**.** *Нехай φ – гомоморфізм групи G на групу T. Тоді фактор-група $G/\operatorname{Ker}\varphi$ групи G за ядром гомоморфізму $\operatorname{Ker}\varphi$ ізоморфна групі T.*

Наслідок. *Нехай $G \overset{\varphi}{\simeq} T$, $|G| < \infty$. Тоді $|\varphi(G)| \big| |G|$.*

ПРИКЛАДИ І ЗАДАЧІ

Приклад 69. Знайти всі гомоморфізми:
а) циклічної групи 10-го порядку в себе;
б) циклічної групи 8-го порядку в циклічну групу 6-го порядку;
в) циклічної групи 15-го порядку на циклічну групу 10-го порядку.

Розв'язання. Покажемо спочатку, що циклічна група L є гомоморфним образом скінченної циклічної групи G тоді і лише тоді, коли число $|L|$ є дільником числа $|G|$. Крім того, якщо $G = \langle a \rangle$, $L = \langle b \rangle$, то відображення $\varphi(a^s) = b^s$ є гомоморфізмом групи G на групу T.

Дійсно, якщо L – гомоморфний образ групи G, то, за наслідком із основної теореми гомоморфізму груп, $|H| \mid |G|$. Навпаки, нехай $|G| = n$, $|L| = m$, $m \mid n$. Розглянемо відображення $\varphi(a^s) = b^s$. Маємо:
1) Для довільного $a^s \in G$ справедливо, що $\varphi(a^s)$ існує, єдиний і належить до L.
2) Нехай $b^k \in L$, тоді $k \in \overline{0, m-1}$; прообразом елемента b^k в G є, наприклад, елемент a^k, оскільки $\varphi(a^k) = b^k$; елемент $a^k \in$ завжди існує в G.
3) Нехай $a^s, a^t \in G$, тоді $\varphi(a^s \cdot a^t) = \varphi(a^{s+t}) = b^{s+t} = b^s \cdot b^t = \varphi(a^s)\varphi(a^t)$.

Умови 1)-3) означення гомоморфізму виконуються, отже, φ– гомоморфізм групи G на групу T. Таким чином, для довільної циклічної групи T, порядок якої є дільником числа $|G|$, існує гомоморфізм G на T.

Перейдемо тепер до розв'язання задачі.

а) Знайти всі гомоморфізми групи G в себе означає знайти всі можливі гомоморфні відображення групи G на її підгрупи. Нехай $G = \langle a \rangle$, $|G| = 10$, $G = \{a, a^2, ..., a^{10} = e\}$. За твердженням 4.2 п.8, для кожного дільника k порядку $n = 10$ групи G існує, причому єдина, підгрупа $\langle a^{\frac{n}{k}} \rangle$ порядку k. Дільниками числа 10 є числа 1, 2, 5, 10. Їм відповідають підгрупи: $H_1 = \{e\}$, $H_2 = \langle a^5 \rangle$, $H_3 = \langle a^2 \rangle$, $H_4 = \langle a \rangle$.

Як було показано вище, для кожної із даних підгруп H_i існує гомоморфізм φ_i групи G на H_i, а саме: $\varphi_1(a^s) = e$; $\varphi_2(a^s) = a^{5s}$; $\varphi_3(a^s) = a^{2s}$; $\varphi_4(a^s) = a^s$. Таким чином, всього існує чотири гомоморфізми групи G в себе.

б) Нехай $G = \langle a \rangle$, $|G| = 8$, $G = \{a, a^2, ..., a^7, a^8 = e\}$, $T = \langle b \rangle$, $|T| = 6$, $T = \{b, b^2, ..., b^5, b^6 = b^0\}$. Знайти всі гомоморфізми групи G в групу T означає знайти всі можливі гомоморфні відображення групи G на підгрупи H групи T.

Нехай $H \leqslant T$. За теоремою Лагранжа, $|H| \mid |T|$, значить,

$$|H| \in \{1, 2, 3, 6\}. \tag{VII.5}$$

Не на кожну із підгруп H групи T існує гомоморфізм групи G: як було показано вище, для того, щоб підгрупа H була гомоморфним образом групи G необхідно і достатньо, щоб порядок H був дільником порядку G, тобто

$$|H| \in \{1, 2, 4, 8\}. \tag{VII.6}$$

Із умов (VII.5) і (VII.6) випливає, що $|H| = 1$ або $|H| = 2$, тобто $H = \{e\}$ або $H = \langle b^3 \rangle$. Таким чином, маємо всього два гомоморфізми групи G в групу T: $\varphi_1(a) = \{e\}$. $\varphi_2(a^s) = \langle b^{3s} \rangle$.

в) Задати гомоморфізм групи G на групу T означає знайти таке відображення φ, що гомоморфним образом $\varphi(G)$ буде вся група T. Якщо група G – скінченна, то порядок її гомоморфного образу $\varphi(G)$ має бути дільником порядку групи G. Проте $10 \nmid 15$, значить, гомоморфізму групи G на групу T не існує.

Розробка процедур. Створимо процедуру **endomorphisms(n)**, яка для циклічної групи $G = \langle a \rangle$ порядку n знаходитиме всі гомоморфізми групи G в себе. В ході процедури:

1) знаходимо множину d всіх дільників числа n:

```
> d:=divisors(n);
```

2) для кожного із дільників $d[i]$ знаходимо твірний елемент genH підгрупи H порядку $d[i]$ і виводимо правило, яке задає гомоморфізм, на екран:

```
> for i from 1 to nops(d) do
    genH:=a^(n/d[i] mod n);
    print('phi(a^s)'=genH^s);
  end do;
```

Код процедури наступний:

```
endomorphisms:=proc(n)
uses numtheory;
local d,i,genH;
   d:=divisors(n);
   for i from 1 to nops(d) do
      genH:=a^(n/d[i] mod n);
      print('Phi(a^s)'=genH^s);
   end do;
end proc:
```

Далі створимо процедуру **homomorphisms(n,m)**, яка для заданих циклічних груп $G = \langle a \rangle$ і $T = \langle b \rangle$ порядків n і m відповідно знаходить всі гомоморфізми групи G в T. Як було показано в ході аналітичного розв'язування даного прикладу, порядок підгрупи H групи T, на яку існує гомоморфізм групи G, є дільником і числа n, і числа m. Тому в ході процедури:

1) знаходимо множину всіх спільних дільників чисел n і m:

```
> d:=divisors(n) intersect divisors(m);
```

2) для кожного із дільників $d[i]$ знаходимо твірний елемент genH підгрупи H порядку $d[i]$ і виводимо відповідне правило на екран:

```
> for i from 1 to nops(d) do
  genH:=b^(m/d[i] mod m);
  print('Phi(a^s)'=genH^s);
  end do;
```

Процедура матиме наступний код:

```
homomorphisms:=proc(n,m)
local d,i,genH;
uses numtheory;
   d:=divisors(n) intersect divisors(m);
   for i from 1 to nops(d) do
      genH:=b^(m/d[i] mod m);
      print('Phi(a^s)'=genH^s);
   end do;
end proc:
```

Тепер створимо процедуру **homomorphismOnto(n,m)**, яка для заданих циклічних груп $G = \langle a \rangle$ і $T = \langle b \rangle$ порядків n і m відповідно знаходить всі гомоморфізми групи G на групу T.

Оскільки гомоморфізм групи $G = \langle a \rangle$, $|G| = n$, на групу $T = \langle b \rangle$, $|T| = m$, існує тоді і лише тоді, коли $n \vdots m$, то в ході процедури спершу необхідно перевірити, чи виконується умова $n \vdots m$: якщо дана умова виконується, то екран виводиться відповідний гомоморфізм $\varphi(a^s) = b^s$:

```
> if n mod m=0 then return('Phi(a^s)=b^s')
```

якщо ж ні – з'являється запис: "homomorphismu ne isnue"

```
> else return("homomorphismu ne isnue"); end if;
```

Код даної процедури наступний:

```
homomorphismOnto:=proc(n,m)
uses numtheory;
   if n mod m=0 then return('phi(a^ s)=b^ s')
   else return("homomorphismu ne isnue");
   end if;
end proc:
```

Розв'язання в Maple. Використовуємо створені процедури. Підключаємо бібліотеку atchlib:

```
> read(‘e:/atchlib.m‘);  with(atchlib):
```

а) Знаходимо всі гомоморфізми групи $G = \langle a \rangle$ порядку 10 в себе (такі гомоморфізми називають ще ендоморфізмами):

```
> endomorphisms(10);
```

$$\Phi(a^s) = 1$$
$$\Phi(a^s) = (a^5)^s$$
$$\Phi(a^s) = (a^2)^s$$
$$\Phi(a^s) = a^s$$

Таким чином, всього існує чотири гомоморфізми групи G в себе: $\varphi_1(a^s) = a^{0s} = e$; $\varphi_2(a^s) = a^{5s}$; $\varphi_3(a^s) = a^{2s}$; $\varphi_4(a^s) = a^s$.

б) Знаходимо всі гомоморфізми групи $G = \langle a \rangle$ 8-го порядку в групу $T = \langle b \rangle$ 6-го порядку:

```
> homomorphisms(8,6);
```

$$\Phi(a^s) = 1$$
$$\Phi(a^s) = (b^3)^s$$

Таким чином, маємо всього два гомоморфізми групи G в групу T: $\varphi_1(a) = \{e\}$. $\varphi_2(a^s) = \langle b^{3s} \rangle$.

в) Визначаємо, чи існує гомоморфізм групи $G = \langle a \rangle$ 15-го порядку на групу $T = \langle b \rangle$ 10-го порядку:

```
> homomorphismOnto(15,10);
```

"*homomorphismu ne isnue*"

Гомоморфізму групи G на групу T не існує.

Завдання 69. Знайти всі гомоморфізми:

69.1. циклічної групи 15-го порядку в себе.

69.2. мультиплікативної групи коренів 8 степеня з одиниці в адитивну групу $\mathbb{Z}_{10}$.

69.3. адитивної групи $\mathbb{Z}_{28}$ на мультиплікативну групу коренів 7-го степеня з одиниці.

69.4. мультиплікативної групи коренів 7 степеня з одиниці в адитивну групу $\mathbb{Z}_{10}$.

69.5. циклічної групи 10-го порядку в себе.

69.6. адитивної групи $\mathbb{Z}_{20}$ в адитивну групу $\mathbb{Z}_{40}$.

