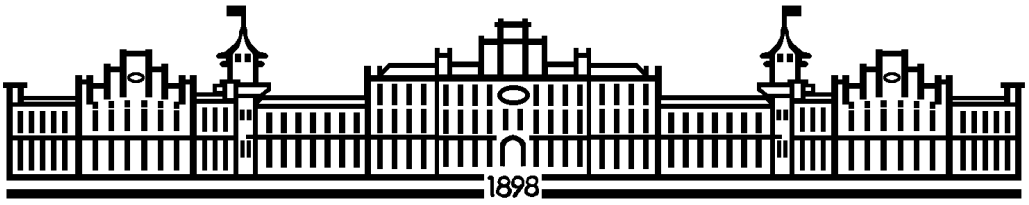


МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«Київський політехнічний інститут»

Т.В. Авдєєва В.М. Горбачук

АЛГЕБРА

ОСНОВИ АЛГЕБРАЇЧНИХ СТРУКТУР

Навчальний посібник

Київ
НТУУ «КПІ»
2015

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«Київський політехнічний інститут»

Т.В. Авдєєва В.М. Горбачук

АЛГЕБРА

ОСНОВИ АЛГЕБРАЇЧНИХ СТРУКТУР

Навчальний посібник

“Рекомендовано”
Методичною радою НТУУ “КПІ”

Київ
НТУУ «КПІ»
2015

УДК 512.8 (076)
512 (075.8)
ББК 22.14

Гриф надано методичною радою НТУУ «КПІ»
(протокол № 5 від 8 червня 2015 р.)

Рецензенти: ***О.Г. Ганюшкін,*** канд. фіз.-мат. наук, доцент.,
Київський національний університет
Імені Тараса Шевченка

В*.В. Сергійчук**,* доктор фіз.-мат. наук,
провідний науковий співробітник
Інституту математики НАН України

Відповідальний
редактор: ***Н.О. Вірченко,*** д-р фіз.-мат. наук, проф.,
Національний технічний університет України
«Київський політехнічний інститут»

Алгебра. Основи алгебраїчних структур. Навчальний посібник
/Т.В. Авдєєва, В.М. Горбачук.- К.: НТУУ «КПІ», 2015. – 79 с. – Бібліогр.:
с. 79. –100 пр.

В навчально-методичному посібнику викладено короткі теоретичні відомості з теорії груп, кілець і полів, даються приклади розв’язування задач з відповідних розділів. Наводяться варіанти індивідуальних завдань для студентів.

Призначений для студентів фізико-математичного факультету НТУУ “ КПІ ”, може бути використаний також в інших університетах при вивчені курсу “ Алгебри і теорії чисел ”.

УДК 512.8 (076)
512 (075.8)
ББК 22.14

ЗМІСТ

Передмова

Посібник є методичним забезпеченням курсу алгебри, який, як відомо, є невід'ємною частиною фундаментальної підготовки для студентів спеціальності "Математика".

Даний посібник містить короткі теоретичні відомості та велику кількість прикладів, вправ і задач, необхідних для виконання типових розрахунків з цього курсу. Наводяться також наближені варіанти планових контрольних та самостійних робіт і перелік питань для колоквіумів.

Посібник розрахований на студентів фізико-математичного та інших факультетів для використання в навчальному процесі, пов'язаному з алгеброю. Цей посібник може бути корисним для організації самостійної роботи студентів університетів та вищих педагогічних навчальних закладів, які вивчають цей курс

ПРОГРАМА КУРСУ

1 семестр

Тема 1. Групи, кільця, поля

Групи, основні властивості груп, підгрупи, їх властивості, циклічні групи, групи симетрії, знакозмінна група, групи підстановок, ізоморфізм груп, теорема Келі, розклад групи за підгрупою, терема Лагранжа, теореми Сілова.

Кільця, основні властивості кілець, кільця з одиницею, дільники нуля, гомоморфізм кілець.

Поля, поле класів лишків за простим модулем, властивості полів, підполе.

Тема 3. Поліноми, симетричні поліноми

Кільце многочленів над областю цілісності, теорія подільності многочленів, схема Горнера, незвідні многочлени, канонічний розклад многочлена, корені многочленів, метод Штурма, критерій Айзенштайна, многочлени з багатьма змінними, симетричні многочлени, основна теорема про симетричні многочлени.

Розділ 1. АЛГЕБРАЇЧНІ СТРУКТУРИ

1.1. Бінарна операція. Напівгрупа. Група

Нехай M – довільна непорожня множина елементів. **Бінарною алгебраїчною операцією** *(*або просто **бінарною операцією***)* на множині M називається довільне відображення декартового квадрата множини M на множину M, тобто $\tau : M \times M \to M$. Інакше кажучи, під бінарною операцією на множині M розуміють закон $(*)$, за яким будь-яким двом (різним чи однаковим) елементом a і b множини M, взятим у певному порядку, ставиться у відповідність єдиний елемент $a * b$ множини M.

Бінарна операція $(*)$ на множині M називається **асоціативною**, якщо для будь-яких трьох елементів a, b *і* c множини M справджується рівність $(a * b) * c = a * (b * c)$. Операція називається **неасоціативною**, якщо в множині M існує хоча б одна трійка елементів a, b *і* c, для яких $(a * b) * c \neq a * (b * c)$.

Бінарна операція $(*)$ називається **комутативною**, якщо для будь-яких двох елементів a і b множини M справджується рівність $a * b = b * a$. Операція називається **некомутативною**, якщо в множині M існує хоча б одна пара елементів a і b, для яких $a * b \neq b * a$.

Елемент $\eta \in M$ називається **нейтральним елементом** відносно операції $(*)$, якщо для будь-якого елемента a з множини M справджуються рівності $a * \eta = \eta * a = a$. Нейтральний елемент називають також **одиницею** e.

Нехай у множині M з бінарною операцією $(*)$ є нейтральний елемент η. Елемент $a' \in M$ називається **симетричним** елементу $a \in M$ (або оберненим до a), якщо $a * a' = a' * a = \eta$.

Множина M з бінарною операцією $(*)$ називається **напівгрупою**, якщо операція $*$ асоціативна. Якщо напівгрупа $(M,*)$ містить нейтральний елемент, то її називають напівгрупою з одиницею або **моноїдом**.

У напівгрупі з одиницею η для кожного елемента існує щонайбільше один обернений елемент. Справді, якщо $a*a'=a'*a=\eta$ і $a*a''=a''*a=\eta$, то маємо такий ланцюжок рівностей:

$$a'=a'*\eta=a'*(a*a'')=(a'*a)*a''=\eta*a''=a''.$$

Далі обернений до a елемент (якщо він існує) ми позначатимемо через a^{-1}. Елемент, для якого існує обернений, називається **оборотним**.

Напівгрупа з одиницею, в якій всі елементи оборотні, називається **групою**. Іншими словами, множина G з бінарною операцією $(*)$ називається **групою**, якщо виконуються три наступні умови:

1) операція $(*)$ асоціативна;
2) в G існує нейтральний елемент η;
3) для кожного елемента $a\in G$ в множині G існує обернений до a елемент a'.

Зауважимо, що множина G повинна бути замкненою відносно операції $*$ (за означенням бінарної операції).

Якщо операцію в групі G називають множенням, то групу називають **мультиплікативною** (від лат. *multipliko* – множити), якщо G утворює групу відносно звичайного додавання, то групу називають **адитивною** (від лат. *additio* –додавати).

Якщо бінарна операція $(*)$ комутативна, то **група** G називається **комутативною або абелевою**. Групу, що містить скінчену кількість елементів, називають **скінченною**. Кількість елементів скінченної групи називають її **порядком**. Групу, що не є скінченною, називають **нескінченною**.

Наведемо деякі приклади груп.

Множина Z цілих чисел утворює групою відносно додавання. Справді, додавання цілих чисел асоціативне, нейтральним елементом для додавання буде число 0, а протилежним до a – число $-a$. Зауважимо, що ця група буде комутативною.

Множина $\{1,-1\}$ утворює комутативну групу відносно множення.