69.7. мультиплікативної групи коренів 8 степеня з одиниці на адитивну групу $\mathbb{Z}_{10}$.

69.8. адитивної групи $\mathbb{Z}_{15}$ в мультиплікативну групу коренів 5-го степеня з одиниці.

69.9. адитивної групи $\mathbb{Z}_6$ на адитивну групу $\mathbb{Z}_4$.

69.10. мультиплікативної групи коренів 36 степеня з одиниці в мультиплікативну групу коренів 8 степеня з одиниці.

69.11. циклічної групи 16-го порядку на циклічну групу порядку 4.

69.12. адитивної групи $\mathbb{Z}_{21}$ в себе.

69.13. циклічної групи 12-го порядку в циклічну групу порядку 10.

69.14. мультиплікативної групи коренів 12 степеня з одиниці в себе.

69.15. адитивної групи $\mathbb{Z}_{18}$ в адитивну групу $\mathbb{Z}_{12}$.

69.16. циклічної групи 20-го порядку в себе.

69.17. адитивної групи $\mathbb{Z}_{21}$ на мультиплікативну групу коренів 14-го степеня з одиниці.

69.18. мультиплікативної групи коренів 30 степеня з одиниці в мультиплікативну групу коренів 10 степеня з одиниці.

69.19. адитивної групи $\mathbb{Z}_6$ на адитивну групу $\mathbb{Z}_{12}$.

69.20. циклічної групи 24-го порядку в себе.

69.21. адитивної групи $\mathbb{Z}_{12}$ в мультиплікативну групу коренів 8-го степеня з одиниці.

69.22. мультиплікативної групи коренів 18 степеня з одиниці в себе.

69.23. мультиплікативної групи коренів 18 степеня з одиниці в себе.

69.24. мультиплікативної групи коренів 16 степеня з одиниці в адитивну групу $\mathbb{Z}_{10}$.

69.25. адитивної групи $\mathbb{Z}_{12}$ в себе.

Приклад 70. Довести, що фактор-група $\mathfrak{G}/\mathfrak{M}$ мультиплікативної групи $\mathfrak{G} = GL_2(\mathbb{Z}_5)$ невироджених матриць 2-го порядку над полем $\mathbb{Z}_5$ за підгрупою $\mathfrak{M} = \{X \in GL_2(\mathbb{Z}_5) | \, |X| = \overline{1}\}$ ізоморфна мультиплікативній групі $\mathbb{C}_4$ коренів 4-го степеня з одиниці.

Розв'язання. Спосіб I. Задамо відображення $\varphi : \mathfrak{G} \to \mathbb{C}_4$ наступним чином: для довільної матриці $A \in \mathfrak{G}$

$$\varphi(A) = \begin{cases} 1, & \text{якщо } |A| = \overline{1}, \\ \varepsilon, & \text{якщо } |A| = \overline{2}, \\ \varepsilon^2, & \text{якщо } |A| = \overline{4}, \\ \varepsilon^3, & \text{якщо } |A| = \overline{3}, \end{cases}$$

де $\varepsilon \in \mathbb{C}_4$ – первісний корінь 4-го степеня з одиниці.

Оскільки $\overline{4} = \overline{2^2}$, $\overline{3} = \overline{2^3}$, то $\varphi(A)$ можна записати наступним чином:

$$\varphi(A) = \varepsilon^k, \qquad \text{якщо } |A| = \overline{2^k}.$$

Покажемо, що φ – гомоморфізм групи $\mathfrak{G}$ на групу $\mathbb{C}_4$.

1) Нехай $A \in \mathfrak{G}$, тоді $|A| \in \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, а значить, $\varphi(A)$ існує, єдиний і належить до $\mathbb{C}_4$.

2) Нехай $c \in \mathbb{C}_4$, тоді $c = \varepsilon^l$, $l \in \overline{0,3}$, прообразом елемента c в $\mathfrak{G}$ є кожна матриця C така, що $|C| = \overline{2^l}$, наприклад $C = \begin{pmatrix} \overline{2^l} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$.

3) Нехай A, B – довільні два елементи із $\mathfrak{G}$ і нехай $|A| = \overline{2^k}$, $|B| = \overline{2^l}$, тоді $|AB| = \overline{2^k} \cdot \overline{2^l} = \overline{2^{k+l}}$. Значить, $\varphi(A) = \varepsilon^k$, $\varphi(B) = \varepsilon^l$, $\varphi(AB) = \varepsilon^{k+l}$. Як бачимо, $\varphi(AB) = \varphi(A)\varphi(B)$, отже, φ зберігає операцію.

Таким чином, φ – гомоморфізм групи $\mathfrak{G}$ на групу $\mathbb{C}_4$. Знайдемо ядро гомоморфізму φ. Нейтральним елементом групи $\mathbb{C}_4$ є елемент 1, тому

$$\operatorname{Ker}\varphi = \{X \in \mathfrak{G} | \varphi(X) = 1\} = \left\{X \in \mathfrak{G} \middle| |X| = \overline{1}\right\} = \mathfrak{M}.$$

За основною теоремою гомоморфізму двох груп $\mathfrak{G}/\mathfrak{M} \overset{\varphi}{\cong} \mathbb{C}_4$.

Спосіб II. Знайдемо фактор-групу $\mathfrak{G}/\mathfrak{M}$. В якості першого суміжного класу візьмемо саму підгрупу $\mathfrak{M}$. Для побудови наступного суміжного класу візьмемо будь-який елемент групи $\mathfrak{G}$, який не ввійшов до $\mathfrak{M}$

(будь-яку матрицю, визначник якої відмінний від $\overline{1}$), наприклад матрицю $B = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$. Отримаємо суміжний клас

$$B\mathfrak{M} = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \mathfrak{M} = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \{X \in \mathfrak{G} || X| = \overline{1}\} = \\ = \left\{ \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} X | X \in \mathfrak{G}, |X| = \overline{1} \right\}.$$

Даний клас складається з тих і лише тих матриць із $\mathfrak{G}$, визначник яких дорівнює $\overline{2}$. Дійсно, кожен елемент цього класу має визначник, що дорівнює $|\begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} X| = \begin{vmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{vmatrix} \cdot |X| = \overline{2} \cdot \overline{1} = \overline{2}$. Навпаки, нехай Y – довільна матриця із $\mathfrak{G}$, визначник якої дорівнює $\overline{2}$. Покажемо, що $Y \in B\mathfrak{M}$. Для матриці B існує обернена матриця B^{-1}. Розглянемо добуток $B^{-1}Y$. Оскільки $|B^{-1}Y| = |B^{-1}||Y| = \overline{2}^{-1}\overline{2} = \overline{1}$, то $B^{-1}Y \in \mathfrak{M}$, тобто в $\mathfrak{M}$ існує матриця M така, що $B^{-1}Y = M$, тоді $Y = BM \in B\mathfrak{M}$.

Щоб отримати третій суміжний клас, візьмемо довільну матрицю, що не ввійшла в суміжні класи $\mathfrak{M}$ і $B\mathfrak{M}$ (тобто матрицю, визначник якої відмінний від $\overline{1}$ і $\overline{2}$). Такою матрицею є, наприклад, матриця $C = \begin{pmatrix} \overline{3} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$. Отримаємо суміжний клас $C\mathfrak{M}$. Аналогічними міркуваннями неважко показати, що даний суміжний клас складається з тих і лише тих матриць із $\mathfrak{G}$, визначник яких дорівнює $\overline{3}$.

В $\mathfrak{G}$ ще залишились елементи, що не ввійшли до суміжних класів $\mathfrak{M}$, $B\mathfrak{M}$, $C\mathfrak{M}$: матриці, визначник яких дорівнює $\overline{4}$. Вони утворюють четвертий суміжний клас, в якості представника цього класу можна взяти, наприклад, матрицю $D = \begin{pmatrix} \overline{4} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$. Маємо суміжний клас $D\mathfrak{M}$. Оскільки суміжні класи $\mathfrak{M}$, $B\mathfrak{M}$, $C\mathfrak{M}$, $D\mathfrak{M}$ попарно не перетинаються і в об'єднанні дають множину $\mathfrak{G}$, то

$$\mathfrak{G}/\mathfrak{M} = \{\mathfrak{M}, B\mathfrak{M}, C\mathfrak{M}, D\mathfrak{M}\}$$

Покажемо, що група $\mathfrak{G}/\mathfrak{M}$ є циклічною. Для цього достатньо показати, що в $\mathfrak{G}/\mathfrak{M}$ є елемент порядку 4. Таким елементом є, наприклад, суміжний клас $B\mathfrak{M}$. Дійсно, нейтральним елементом є суміжний клас $\mathfrak{M}$, маємо:

$$\begin{aligned} B\mathfrak{M} &\neq \mathfrak{M}, \\ (B\mathfrak{M})^2 &= B^2\mathfrak{M} = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{4} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \neq \mathfrak{M}, \end{aligned}$$

значить, $|B\mathfrak{M}| = 4$. Але тоді група $\mathfrak{G}/\mathfrak{M}$ – циклічна.

Група $\mathbb{C}_4$ також циклічна 4-го порядку. Оскільки всі скінченні циклічні групи однакового порядку ізоморфні між собою, то $\mathfrak{G}/\mathfrak{M} \cong \mathbb{C}_4$.