Множина $GL_n(R)$ всіх невироджених матриць n-го порядку з дійсними елементами є групою відносно множення матриць. Дійсно, якщо матриці A і $B-$ невироджені, тобто $\det A \neq 0$, $\det B \neq 0$, то $\det(AB) = \det A \cdot \det B \neq 0$. Отже, множення є бінарною операцією на множині $GL_n(R)$. Ця операція є асоціативною, оскільки асоціативним є множення довільних квадратних матриць. Нейтральним елементом буде одинична матриця E_n, і для кожної невиродженої матриці A існує невироджена обернена матриця A^{-1}.

Зауваження: часто буває, що бінарна операція $(*)$ початково визначена на множині, більшій за M. Тому перш ніж з'ясовувати, чи буде множина M утворювати відносно $(*)$ групу або напівгрупу, потрібно пересвідчитись, чи можна операцію $(*)$ обмежити на множину M, тобто чи для довільної пари елементів $a,b \in M$ результат $a*b$ також належить M. Якщо це так, то кажуть, що **множина** M **замкнена** відносно операції$(*)$. Наприклад, сума двох непарних чисел завжди є парним числом, тому множина непарних чисел не є замкненою відносно операції додавання. Іншими словами, додавання не є бінарною операцією на множині непарних чисел.

Вкажемо деякі властивості груп. При цьому операцію будемо називати множенням і позначати символом $*$, а результат $a*b$ її застосування до елементів a і b називати добутком a і b.

Властивість 1. Для довільних цілих чисел m і n та елемента a групи G справджуються рівності $a^m * a^n = a^{m+n}$ та $\left(a^m\right)^n = a^{m \cdot n}$.

Властивість 2. Для довільних елементів a і b групи G кожне з рівнянь $a * x = b$ і $y * a = b$ має єдиний розв'язок.

Властивість 3. Для будь-яких елементів a,b,c групи G з рівності $a * b = a * c$ випливає рівність $b = c$, а з рівності $a * c = b * c$ випливає рівність $a = b$.

Множина S_n всіх взаємно однозначних перетворень множини $S = \{1,2,...,n\}$ утворює групу відносно суперпозиції відображень. Дійсно, суперпозиція відображень є асоціативною, нейтральним елементом для суперпозиції буде тотожне відображення $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, а оберненим до перетворення $\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ буде перетворення $\varphi^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$. Взаємно однозначні перетворення множини S називають також **підстановками** або **підстановками n-го степеня**. Групу S_n називають **симетричною групою степеня n.**

Відомо, що довільну підстановку φ із S_n можна розкласти в добуток взаємно незалежних циклів, причому такий розклад єдиний з точністю до порядку слідування множників. Наприклад,

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 3 & 8 & 9 & 10 & 2 & 4 & 6 & 1 \end{pmatrix} \in S_{10}$$

може бути записаний $\varphi = (1\,5\,9\,6\,10)(2\,7)(3)(4\,8)$ або, опускаючи цикл довжини один, $\varphi = (1\,5\,9\,6\,10)(2\,7)(4\,8)$. Якщо в підстановки φ всі точки, крім двох, є нерухомими, тобто $\varphi = (i\ j)$, то її називають **транспозицією**. Відомо, що кожну підстановку n-го степеня можна подати у вигляді добутку скінченної кількості транспозицій. Кажуть, що в підстановці

$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$ числа k_i та k_j утворюють **інверсію**, якщо $i < j$, але $k_i > k_j$. Так для підстановки $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 3 & 8 & 9 & 10 & 2 & 4 & 6 & 1 \end{pmatrix}$ числа 5 та 4 в нижньому рядку утворюють інверсію, а 7 та 8 – ні. Для вказаної вище підстановки число 2 утворює 6 інверсій (у нижньому рядку перед 2 стоять числа $5,7,3,8,9,10$ та всі вони більше за 2), кількість інверсій числа 9 дорівнює 0 (у нижньому рядку перед 9 стоять числа $5,7,3,8$, але більших за 9 серед них немає). Підстановка називається **парною**, якщо загальна кількість інверсій її чисел є парною, і називається **непарною**, якщо загальна кількість інверсій непарна. Для вказаної вище підстановки загальна кількість інверсій дорівнює $9+6+2+5+0+4+0+0+0+0=26$, отже, підстановка є парною.

Відомо, що у групі S_n кількість парних підстановок дорівнює кількості непарних підстановок. Можна довести, що множина всіх парних підстановок групи S_n утворює групу відносно множення (добуток парних підстановок є парною підстановкою, обернена до парної підстановки є парною підстановкою, тотожна підстановка також є парною). Цю групу називають **знакозмінною групою n-го степеня** та позначають A_n. Зауважимо, що множина B_n всіх непарних підстановок групи S_n не утворює групу відносно множення, оскільки добуток двох непарних підстановок є парною підстановкою.

Непорожня підмножина H групи G називається **підгрупою** групи G (позначають $H < G$), якщо вона сама утворює групу відносно тієї самої операції, що визначена на G. Наприклад, знакозмінна група A_n степеня n є підгрупою симетричної групи S_n, а множина $SL_n(R)$ квадратних матриць з визначником $\det A = 1$ є підгрупою групи $GL_n(R)$ невироджених матриць.

Із означення векторного простору випливає, що множина векторів цього простору утворює комутативну групу відносно додавання векторів.

Для того, щоб з'ясувати, чи є непорожня підмножина підгрупою можна скористатися наступною теоремою:

Критерій підгрупи (через дві умови): Непорожня підмножина H групи G буде підгрупою тоді й лише тоді, коли вона замкнена відносно множення (тобто $a * b \in H$ для довільних $a,b \in H$) і взяття оберненого елемента (тобто $a^{-1} \in H$ для кожного $a \in H$).

Сама група G та множина $E = \{e\}$, яка складається лише з нейтрального елемента групи, є **тривіальними** (найпростішими) підгрупами групи G. Усі інші підгрупи називаються нетривіальними. Підгрупа H групи G називається **власною** підгрупою, якщо $H \neq G$. Власна підгрупа H групи G називається **максимальною підгрупою** в G, якщо не існує жодної іншої власної підгрупи групи G, яка б містила підгрупу H. Власна підгрупа $H \neq E$ групи G називається **мінімальною підгрупою** в G, якщо не існує жодної іншої власної підгрупи групи G, відмінної від групи $\{e\} = E$, яка б містилася у підгрупі H.

Приклад 1. З'ясувати, чи утворює групу відносно операції додавання множина всіх цілих чисел, які кратні 3.

Нехай $G-$ множина всіх цілих чисел, які кратні 3, тобто $G = \{3k : k \in Z\} = \{0,\pm 3,\pm 6,....\}$. Оскільки $3k + 3m = 3(k + m)$, тобто сума чисел, кратних 3, саме є кратною 3, і $-3k = 3 \cdot (-k)$, тобто число, протилежне кратному 3, саме є кратним 3, то множина цілих чисел, кратних 3, є замкненою відносно додавання і взяття протилежного елемента. Тому вона утворює підгрупу групи цілих чисел, а отже, є групою. Групу всіх цілих чисел, які кратні 3, позначатиме $3Z$.

Приклад 2. З'ясувати, чи утворює групу відносно операції множення множина всіх дійсних кососиметричних матриць.

Квадратна матриця A називається кососиметричною, якщо $A^T = -A$. Зрозуміло, що всі діагональні елементи кососиметричної матриці дорівнюють нулю. Неважко переконатися, що множина кососиметричних матриць не утворює групу за множенням, оскільки до множини не попадає одинична матриця. Зауважимо також, що добуток двох кососиметричних матриць може бути матрицею не кососиметричною. Наприклад,

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

Твердження. Якщо H_1, H_2 підгрупи групи G, то їхній перетин $H_1 \bigcap H_2$ також є підгрупою групи G.

Це твердження узагальнюється на будь-яке число (скінченне чи нескінченне) підгруп групи G.