Розв'язання в Maple. Задаємо множину $GL_2(\mathbb{Z}_5)$ і операцію mmult множення матриць:

```
> T:={seq(seq(seq(seq([[x,y],[z,t]],x=0..4),y=0..4),
                                          z=0..4),t=0..4)}:
> GL2:=select(A->evalb(A[1,1]*A[2,2]-A[1,2]*A[2,1] mod 5<>0),T):
> mmult:=(A,B)->[[A[1,1]*B[1,1]+A[1,2]*B[2,1] mod 5,
                  A[1,1]*B[1,2]+A[1,2]*B[2,2] mod 5],
                  [A[2,1]*B[1,1]+A[2,2]*B[2,1] mod 5,
                  A[2,1]*B[1,2]+A[2,2]*B[2,2] mod 5]]:
```

множину $\mathfrak{M}$:

```
> M:=select(A->evalb(A[1,1]*A[2,2]-A[1,2]*A[2,1] mod 5=1),T):
```

і множину $\mathbb{C}_4$ та операцію ml множення на ній:

```
> C4:={seq(epsilon^i,i=0..3)};
```

$$C4 := \{1, \varepsilon, \varepsilon^2, \varepsilon^3\}$$

```
> ml:=(C,D)->
      (epsilon^(degree(C,epsilon)+degree(D,epsilon) mod 4)):
```

Тепер задаємо відображення φ. Для цього спочатку задаємо функцію **determ** для відшукання визначника матриці A:

```
> determ:=A->A[1,1]*A[2,2]-A[2,1]*A[1,2] mod 5:
```

Задання функції f виду

$$f(x) = \begin{cases} \text{result1}, & \text{якщо} \quad \text{condition1}; \\ \text{result2}, & \text{якщо} \quad \text{condition2}; \\ \ldots, & \ldots \\ \text{resultK}, & \text{якщо} \quad \text{conditionK}; \end{cases}$$

здійснюється із використанням команди **piecewise** у форматі: **piecewice(result1,condition1,result2,condition2,...,resultK,conditionK)**. Маємо:

```
> PHI:=A -> piecewise(determ(A)=1,1,determ(A)=2,epsilon,
determ(A)=4,epsilon^2, determ(A)=3,epsilon^3):
```

Далі використовуємо процедури, створені при розв'язанні Прикладу 28.1.

```
> read(‘e:/atchlib.m‘); with(atchlib):
> existsIm(PHI,GL2,C4);
```

true

```
> existsProim(PHI,GL2,C4);
```

true

```
> savesOperation(PHI,GL2,C4,mmult,ml);
```

true

Відображення $\varphi : GL_2(\mathbb{Z}_5) \to \mathbb{C}_4$ задовольняє умови означення гомоморфізму, отже, φ – гомоморфізм групи $GL_2(\mathbb{Z}_5)$ на групу $\mathbb{C}_4$.

Знаходимо ядро гомоморфізму із використанням процедури **kerPHI** із Прикладу 28.1:

```
> kerPHI(PHI,GL2,C4,ml);
```

{[[0, 1], [4, 0]], [[0, 1], [4, 1]], [[0, 1], [4, 2]], [[0, 1], [4, 3]], [[0, 1], [4, 4]],
[[0, 2], [2, 0]], [[0, 2], [2, 1]], [[0, 2], [2, 2]], [[0, 2], [2, 3]], [[0, 2], [2, 4]],
[[0, 3], [3, 0]], [[0, 3], [3, 1]], [[0, 3], [3, 2]], [[0, 3], [3, 3]], [[0, 3], [3, 4]],
[[0, 4], [1, 0]], [[0, 4], [1, 1]], [[0, 4], [1, 2]], [[0, 4], [1, 3]], [[0, 4], [1, 4]],
[[1, 0], [0, 1]], [[1, 0], [1, 1]], [[1, 0], [2, 1]], [[1, 0], [3, 1]], [[1, 0], [4, 1]],
[[1, 1], [0, 1]], [[1, 1], [1, 2]], [[1, 1], [2, 3]], [[1, 1], [3, 4]], [[1, 1], [4, 0]],
[[1, 2], [0, 1]], [[1, 2], [1, 3]], [[1, 2], [2, 0]], [[1, 2], [3, 2]], [[1, 2], [4, 4]],
[[1, 3], [0, 1]], [[1, 3], [1, 4]], [[1, 3], [2, 2]], [[1, 3], [3, 0]], [[1, 3], [4, 3]],
[[1, 4], [0, 1]], [[1, 4], [1, 0]], [[1, 4], [2, 4]], [[1, 4], [3, 3]], [[1, 4], [4, 2]],
[[2, 0], [0, 3]], [[2, 0], [1, 3]], [[2, 0], [2, 3]], [[2, 0], [3, 3]], [[2, 0], [4, 3]],
[[2, 1], [0, 3]], [[2, 1], [1, 1]], [[2, 1], [2, 4]], [[2, 1], [3, 2]], [[2, 1], [4, 0]],
[[2, 2], [0, 3]], [[2, 2], [1, 4]], [[2, 2], [2, 0]], [[2, 2], [3, 1]], [[2, 2], [4, 2]],
[[2, 3], [0, 3]], [[2, 3], [1, 2]], [[2, 3], [2, 1]], [[2, 3], [3, 0]], [[2, 3], [4, 4]],
[[2, 4], [0, 3]], [[2, 4], [1, 0]], [[2, 4], [2, 2]], [[2, 4], [3, 4]], [[2, 4], [4, 1]],
[[3, 0], [0, 2]], [[3, 0], [1, 2]], [[3, 0], [2, 2]], [[3, 0], [3, 2]], [[3, 0], [4, 2]],
[[3, 1], [0, 2]], [[3, 1], [1, 4]], [[3, 1], [2, 1]], [[3, 1], [3, 3]], [[3, 1], [4, 0]],
[[3, 2], [0, 2]], [[3, 2], [1, 1]], [[3, 2], [2, 0]], [[3, 2], [3, 4]], [[3, 2], [4, 3]],
[[3, 3], [0, 2]], [[3, 3], [1, 3]], [[3, 3], [2, 4]], [[3, 3], [3, 0]], [[3, 3], [4, 1]],
[[3, 4], [0, 2]], [[3, 4], [1, 0]], [[3, 4], [2, 3]], [[3, 4], [3, 1]], [[3, 4], [4, 4]],
[[4, 0], [0, 4]], [[4, 0], [1, 4]], [[4, 0], [2, 4]], [[4, 0], [3, 4]], [[4, 0], [4, 4]],
[[4, 1], [0, 4]], [[4, 1], [1, 3]], [[4, 1], [2, 2]], [[4, 1], [3, 1]], [[4, 1], [4, 0]],
[[4, 2], [0, 4]], [[4, 2], [1, 2]], [[4, 2], [2, 0]], [[4, 2], [3, 3]], [[4, 2], [4, 1]],
[[4, 3], [0, 4]], [[4, 3], [1, 1]], [[4, 3], [2, 3]], [[4, 3], [3, 0]], [[4, 3], [4, 2]],
[[4, 4], [0, 4]], [[4, 4], [1, 0]], [[4, 4], [2, 1]], [[4, 4], [3, 2]], [[4, 4], [4, 3]]}

Перевіримо, чи збігається ядро гомоморфізму із підгрупою $\mathfrak{M}$:

```
> evalb(Ker_phi(PHI,GL2,C4,ml)=M);
```

true

Отже, $\operatorname{Ker}\varphi = \mathfrak{M}$.

За основною теоремою гомоморфізму двох груп, $\mathfrak{G}/\mathfrak{M} \overset{\varphi}{\cong} \mathbb{C}_4$.

Завдання 70.

70.1. Задати гомоморфізм симетричної групи підстановок S_3 на мультиплікативну групу $T = \{-1, 1\}$.

70.2. Довести, що група $GL_2(\mathbb{Z}_2)$ ізоморфна симетричній групі підстановок S_3.

70.3. Визначити, чи є відображення φ мультиплікативної групи $\mathbb{Z}_{15}^*$ на мультиплікативну групу $\mathbb{C}_8$ коренів 8-го степеня з одиниці за правилом: $\varphi(A) = \varepsilon^i$ гомоморфізмом $\mathbb{Z}_{15}^*$ на $\mathbb{C}_8$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

70.4. Задати гомоморфізм мультиплікативної групи $G = GL_3(\mathbb{Z}_5)$ на мультиплікативну групу $G = GL_2(\mathbb{Z}_5)$. Знайти ядро цього гомоморфізму.

70.5. Довести, що існує гомоморфізм групи $GL_2(\mathbb{Z}_4)$ на адитивну групу $\mathbb{Z}_3$.

70.6. Визначити, чи є відображення φ мультиплікативної групи $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{Z}_5, a^2 + b^2 \neq \overline{0} \right\}$ на мультиплікативну групу $T = \left\{ \begin{pmatrix} c & \overline{0} \\ \overline{0} & c \end{pmatrix} | c \in \mathbb{Z}_5, c \neq \overline{0} \right\}$ за правилом: $\varphi(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) = \begin{pmatrix} a & \overline{0} \\ \overline{0} & a \end{pmatrix}$ гомоморфізмом G на T. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

70.7. Визначити, чи є гомоморфною (ізоморфною) група $\langle \mathbb{Z}_5, * \rangle$, в якій операція $*$ задана рівністю: $a * b = a + b + \overline{1}$, адитивній групі $\mathbb{Z}_5$.

70.8. Задати гомоморфізм адитивної групи $\mathbb{Z}_{18}$ на мультиплікативну групу $T = \{-1, 1\}$. Знайти ядро цього гомоморфізму.

70.9. Довести, що фактор-група S_4/V симетричної групи підстановок S_4 за її підгрупою

$$V = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

ізоморфна групі S_3.

70.10. Задати гомоморфізм мультиплікативної групи $G = \left\{ \begin{pmatrix} a & b \\ \overline{0} & c \end{pmatrix} | a, b, c \in \mathbb{Z}_7, ac \neq \overline{0} \right\}$ на мультиплікативну групу T всіх діагональних матриць 2-го порядку над полем $\mathbb{Z}_7$. Знайти ядро цього гомоморфізму.

70.11. Визначити, чи існує гомоморфізм (ізоморфізм) мультиплікативної групи $\mathbb{Z}_{16}^*$ на мультиплікативну групу $\mathbb{C}_8$ коренів 8-го степеня з одиниці.

70.12. Задати гомоморфізм мультиплікативної групи $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{Z}_5, a^2 + b^2 \neq \overline{0} \right\}$ на мультиплікативну групу $T = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} | x, y \in \mathbb{Z}_5, x^2 + y^2 = \overline{1} \right\}$. Знайти ядро цього гомоморфізму.

70.13. Знайти всі гомоморфізми (або довести, що їх не існує) симетричної групи підстановок S_3 в адитивну групу $\mathbb{Z}_{10}$ та їхні ядра.

70.14. Визначити, чи є відображення φ мультиплікативної групи $G = \left\{ \begin{pmatrix} a & b \\ \overline{4}b & a \end{pmatrix} | a, b, c \in \mathbb{Z}_5, a^2 + b^2 \neq \overline{0} \right\}$ на адитивну групу $\mathbb{Z}_5$ за правилом: $\varphi(A) = \frac{1}{|A|}$ гомоморфізмом G на $\mathbb{Z}_5$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

70.15. Визначити, чи є відображення φ мультиплікативної групи $G = GL_2(\mathbb{Z}_5)$ на мультиплікативну групу $T = \left\{ \begin{pmatrix} a & b \\ \overline{0} & c \end{pmatrix} | a, b, c \in \mathbb{Z}_5, ac \neq \overline{0} \right\}$ за правилом: $\varphi(\begin{pmatrix} x & y \\ z & u \end{pmatrix}) = \begin{pmatrix} x & y \\ \overline{0} & u \end{pmatrix}$ гомоморфізмом G на T. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

70.16. Довести, що фактор-група G/H групи підстановок

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

за її підгрупою $H = \{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \}$ ізоморфна мультиплікативній групі $T = \{-1, 1\}$.

70.17. Задати гомоморфізм групи G пар (a, b), де $a, b \in \mathbb{Z}_5$, на якій задано операцію $*$ за правилом: $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$, на адитивну групу $\mathbb{Z}_5$. Знайти ядро цього гомоморфізму.

70.18. Довести, що фактор-група $\mathbb{Z}_{12}/H$ адитивної групи $\mathbb{Z}_{12}$ за її підгрупою $H = \langle\overline{8}\rangle$ ізоморфна мультиплікативній групі $T = \{1, -1, i, -i\}$.

70.19. Визначити, чи існує гомоморфізм адитивної групи $\mathbb{Z}_{12}$ на знакозмінну групу підстановок A_3 Якщо так, вказати його і знайти ядро цього гомоморфізму.

70.20. Визначити, чи є відображення φ мультиплікативної групи $G = \left\{ \begin{pmatrix} a & \overline{0} & d \\ \overline{0} & b & \overline{0} \\ \overline{0} & \overline{0} & c \end{pmatrix} | a, b, c \in \mathbb{Z}_3, abc \neq \overline{0} \right\}$ на адитивну групу $\mathbb{Z}_3$ за правилом: $\varphi(\begin{pmatrix} a & \overline{0} & d \\ \overline{0} & b & \overline{0} \\ \overline{0} & \overline{0} & c \end{pmatrix}) = b$ гомоморфізмом G на $\mathbb{Z}_3$. Якщо так, знайти ядро цього гомоморфізму. Чи є φ ізоморфізмом?

70.21. Задати гомоморфізм мультиплікативної групи $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{Z}_5, a^2 + b^2 \neq \overline{0} \right\}$ на мультиплікативну групу $\mathbb{Z}_5^*$. Знайти ядро цього гомоморфізму.

70.22. Довести, що фактор-група A_4/V знакозмінної групи підстановок A_4 за її підгрупою

$$V = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

ізоморфна адитивній групі Z_3.

70.23. Задати гомоморфізм адитивної групи $\mathbb{Z}_{20}$ на мультиплікативну групу $T = \langle i \rangle$. Знайти ядро цього гомоморфізму.

70.24. Довести, що фактор-група G/H мультиплікативної групи $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{Z}_7, a^2 + b^2 \neq \overline{0} \right\}$ за її підгрупою H матриць, визначник яких дорівнює $\overline{1}$, ізоморфна мультиплікативній групі коренів 6-го степеня з одиниці.

70.25. Визначити, чи існує гомоморфізм адитивної групи $\mathbb{Z}_{12}$ на симетричну групу підстановок S_3 Якщо так, вказати його і знайти ядро цього гомоморфізму.

Розділ VIII

Теорія полів

1. Алгебраїчні розширення. Мінімальний многочлен

ТЕОРЕТИЧНІ ВІДОМОСТІ

Нехай P – деяке числове поле. Число α називають алгебраїчним над полем P, якщо воно є коренем деякого ненульового многочлена над полем P. Число, яке не є алгебраїчним відносно поля P, називають трансцендентним над полем P. Зокрема, алгебраїчні і трансцендентні числа над полем $\mathbb{Q}$ називають просто алгебраїчними і трансцендентними.

Якщо α є алгебраїчним числом над полем P, то в кільці $P[x]$ існує єдиний незвідний нормований многочлен $f(x)$, який має α своїм коренем, а його степінь n є найменшим серед степенів усіх многочленів з коренем α. При цьому многочлен $f(x)$ називають мінімальним многочленом числа α, а його степінь n – степенем числа α над полем P.

Мінімальне розширення поля P, яке містить число $\alpha \notin P$, називають простим розширенням поля P, породженим над P числом α, і позначають через $P(\alpha)$.

ПРИКЛАДИ І ЗАДАЧІ

Приклад 71. Довести, що число $\alpha = \sqrt[5]{\sqrt[3]{6+\sqrt{2}}-2}$ алгебраїчне, і знайти його мінімальний многочлен.

Розв'язання. Позбавимося радикалів. Для цього послідовно піднесемо обидві частини рівності

$$\alpha = \sqrt[5]{\sqrt[3]{6+\sqrt{2}}-2}$$

$$\begin{aligned}
\text{до п'ятого:} \qquad & \alpha^5 = \sqrt[3]{6+\sqrt{2}} - 2, \\
& \alpha^5 + 2 = \sqrt[3]{6+\sqrt{2}}, \\
\text{третього:} \qquad & (\alpha^5+2)^3 = 6+\sqrt{2}, \\
& (\alpha^5+2)^3 - 6 = \sqrt{2}, \\
\text{і другого степенів:} \qquad & ((\alpha^5+2)^3-6)^2 = 2. \\
\text{Отримаємо:} \qquad & ((\alpha^5+2)^3-6)^2 - 2 = 0.
\end{aligned}$$

Остання рівність означає, що число α є коренем многочлена

$$f(x) = ((x^5+2)^3-6)^2 - 2$$

з раціональними коефіцієнтами. Отже, α є алгебраїчним числом.

Покажемо, що многочлен $f(x)$ є мінімальним многочленом числа α. Многочлен $f(x)$ – нормований, тому залишається показати, що цей многочлен є незвідним над полем $\mathbb{Q}$. Запишемо многочлен $f(x)$ в стандартному вигляді:

$$f(x) = ((x^5+2)^3-6)^2 - 2 = x^{30} + 12x^{25} + 60x^{20} + 148x^{15} + 168x^{10} + 48x^5 + 2.$$

Оскільки всі коефіцієнти многочлена $f(x)$, крім старшого, діляться на 2, а вільний член не ділиться на 4, то за ознакою Айзенштайна многочлен $f(x)$ є незвідним над полем $\mathbb{Q}$. Отже, $f(x)$ є мінімальним многочленом числа α.

Розв'язання в Maple. В пакеті **PolynomialTools** є команда під назвою **MinimalPolynomial** (повний формат **MinimalPolynomial(**α**,n,**ε**)**). Однак за допомогою цієї команди знаходять НЕ мінімальний многочлен заданого числа α, а многочлен степеня n (або меншого) з найменшими цілими коефіцієнтами, для якого з точністю ε число α є коренем.

Знайдемо мінімальний многочлен в наступний спосіб. Для дій над алгебраїчними числами використовується команда **evala** та (якщо потрібно) додаткові команди. Зокрема, для відшукання мінімального многочлена числа α використовуватимемо конструкцію **evala(Norm(x-**α**))**. Слід зауважити, що число α попередньо подають в RootOf-записі (такий запис містить мінімальний многочлен для кожного окремого радикала у складі числа α). Такий RootOf-запис знаходять за допомогою команди **convert**.

Так, наприклад, для числа $\alpha = \sqrt{2}$ RootOf-запис виглядатиме наступним чином:

```
> alpha:=sqrt(2):
  convert(alpha,RootOf);
```

$$\mathrm{RootOf}(\_Z^2-2,\ index=1)$$

А для числа $\alpha=\sqrt{2}+\sqrt{3}$ матимемо:

```
> alpha:=sqrt(2)+sqrt(3): convert(alpha,RootOf);
```

$$\mathrm{RootOf}(\_Z^2-2,\ index=1)+\mathrm{RootOf}(\_Z^2-3,\ index=1)$$

Для заданого числа $\alpha=\sqrt[5]{\sqrt[3]{6+\sqrt{2}}-2}$ матимемо:

```
> alpha:=((6+sqrt(2))^(1/3)-2)^(1/5);
```

$$\alpha:=((6+\sqrt{2})^{(1/3)}-2)^{(1/5)}$$

Знаходимо RootOf-запис числа α (назвемо його ra):

```
> ra:=convert(alpha,RootOf);
```

$$ra:=\mathrm{RootOf}(\_Z^5-\mathrm{RootOf}(\_Z^3-6-\mathrm{RootOf}(\_Z^2-2,\ index=1),\ index=1)+2,\ index=1)$$

Тепер знаходимо мінімальний многочлен числа α:

```
> evala(Norm(x-ra));
```

$$2+48\,x^5+168\,x^{10}+148\,x^{15}+60\,x^{20}+12\,x^{25}+x^{30}$$

Завдання 71. Довести, що число α алгебраїчне, і знайти його мінімальний многочлен.

71.1. $\alpha=2+\sqrt[3]{5+\sqrt{7}}$.

71.2. $\alpha+\sqrt[5]{7}+2=0$.

71.3. $\alpha=\sqrt{5+\sqrt{3}}$.

71.4. $\alpha=\sqrt[3]{7+i}$.

71.5. $\alpha=\sqrt{2+\sqrt[3]{3}}+3$.

71.6. $\alpha=\sqrt[5]{3+\sqrt[3]{6+\sqrt{3}}}$.

71.7. $\alpha=\sqrt[4]{\sqrt{2+\sqrt{3}}+5}$.

71.8. $\alpha=\sqrt[5]{1+\sqrt[4]{5+\sqrt{2}}}$.

71.9. $\alpha=2+\sqrt[3]{1+\sqrt{7}}$.

71.10. $\alpha=\sqrt{5-\sqrt{3}}$.

71.11. $\alpha+\sqrt[7]{6}-3=0$.

71.12. $\alpha=\sqrt[2008]{i\sqrt{13}+3}$.

71.13. $\alpha=\sqrt[5]{\sqrt[4]{7+\sqrt{2}}+3}$.

71.14. $\alpha=\sqrt{\sqrt[3]{7}-4}+2$.

71.15. $\alpha=\sqrt[3]{7+\sqrt{5}i}$.

71.16. $\alpha=\sqrt[3]{2+\sqrt{3}}$.

71.17. $\alpha=1+\sqrt[3]{\sqrt{7}-2}$.

71.18. $\alpha+\sqrt[4]{7}-9=0$.

71.19. $\alpha=\sqrt[4]{3+\sqrt{4+\sqrt{3}}}$.

71.20. $\alpha=1+\sqrt[3]{3+\sqrt{2}}$.

71.21. $\alpha=\sqrt[4]{\sqrt{\sqrt{3}-2}-5}$.

71.22. $\alpha=\sqrt[3]{\sqrt{5}-4}$.

71.23. $\alpha=\sqrt[5]{i\sqrt{10}+2}$.

71.24. $\alpha=\sqrt[3]{5+\sqrt[4]{3}}+2$.

71.25. $\alpha+2+\sqrt[5]{6}=0$.

2. Позбавлення від алгебраїчної ірраціональності в знаменнику дробу

ТЕОРЕТИЧНІ ВІДОМОСТІ

Основні методи розв'язування задач на позбавлення від ірраціональності в знаменнику дробу грунтуються на таких фактах:

1. Якщо $f(x)$ – многочлен від однієї змінної над полем P з коренями $\alpha_1, \alpha_2, ..., \alpha_n$ (які можуть не належати до P), то кожен симетричний многочлен $g(x_1, x_2, ..., x_n)$ над полем P при $x_1 = \alpha_1$, $x_2 = \alpha_2$,..., $x_n = \alpha_n$ набуває значення, яке є елементом поля P.

2. Поле $P(\alpha)$, утворене з числового поля P приєднанням числа α, мінімальний многочлен якого над полем P має степінь n, складається з усіх чисел виду

$$c_0 + c_1\alpha + c_2\alpha^2 + ... + c_{n-1}\alpha^{n-1},$$

де $c_0, c_1, c_2, ..., c_{n-1}$ – довільні числа з поля P.

Крім цього, при розв'язуванні таких задач застосовуються формули скороченого множення:

$$\begin{aligned} x^n - y^n &= (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + ... + xy^{n-2} + y^{n-1}), \\ x^{2k+1} + y^{2k+1} &= (x+y)(x^{2k} - x^{2k-1}y + x^{2k-2}y^2 - ... - xy^{2k-1} + y^{2k}). \end{aligned}$$

ПРИКЛАДИ І ЗАДАЧІ

Приклад 72. Позбавитись від ірраціональності в знаменнику дробу $\frac{1}{\omega_1^2 - 1}$, де ω_1 – один із коренів рівняння

$$x^3 - 2x + 2 = 0. \tag{VIII.1}$$

Розв'язання. Спосіб I. Використаємо метод симетричних многочленів. Нехай ω_2^2, ω_3^2 – решта коренів рівняння (VIII.1). Тоді

$$\frac{(\omega_2^2 - 1)(\omega_3^2 - 1)}{(\omega_1^2 - 1)(\omega_2^2 - 1)(\omega_3^2 - 1)} = \frac{\omega_2^2\omega_3^2 - \omega_2^2 - \omega_3^2 + 1}{\omega_1^2\omega_2^2\omega_3^2 - \omega_1^2\omega_2^2 - \omega_2^2\omega_3^2 - \omega_1^2\omega_3^2 + \omega_1^2 + \omega_2^2 + \omega_3^2 - 1}.$$

Знаменник дробу

$$\frac{\omega_2^2\omega_3^2 - \omega_2^2 - \omega_3^2 + 1}{\omega_1^2\omega_2^2\omega_3^2 - \omega_1^2\omega_2^2 - \omega_2^2\omega_3^2 - \omega_1^2\omega_3^2 + \omega_1^2 + \omega_2^2 + \omega_3^2 - 1} \tag{VIII.2}$$

можна розглядати як симетричний многочлен $\varphi(\omega_1, \omega_2, \omega_3)$ від змінних $\omega_1, \omega_2, \omega_3$. Виразимо його через елементарні симетричні многочлени

$$\begin{aligned} \sigma_1 &= \omega_1 + \omega_2 + \omega_3, \\ \sigma_2 &= \omega_1\omega_2 + \omega_1\omega_3 + \omega_2\omega_3, \\ \sigma_2 &= \omega_1\omega_2\omega_3 \end{aligned}$$

(див. приклад 44). Спочатку запишемо $\varphi(\omega_1,\omega_2,\omega_3)$ як суму однорідних многочленів:

$$\varphi(\omega_1,\omega_2,\omega_3)=\sigma_3^2-\varphi_1(\omega_1,\omega_2,\omega_3)+\varphi_2(\omega_1,\omega_2,\omega_3)-1,$$

$$\text{де}\qquad \begin{aligned}\varphi_1(\omega_1,\omega_2,\omega_3)&=\omega_1^2\omega_2^2+\omega_2^2\omega_3^2+\omega_1^2\omega_3^2,\\ \varphi_2(\omega_1,\omega_2,\omega_3)&=\omega_1^2+\omega_2^2+\omega_3^2.\end{aligned}$$

Система показників вищого члена			Вищий член	Відповідний добуток елементарних симетричних многочленів
ω_1	ω_2	ω_3		
2	2	0	$\omega_1^2\omega_2$	$\sigma_1^{2-}\sigma_2^{2-0}\sigma_3^0=\sigma_2^2$
2	1	1	$a\omega_1^2\omega_2\omega_3$	$a\sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^1=a\sigma_1\sigma_3$

ω_1	ω_2	ω_3	σ_1 $=\omega_1+\omega_2+\omega_3$	σ_2 $=\omega_1\omega_2+\omega_1\omega_3+\omega_2\omega_3$	σ_3 $=\omega_1\omega_2\omega_3$	$\varphi_1(\omega_1,\omega_2,\omega_3)$ $=\sigma_2^2+a\sigma_1\sigma_3$
1	1	-1	1	-1	-1	$3=1-a$

Отже, $a=-2$, а значить, $\varphi_1(\omega_1,\omega_2,\omega_3)=\sigma_2^2-2\sigma_1\sigma_3$. Легко бачити, що

$$\varphi_2(\omega_1,\omega_2,\omega_3)=\omega_1^2+\omega_2^2+\omega_3^2=(\omega_1+\omega_2+\omega_3)^2-2(\omega_1\omega_2+\omega_1\omega_3+\omega_2\omega_3)=\sigma_1^2-2\sigma_2,$$

а отже,

$$\varphi(\omega_1,\omega_2,\omega_3)=\sigma_3^2-(\sigma_2^2-2\sigma_1\sigma_3)+\sigma_1^2-2\sigma_2-1=\sigma_1^2-2\sigma_2^2+\sigma_3^2+2\sigma_1\sigma_3-2\sigma_2-1.$$

Оскільки $\omega_1,\omega_2,\omega_3$ є коренями рівняння (VIII.1), за теоремою Вієта

$$\begin{cases}\omega_1+\omega_2+\omega_3=0,\\ \omega_1\omega_2+\omega_1\omega_3+\omega_2\omega_3=-2,\\ \omega_1\omega_2\omega_3=-2;\end{cases}\qquad\text{або}\qquad\begin{cases}\sigma_1=0,\\ \sigma_2=-2,\\ \sigma_3=-2;\end{cases}$$

звідки $\varphi(\omega_1,\omega_2,\omega_3)=3$.

Розглянемо тепер чисельник дробу (VIII.2):

$$\omega_2^2\omega_3^2-\omega_2^2-\omega_3^2+1=(\omega_2\omega_3)^2-(\omega_2+\omega_3)^2+2\omega_2\omega_3+1.$$

Числа ω_2 і ω_3 є коренями рівняння $\frac{x^3-2x+2}{x-\omega_1}=0$. Виконаємо ділення за схемою Горнера:

	1	0	-2	2
ω_1	1	ω_1	ω_1^2-2	$\underbrace{\omega_1^3-2\omega_1+2}_{=0}$

Таким чином, $\frac{x^3-2x+2}{x-\omega_1} = x^2 + \omega_1 x + (\omega_1^2 - 2)$. Отже, ω_2 і ω_3 є коренями рівняння $x^2 + \omega_1 x + \omega_1^2 - 2 = 0$. За теоремою Вієта

$$\begin{cases} \omega_2 + \omega_3 = -\omega_1, \\ \omega_2\omega_3 = \omega_1^2 - 2. \end{cases}$$

А отже,

$$\frac{1}{\omega_1^2 - 1} = \frac{(\omega_1^2 - 2)^2 - \omega_1^2 + 2(\omega_1^2 - 2) + 1}{3} = \frac{\omega_1^4 - 3\omega_1 + 1}{3}.$$

Степінь чисельника можна понизити. Оскільки ω_1 є коренем рівняння (VIII.1), то $\omega_1^3 = 2\omega_1 - 2$, а тому

$$\frac{1}{\omega_1^2 - 1} = \frac{\omega_1^3\omega_1 - 3\omega_1 + 1}{3} = \frac{(2\omega_1 - 2)\omega_1 - 3\omega_1 + 1}{3} = \frac{-\omega_1^2 - 2\omega_1 + 1}{3}.$$

Спосіб II. Використаємо метод лінійного представлення найбільшого спільного дільника. Многочлен $h(x) = x^3 - 2x + 2$ є незвідним над полем $\mathbb{Q}$ за ознакою Айзенштайна, тому многочлени $g(x) = x^2 - 1$ і $h(x)$ взаємно прості. Знайдемо лінійне представлення їхнього найбільшого спільного дільника $d(x)$ (див. приклад 40.1).

Спочатку ділимо многочлен $h(x)$ на многочлен $g(x)$:

$$\begin{array}{rl|l} h(x) = x^3 - 2x + 2 & x^2 - 1 & = g(x) \\ \cline{3-3} x^3 - x & x & \\ \cline{2-2} -x + 2 & & = r_1(x) \end{array}$$

Далі ділимо $g(x)$ на $r_1(x)$:

$$\begin{array}{rl|l} g(x) = x^2 - 1 & -x + 2 & = r_1(x) \\ \cline{3-3} x^2 - 2x & -x - 2 & \\ \cline{2-2} 2x - 1 & & \\ 2x - 4 & & \\ \cline{2-2} 3 & & = d(x) \end{array}$$

Маємо:

$$\begin{cases} h(x) = x \cdot g(x) + r_1(x), \\ g(x) = (-x - 2)r_1(x) + d(x). \end{cases}$$

Звідси,

$$d(x) = g(x) - (-x - 2)r_1(x) = (-x - 2)(h(x) - x \cdot g(x)) = \\ = g(x)(-x^2 - 2x + 1) + h(x)(x + 2)$$

або

$$3 = g(x)(-x^2 - 2x + 1) + h(x)(x + 2).$$

Покладемо в останній рівності $x = \omega_1$. Враховуючи те, що ω_1 є коренем многочлена $h(x)$, тобто $h(\omega_1) = 0$, маємо: $3 = g(\omega_1)(-\omega_1^2 - 2\omega_1 + 1)$. Таким чином, щоб позбавитись ірраціональності в знаменнику заданого дробу, слід помножити його чисельник і знаменник на вираз $-\omega_1^2 - 2\omega_1 + 1$:

$$\frac{1}{\omega_1^2 - 1} = \frac{-\omega_1^2 - 2\omega_1 + 1}{(\omega_1^2 - 1)(-\omega_1^2 - 2\omega_1 + 1)} = \frac{-\omega_1^2 - 2\omega_1 + 1}{3}.$$

Спосіб III. Використаємо метод невизначених коефіцієнтів. Будемо шукати вираз, на який слід помножити чисельник і знаменник дробу у вигляді многочлена $s(\omega_1)$ з раціональними коефіцієнтами від змінної ω_1 степеня, меншого за степінь многочлена $h(x) = x^3 - 2x + 2$, тобто у вигляді $A\omega_1^2 + B\omega_1 + C$. Нехай $(\omega_1^2 - 1)(A\omega_1^2 + B\omega_1 + C) = 1$. Розкривши дужки: $A\omega_1^4 + b\omega_1^3 + (C - A)\omega_1^2 - B\omega_1 - C = 1$ і підставши замість ω_1^3 вираз $2\omega_1 - 2$ (із урахуванням (VIII.1)), одержимо:

$$(A + C)\omega_1^2 + (B - 2A)\omega_1 + (-2B - C) = 1.$$

Прирівняємо коефіцієнти при відповідних степенях:

$$\begin{cases} A + C = 0, \\ B - 2A = 0, \\ -2B - C = 1, \end{cases}$$

звідки $A = -\frac{1}{3}, B = -\frac{2}{3}, C = \frac{1}{3}$. Таким чином, $s(\omega_1) = -\frac{1}{3}\omega_1 - \frac{2}{3}\omega_1 + \frac{1}{3}$, а тому

$$\frac{1}{\omega_1^2 - 1} = \frac{-\frac{1}{3}\omega_1 - \frac{2}{3}\omega_1 + \frac{1}{3}}{(\omega_1^2 - 1)(-\frac{1}{3}\omega_1 - \frac{2}{3}\omega_1 + \frac{1}{3})} = \frac{-\frac{1}{3}\omega_1 - \frac{2}{3}\omega_1 + \frac{1}{3}}{1} = \frac{-\omega_1^2 - 2\omega_1 + 1}{3}.$$

Розв'язання в Maple. Для позбавлення від ірраціональності в знаменнику дробу просто обчислимо (за допомогою команди **evala**) значення $\frac{1}{\omega_1^2 - 1}$. Те, що ω_1 є коренем рівняння $x^3 - 2x + 2 = 0$, записуємо за допомогою RootOf:

```
> omega1:=RootOf(_Z^3-2*_Z+2):
```

Далі знаходимо частку:

```
> evala(1/(omega1^2-1));
```

$$\frac{1}{3} - \frac{2}{3}\,\mathrm{RootOf}(\_Z^3 - 2\,\_Z + 2) - \frac{1}{3}\,\mathrm{RootOf}(\_Z^3 - 2\,\_Z + 2)^2$$

Це означає, що $\frac{1}{\omega_1^2 - 1} = \frac{1}{3} - \frac{2}{3}\omega_1 - \frac{1}{3}\omega_1^2$.

Завдання 72. Позбавитись від ірраціональності в знаменнику дробу трьома способами:

1) методом симетричних многочленів;
2) методом лінійного представлення найбільшого спільного дільника;
3) методом невизначених коефіцієнтів.

72.1. $\frac{3}{\omega^3+2}$, де ω – один із коренів рівняння $x^4 - 3x + 1 = 0$.

72.2. $\frac{1}{\omega^2+1}$, де ω – один із коренів рівняння $x^3 + 2x^2 + 2 = 0$.

72.3. $\frac{4}{\omega^2+\omega}$, де ω – один із коренів рівняння $x^3 - x - 1 = 0$.

72.4. $\frac{2}{2-\omega^2}$, де ω – один із коренів рівняння $x^3 - x^2 - x + 2 = 0$.

72.5. $\frac{3}{2+\omega^2}$, де ω – один із коренів рівняння $x^3 - x^2 - 3x + 4 = 0$.

72.6. $\frac{4}{\omega-4}$, де ω – один із коренів рівняння $x^4 - x - 2 = 0$.

72.7. $\frac{2}{\omega^2+\omega+1}$, де ω – один із коренів рівняння $x^3 - 3x + 3 = 0$.

72.8. $\frac{3}{\omega-1}$, де ω – один із коренів рівняння $x^3 - 3x^2 + 5 = 0$.

72.9. $\frac{1}{\omega^3+\omega}$, де ω – один із коренів рівняння $x^4 - 3x + 1 = 0$.

72.10. $\frac{1}{\omega^2+3}$, де ω – один із коренів рівняння $x^3 - x + 5 = 0$.

72.11. $\frac{3}{\omega^3-2}$, де ω – один із коренів рівняння $x^4 - 2x + 1 = 0$.

72.12. $\frac{1}{\omega^2-\omega+1}$, де ω – один із коренів рівняння $x^3 - 3x + 4 = 0$.

72.13. $\frac{2}{\omega^2-\omega}$, де ω – один із коренів рівняння $x^3 + x + 1 = 0$.

72.14. $\frac{1}{\omega^2+2}$, де ω – один із коренів рівняння $x^3 - x + 2 = 0$.

72.15. $\frac{3}{\omega+2}$, де ω – один із коренів рівняння $x^3 - 5x + 6 = 0$.

72.16. $\frac{1}{\omega^2+1}$, де ω – один із коренів рівняння $x^3 - 2x^2 + 4 = 0$.

72.17. $\frac{4}{\omega+3}$, де ω – один із коренів рівняння $x^4 - x - 4 = 0$.

72.18. $\frac{5}{\omega-2}$, де ω – один із коренів рівняння $x^3 - 2x + 5 = 0$.

72.19. $\frac{1}{\omega^2+3}$, де ω – один із коренів рівняння $x^3 - 2x^2 + 2 = 0$.

72.20. $\frac{3}{2\omega-1}$, де ω – один із коренів рівняння $x^3 - 2x + 6 = 0$.

72.21. $\frac{1}{\omega^2-4}$, де ω – один із коренів рівняння $x^4 - 2x + 1 = 0$.

72.22. $\frac{\omega}{\omega+1}$, де ω – один із коренів рівняння $x^3 - x - 4 = 0$.

72.23. $\frac{4}{\omega^2+\omega}$, де ω – один із коренів рівняння $x^4 - x + 2 = 0$.

72.24. $\frac{1}{\omega^2+\omega}$, де ω – один із коренів рівняння $x^3 - 2x^2 + 5 = 0$.

72.25. $\frac{3}{2+\omega^2}$, де ω – один із коренів рівняння $x^3 - 2x^2 + 6 = 0$.

Приклад 73.1. Позбавитись від ірраціональності в знаменнику дробу $\frac{1}{\sqrt[3]{4}-\sqrt[3]{2}-1}$.

Розв'язання. Заданий дріб є значенням раціонального дробу $\frac{1}{x^2-x-1}$ при $x = \sqrt[3]{2}$, яке є коренем незвідного над полем $\mathbb{Q}$ многочлена $h(x) = x^3 - 2$. Многочлени $g(x)$ і $h(x)$ взаємно прості. Знайдемо лінійне представлення їхнього найбільшого спільного дільника $d(x)$:

$$\begin{array}{rl|l} h(x) = x^3 - 2 & & x^2 - x - 1 = g(x) \\ \cline{3-3} \underline{x^3 - x^2 - x} & & x + 1 \\ x^2 + x - 2 & & \\ \underline{x^2 - x - 1} & & \\ 2x - 1 = r_1(x) & & \end{array}$$

$$\begin{array}{rl|l} g(x) = x^2 - x - 1 & & 2x - 1 = r_1(x) \\ \cline{3-3} \underline{x^2 - \frac{1}{2}x} & & \frac{1}{2}x - \frac{1}{4} \\ -\frac{1}{2}x - 1 & & \\ \underline{-\frac{1}{2}x + \frac{1}{4}} & & \\ -\frac{5}{4} = d(x) & & \end{array}$$

Маємо:

$$\begin{cases} h(x) = (x+1)\cdot g(x) + r_1(x), \\ g(x) = (\frac{1}{2}x - \frac{1}{4})r_1(x) + d(x), \end{cases}$$

звідки

$$d(x) = g(x) - \left(\frac{1}{2}x - \frac{1}{4}\right) r_1(x) = g(x) - \left(\frac{1}{2}x - \frac{1}{4}\right)\Big(h(x) - (x+1)\cdot g(x)\Big) =$$
$$= g(x)\left(\frac{1}{2}x^2 + \frac{1}{4}x + \frac{3}{4}\right) + h(x)\left(-\frac{1}{2}x + \frac{1}{4}\right)$$

або

$$-\frac{5}{4} = g(x)\left(\frac{1}{2}x^2 + \frac{1}{4}x + \frac{3}{4}\right) + h(x)\left(-\frac{1}{2}x + \frac{1}{4}\right).$$

Покладемо в останній рівності $x = \sqrt[3]{2}$ і враховуючи, що $h(\sqrt[3]{2}) = 0$, маємо:

$$-\frac{5}{4} = g(\sqrt[3]{2})\left(\frac{1}{2}\sqrt[3]{4} + \frac{1}{4}\sqrt[3]{2} + \frac{3}{4}\right)$$

або

$$-5 = g(\sqrt[3]{2})\left(2\sqrt[3]{4} + 2\sqrt[3]{2} + 3\right).$$

Таким чином, щоб позбавитись від ірраціональності в знаменнику заданого дробу $\frac{1}{\sqrt[3]{4}-\sqrt[3]{2}-1} = \frac{1}{g(\sqrt[3]{2})}$, слід помножити його чисельник і знаменник на вираз $2\sqrt[3]{4} + 2\sqrt[3]{2} + 3$:

$$\frac{1}{\sqrt[3]{4} - \sqrt[3]{2} - 1} = \frac{1}{g(\sqrt[3]{2})} = \frac{2\sqrt[3]{4} + 2\sqrt[3]{2} + 3}{g(\sqrt[3]{2})(2\sqrt[3]{4} + 2\sqrt[3]{2} + 3)} = \frac{2\sqrt[3]{4} + 2\sqrt[3]{2} + 3}{-5}.$$

Розв'язання в Maple. Для позбавлення від ірраціональності в знаменнику дробу використаємо, як і в попередньому прикладі, команду **evala**. При цьому можна спочатку подати число $\alpha = \sqrt[3]{2}$ в RootOf-записі (як у Прикладі 72):

```
> alpha:=RootOf(_Z^3-2):
> evala(1/(alpha^2-alpha-1));
```

$$-\frac{3}{5} - \frac{1}{5}\,\mathrm{RootOf}(\_Z^3 - 2) - \frac{2}{5}\,\mathrm{RootOf}(\_Z^3 - 2)^2$$

а можна і не подавати:

```
> evala(1/(4^(1/3)-2^(1/3)-1));
```

$$-\frac{3}{5} - \frac{2^{(1/3)}}{5} - \frac{2\,2^{(2/3)}}{5}$$

Приклад 73.2. Позбавитись від ірраціональності в знаменнику дробу $\frac{1}{\sqrt[3]{5}-\sqrt{2}}$.

Розв'язання. Спосіб I. Заданий дріб будемо розглядати як значення раціонального дробу $\frac{f(x)}{g(x)} = \frac{1}{x-\sqrt{2}}$ при $x = \sqrt[3]{5}$, яке є коренем незвідного над полем $\mathbb{Q}$ многочлена $h(x) = x^3 - 5$. Многочлени $g(x)$ і $h(x)$ взаємно прості. Знайдемо лінійне представлення їхнього найбільшого спільного дільника $d(x)$:

$$\begin{array}{r|l} h(x) = x^3 - 5 & x - \sqrt{2} \\ \cline{2-2} \underline{x^3 - \sqrt{2}x^2} & x^2 + \sqrt{2}x + 2 \\ \sqrt{2}x^2 - 5 & \\ \underline{\sqrt{2}x^2 - 2x} & \\ 2x - 5 & \\ \underline{2x - 2\sqrt{2}} & \\ 2\sqrt{2} - 5 & \end{array} = g(x) = d(x)$$

Маємо:

$$h(x) = (x^2 + \sqrt{2}x + 2) \cdot g(x) + d(x),$$

звідки $d(x) = h(x) - (x^2 + \sqrt{2}x + 2) \cdot g(x)$ або

$$5 - 2\sqrt{2} = (x^2 + \sqrt{2}x + 2) \cdot g(x) - h(x).$$

Покладемо $x = \sqrt[3]{5}$. Тоді з урахуванням того, що $h(\sqrt[3]{5}) = 0$, маємо:

$$5 - 2\sqrt{2} = (\sqrt[3]{25} + \sqrt{2}\sqrt[3]{5} + 2) \cdot g(\sqrt[3]{5}).$$

Таким чином, чисельник і знаменник заданого дробу слід помножити на вираз $\sqrt[3]{25} + \sqrt{2}\sqrt[3]{5} + 2$:

$$\frac{1}{\sqrt[3]{5} - \sqrt{2}} = \frac{\sqrt[3]{25} + \sqrt{2}\sqrt[3]{5} + 2}{(\sqrt[3]{5} - \sqrt{2})(\sqrt[3]{25} + \sqrt{2}\sqrt[3]{5} + 2)} = \frac{\sqrt[3]{25} + \sqrt{2}\sqrt[3]{5} + 2}{5 - 2\sqrt{2}}.$$

Домножимо чисельник і знаменник одержаного дробу на вираз $5 + 2\sqrt{2}$, спряжений до знаменника:

$$\frac{1}{\sqrt[3]{5} - \sqrt{2}} = \frac{(\sqrt[3]{25} + \sqrt{2}\sqrt[3]{5} + 2)(5 + 2\sqrt{2})}{(5 - 2\sqrt{2})(5 + 2\sqrt{2})} = \\ = \frac{10 + 5\sqrt[3]{25} + 2\sqrt[3]{25}\sqrt{2} + 4\sqrt[3]{5} + 5\sqrt[3]{5}\sqrt{2} + 4\sqrt{2}}{17}.$$

Спосіб II. Застосуємо формулу скороченого множення:

$$x^6 - y^6 = (x - y)(x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5).$$

Маємо:

$$\frac{1}{\sqrt[3]{5}-\sqrt{2}} =$$
$$= \frac{\sqrt[3]{5}^5+\sqrt[3]{5}^4\sqrt{2}+\sqrt[3]{5}^3\sqrt{2}^2+\sqrt[3]{5}^2\sqrt{2}^3+\sqrt[3]{5}\sqrt{2}^4+\sqrt{2}^5}{(\sqrt[3]{5}-\sqrt{2})(\sqrt[3]{5}^5+\sqrt[3]{5}^4\sqrt{2}+\sqrt[3]{5}^3\sqrt{2}^2+\sqrt[3]{5}^2\sqrt{2}^3+\sqrt[3]{5}\sqrt{2}^4+\sqrt{2}^5)} =$$
$$= \frac{10+5\sqrt[3]{5}^2+2\sqrt[3]{5}^2\sqrt{2}+4\sqrt[3]{5}+5\sqrt[3]{5}\sqrt{2}+4\sqrt{2}}{(\sqrt[3]{5})^6-(\sqrt{2})^6} =$$
$$= \frac{10+5\sqrt[3]{25}+2\sqrt[3]{25}\sqrt{2}+4\sqrt[3]{5}+5\sqrt[3]{5}\sqrt{2}+4\sqrt{2}}{17}.$$

Розв'язання в Maple. Аналогічно до Прикладу 73.1 використовуємо команду **evala**:

```
> evala(1/(5^(1/3)-sqrt(2)));
```

$$\frac{10}{17}+\frac{4\sqrt{2}}{17}+\frac{5\sqrt{2}\,5^{(1/3)}}{17}+\frac{4\,5^{(1/3)}}{17}+\frac{5\,5^{(2/3)}}{17}+\frac{2\,5^{(2/3)}\sqrt{2}}{17}$$

Завдання 73. Позбавитись від ірраціональності в знаменнику дробу:

73.1. а) $\frac{1}{\sqrt[3]{4}+3\sqrt[3]{2}+1}$; б) $\frac{1}{\sqrt[3]{2}+\sqrt{3}+4}$.

73.2. а) $\frac{1}{\sqrt{7}+\sqrt[4]{7}-1}$; б) $\frac{1}{1+\sqrt[3]{2}-\sqrt{3}}$.

73.3. а) $\frac{1}{\sqrt[3]{9}+2\sqrt[3]{3}-1}$; б) $\frac{1}{\sqrt{5}-\sqrt[3]{2}}$.

73.4. а) $\frac{1}{1+\sqrt{2}-\sqrt[3]{2}}$; б) $\frac{1}{\sqrt[3]{3}-\sqrt[4]{2}}$.

73.5. а) $\frac{1}{2\sqrt[3]{4}-\sqrt[3]{2}+3}$; б) $\frac{1}{\sqrt[3]{7}-\sqrt[5]{8}}$.

73.6. а) $\frac{1}{\sqrt[3]{7}+\sqrt[3]{49}+5}$; б) $\frac{1}{\sqrt[3]{6}-\sqrt{5}}$.

73.7. а) $\frac{1}{\sqrt[3]{9}+3\sqrt[3]{3}+2}$; б) $\frac{1}{1+\sqrt[3]{2}-\sqrt{3}}$.

73.8. а) $\frac{1}{5\sqrt[3]{7}+\sqrt[3]{49}-3}$; б) $\frac{1}{\sqrt[5]{10}-1}$.

73.9. а) $\frac{1}{\sqrt[3]{25}+\sqrt[3]{5}+4}$; б) $\frac{1}{\sqrt[4]{3}+\sqrt[3]{4}}$.

73.10. а) $\frac{1}{\sqrt[3]{9}+2\sqrt[3]{3}+7}$; б) $\frac{1}{\sqrt{3}+\sqrt[3]{4}-2}$.

73.11. а) $\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+1}$;
б) $\frac{1}{\sqrt{3}-2\sqrt[3]{2}}$.

73.12. а) $\frac{1}{2\sqrt[3]{9}+\sqrt[3]{3}-5}$;
б) $\frac{1}{\sqrt[3]{3}+\sqrt[4]{4}}$.

73.13. а) $\frac{1}{\sqrt[3]{4}-2\sqrt[3]{2}+3}$;
б) $\frac{1}{2\sqrt{5}-\sqrt[3]{7}}$.

73.14. а) $\frac{1}{\sqrt[3]{6}+\sqrt[3]{36}+1}$;
б) $\frac{1}{\sqrt[3]{7}+\sqrt{8}+1}$.

73.15. а) $\frac{1}{\sqrt[4]{5}-\sqrt{5}+3}$;
б) $\frac{1}{\sqrt{5}-\sqrt[3]{4}}$.

73.16. а) $\frac{1}{3\sqrt[3]{5}+2\sqrt[3]{25}+1}$;
б) $\frac{1}{2\sqrt[4]{3}-\sqrt[4]{5}}$.

73.17. а) $\frac{1}{1+\sqrt[3]{2}+2\sqrt[3]{4}}$;
б) $\frac{1}{\sqrt[3]{9}+\sqrt{8}+7}$.

73.18. а) $\frac{1}{\sqrt[3]{25}-2\sqrt[3]{5}+4}$;
б) $\frac{1}{1+\sqrt[7]{7}}$.

73.19. а) $\frac{1}{1+\sqrt[3]{2}-\sqrt[3]{4}}$;
б) $\frac{1}{\sqrt[4]{7}+\sqrt[3]{5}}$.

73.20. а) $\frac{1}{3+\sqrt[3]{2}+5\sqrt[3]{4}}$;
б) $\frac{1}{\sqrt[3]{3}-\sqrt{2}}$.

73.21. а) $\frac{1}{3\sqrt[3]{2}-2\sqrt[3]{4}-1}$;
б) $\frac{1}{\sqrt{3}+3\sqrt[3]{2}}$.

73.22. а) $\frac{1}{\sqrt[3]{9}-\sqrt[3]{3}+2}$;
б) $\frac{1}{\sqrt{5}-\sqrt[4]{3}}$.

73.23. а) $\frac{1}{\sqrt[4]{8}+\sqrt[4]{2}+1}$;
б) $\frac{1}{\sqrt{\sqrt{3}+\sqrt[3]{3}}}$.

73.24. а) $\frac{1}{\sqrt[3]{25}+2\sqrt[3]{5}-1}$;
б) $\frac{1}{\sqrt[3]{4}+\sqrt{5}+6}$.

73.25. а) $\frac{1}{\sqrt[3]{7}+\sqrt[3]{49}+6}$;
б) $\frac{1}{\sqrt[3]{5}-\sqrt[4]{6}}$.

Таблиця простих чисел від 2 до 4057 та їхніх найменших первісних коренів.

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	863	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	2	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	1	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

Таблиця простих чисел від 2 до 4057 та їхніх найменших первісних коренів.

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	3	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3853	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	2	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	1	3881	13
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2641	3	2927	5	3259	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	6	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

Індекси

Просте число 3. Первісні корені: 2.

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Просте число 5. Первісні корені: 2, 3.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Просте число 7. Первісні корені: 3, 5.

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Просте число 11. Первісні корені: 2, 6, 7, 8.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6

Просте число 13. Первісні корені: 2, 6, 7, 11.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7	6							

Просте число 17. Первісні корені: 3, 5, 6, 7, 10, 11, 12, 14.

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Просте число 19. Первісні корені: 2, 3, 10, 13, 14, 15.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Просте число 23. Первісні корені: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

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							

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								

* Скрізь за основу таблиці індексів береться найменший первісний корінь.

Індекси

Просте число 29. Первісні корені: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Просте число 31. Первісні корені: 3, 11, 12, 13, 17, 21, 22, 24.

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23		19	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Просте число 37. Первісні корені: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 33, 35.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Просте число 41. Первісні корені: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Просте число 43. Первісні корені: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Основні позначення

$\mathbb{N}$ – множина всіх натуральних чисел;
$\mathbb{Z}$ – множина всіх цілих чисел;
$\mathbb{Z}^+$ – множина всіх цілих додатних чисел;
$n\mathbb{Z}$ – множина всіх цілих чисел, що діляться на n;
$\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ – кільце класів лишків за модулем n;
$\mathbb{Z}[i]$ – множина всіх цілих гаусових чисел;
$\mathbb{Q}$ – множина всіх раціональних чисел;
$\mathbb{Q}^+$ – множина всіх додатних раціональних чисел;
$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ – множина всіх відмінних від нуля раціональних чисел;
$\mathbb{R}$ – множина всіх дійсних чисел;
$\mathbb{R}^+$ – множина всіх додатних дійсних чисел;
$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ – множина всіх відмінних від нуля дійсних чисел;
$\mathbb{C}$ – множина всіх комплексних чисел;
$\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ – множина всіх відмінних від нуля комплексних чисел;
$\varnothing$ – порожня множина;
$\in$ – відношення належності;
$\notin$ – заперечення відношення належності;
$\subset$ – відношення строгого включення;
$\subseteq$ – відношення нестрогого включення;
$\vdots$ – відношення подільності;
$a \vdots b$ – a ділиться на b;
$\text{НСД}(a, b) = (a, b)$ – найбільший спільний дільник чисел a і b;
$\text{НСК}(a, b) = [a, b]$ – найменше спільне кратне чисел a і b;
$[x]$ – ціла частина числа x;
$\equiv$ – відношення конгруентності;
$a \equiv b \,(\mathrm{mod} I)$ – елементи a і b кільця K конгруентні за ідеалом I;
$a \equiv b \,(\mathrm{mod} m)$ – цілі числа a і b конгруентні за модулем m;
$\star, *, \circ$ – значки для позначення бінарних операцій;
$\cup$ – операція об'єднання множин;
$\cap$ – операція перетину множин;
$\setminus$ – операція віднімання множин;
$\forall, \exists$ – квантори загальності та існування;
$\varphi : A \to B$ – відображення множини A в (на) множину B;
$\varphi(a)$ – образ елемента a при відображенні $\varphi : A \to B$;
$\mathrm{Ker}\,\varphi$ – ядро гомоморфізму φ;
$\langle G; \cdot\rangle$ – група G із заданою на ній операцією $\cdot$;
$\langle K; +, \cdot\rangle$ – кільце K із заданими на ньому операціями $+$ і $\cdot$;
G – загальне позначення групи;
S_n – симетрична група n-го степеня;
A_n – знакозмінна група n-го степеня;
K – загальне позначення кільця;
K^* – мультиплікативна група кільця K;
P – загальне позначення поля;
$M_n\,(P)$ – множина всіх матриць n-го порядку над полем P;
$|A|$ – визначник матриці A;

$|G|$ – порядок групи G;
$|a|$ – порядок елемента a групи;
G/H – фактор-група групи G за підгрупою H;
K/I – фактор-кільце кільця K за ідеалом I;
$\overline{a} = K_a^{(m)}$ – клас лишків з представником a за модулем m;
$\langle a \rangle$ – головний ідеал кільця K, породжений елементом a;
$\langle a \rangle$ – циклічна група, породжена елементом a;
$K[x]$ – кільце многочленів від однієї змінної x над комутативним кільцем K з одиницею;
$P[x]$ – кільце многочленів від однієї змінної x над полем P;
$f(x) = a_n x^n + a_{n-1} + \ldots + a_1 x + a_0$, $a_i \in K$, – канонічна форма запису многочлена від однієї змінної x над областю цілісності K;
$\deg f$ – степінь многочлена $f(x)$;
$K[x_1, x_2, \ldots, x_n]$ – кільце многочленів від n змінних $x_1, x_2, \ldots, x_n$ над комутативним кільцем K з одиницею;
$P[x_1, x_2, \ldots, x_n]$ – кільце многочленів від n змінних $x_1, x_2, \ldots, x_n$ над полем P;
НСД$(f, g) = (f, g)$ – найбільший спільний дільник многочленів $f(x)$ і $g(x)$;
НСК$(f, g) = [f, g]$ – найменше спільне кратне многочленів $f(x)$ і $g(x)$;
$f'(x)$ – похідна многочлена $f(x)$;
$\sigma_1, \sigma_2, \ldots, \sigma_n$ – елементарні симетричні многочлени від n змінних;
$f(x), F_0(x), F_1(x), \ldots, F_m(x)$ – ряд многочленів Штурма;
$P(\alpha)$ – просте розширення поля P за допомогою числа α.

Список рекомендованої літератури

Алгебра і теорія чисел

[1] *Требенко Д.Я., Требенко О.О.* Алгебра і теорія чисел: У 2 ч. – К.: НПУ імені М.П. Драгоманова, 2009. – Ч.1. – 420 с. ISBN 978-966-660-551-4

[2] *Требенко Д.Я., Требенко О.О.* Збірник індивідуальних розрахункових завдань з курсу „Алгебра і теорія чисел": У 2 ч. – К.: НПУ імені М.П.Драгоманова, 2010. – Ч.1. – 172 с. (1-ше вид. 2009 р.) ISBN 978-966-660-657-3

[3] *Требенко Д.Я., Требенко О.О.* Збірник індивідуальних розрахункових завдань з курсу „Алгебра і теорія чисел": У 2 ч. – К.: НПУ імені М.П.Драгоманова, 2011. – Ч.2. – 120 с. (1-ше вид. 2009 р.) ISBN 978-966-660-689-4

[4] *Завало С.Т. Курс алгебри.* – К.: Вища шк., 1985. – 500 с.

[5] *Завало С.Т., Костарчук В.М., Хацет Б.І.* Алгебра і теорія чисел: В 2-х ч. – К.: Вища шк. Головне вид-во, 1974. – Ч.1. – 464 с.

[6] *Завало С.Т., Костарчук В.М., Хацет Б.І.* Алгебра і теорія чисел: В 2-х ч. – К.: Вища шк. Головне вид-во, 1976. – Ч.2. – 384 с.

[7] *Завало С.Т., Левіщенко С.С., Пилаєв В.В., Рокицький І.О.* Алгебра і теорія чисел: В 2-х ч. – К.: Вища шк. Головне вид-во, 1983. – Ч.1. – 232 с.

[8] *Завало С.Т., Левіщенко С.С., Пилаєв В.В., Рокицький І.О.* Алгебра і теорія чисел: В 2-х ч. – К.: Вища шк. Головне вид-во, 1986. – Ч.2. – 264 с.

[9] *Кострикин А.И.* Введение в алгебру. – М.: Наука, 1977. – 496 с.

[10] *Куликов Л.Я.* Алгебра и теория чисел. М.: Высш. шк., 1979. – 560 с.

[11] *Курош А.Г.* Курс высшей алгебры. – М.: Наука, 1971. – 432 с.

[12] *Окунев Л.Я.* Сборник задач по высшей алгебре. – М.: Просвещение, 1964. – 184 с.

[13] *Фаддеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. – М.: Наука, 1977. – 288 с.

СКА Maple

[14] *Говорухин В., Цыбулин Б.* Компьютер в математическом исследовании. – Питер, 2001. – 619 с. ISBN 5-272-00220-2

[15] *Monagan M.B., Geddes K.O., Heal K.M., Labahn G., Vorkoetter S.M., McCarron J., DeMarco P.* Maple. Introductory Programming Guide. – Maplesoft, a division of Waterloo Maple Inc. 2007. - 387 p. ISBN 1-894511-76-X

[16] *Дьяконов В.П.* Maple 10/11/12/13/14 в математических расчетах. – Москва: ДМК Пресс, 2011. - 800 с. ISBN 978-5-94074-751-2

Навчальне видання

Требенко Дмитро Якович
Требенко Оксана Олександрівна

Використання системи комп'ютерної алгебри Maple при вивченні курсу „Алгебра і теорія чисел"

Віддруковано з оригіналів.

Видавництво Національного педагогічного університету
імені М.П. Драгоманова. 01601, м. Київ-30, вул. Пирогова, 9
Свідоцтво про реєстрацію № 1101 від 29.10.2002.
(044) 239-30-26.