Нехай $H < G$ і $a \in G$. **Правим суміжним класом** Ha групи G за підгрупою H називається множина $Ha = \{ha : h \in H\}$. Лівий суміжний клас визначаємо аналогічно: $aH = \{ah : h \in H\}$. Легко перевірити, що два правих суміжних класи за підгрупою H або не перетинаються або збігаються (як множини). Таким чином, праві суміжні класи за підгрупою H утворюють розбиття групи G на класи суміжності. Зрозуміло, що всі суміжні класи за підгрупою H мають однакову кількість елементів, яка збігається з кількістю елементів підгрупи H. Два елементи a і b групи G лежать в одному суміжному класі за підгрупою H тоді й лише тоді, коли $ab^{-1} \in H$. Кількість (правих) суміжних класів називають **індексом підгрупи** H у групі G і позначають $|G : H|$. Справедлива

Теорема Лагранжа: Нехай G – скінченна група, H – підгрупа групи G. Тоді $|G| = |G : H| \cdot |H|$.

Зокрема, порядок підгрупи скінченної групи є дільником порядку групи.

Завдання 1. З'ясувати, чи буде групою

1. Множина всіх дійсних симетричних матриць порядку n відносно множення.
2. Множина всіх дійсних кососиметричних матриць порядку n відносно додавання.
3. Множина всіх дійсних невироджених матриць порядку n відносно множення.
4. Множина всіх дійсних діагональних матриць порядку n відносно додавання.
5. Множина всіх дійсних верхніх трикутних матриць порядку n відносно множення.
6. Множина всіх дійсних матриць порядку n із фіксованим визначником d відносно множення.
7. Множина ненульових дійсних матриць вигляду $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, де число число a – фіксоване, відносно множення.
8. Множина ненульових дійсних матриць вигляду $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, відносно множення.
9. Множина ненульових дійсних матриць вигляду $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, відносно додавання.
10. Множина матриць вигляду $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, де $x \in R$, відносно множення.
11. Множина матриць вигляду $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, де $x \in R$, відносно додавання.
12. Множина матриць вигляду $\begin{pmatrix} m & m-1 \\ 1 & 1 \end{pmatrix}$, де $m \in Z$, відносно множення.
13. Множина матриць вигляду $\begin{pmatrix} m & m-1 \\ 1 & 1 \end{pmatrix}$, де $m \in Z$, відносно додавання.

14. Множина всіх відображень множини $M = \{1,2,\ldots,n\}$ у себе відносно суперпозиції відображень.
15. Множина всіх ін'єктивних відображень множини $M = \{1,2,\ldots,n\}$ у себе відносно суперпозиції відображень.
16. Множина всіх сюр'єктивних відображень множини $M = \{1,2,\ldots,n\}$ у себе відносно суперпозиції відображень.
17. Множина всіх бієктивних відображень множини $M = \{1,2,\ldots,n\}$ у себе відносно суперпозиції відображень.
18. Множина степенів дійсного фіксованого числа $a \neq 0$ з цілими показниками відносно операції множення.
19. Множина всіх комплексних коренів фіксованого степеня n з одиниці відносно операції множення.
20. Множина всіх комплексних коренів усіх степенів з одиниці відносно операції множення.
21. Множина комплексних чисел із фіксованим модулем r відносно операції множення.
22. Множина ненульових комплексних чисел, модуль яких не перевищує даного числа r, відносно операції множення.
23. Множина ненульових комплексних чисел, розташованих на променях, що виходять із початку координат та утворюють з променем $0x$ кути $\varphi_1, \varphi_2, \ldots, \varphi_n$, відносно операції множення.
24. Множина всіх непарних підстановок множини $M = \{1,2,\ldots,n\}$ відносно операції множення.
25. Множина підстановок $\{E, (12)(34), (13)(24), (14)(23)\}$ відносно операції множення.
26. Множина матриць вигляду $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, відносно множення.
27. Множина всіх дійсних невироджених матриць порядку n відносно додавання.

28. Множина всіх дійсних невироджених діагональних матриць порядку n відносно множення.
29. Множина всіх дійсних невироджених діагональних матриць порядку n відносно додавання.
30. Множина підстановок $\{E,(12),(13),(14),(23),(24),(34)\}$ відносно операції множення.

1.2. Таблиця Келі

Нехай є множина $G=\{a_1,a_2,\ldots,a_n\}$ з бінарною операцією $(*)$. **Таблицею Келі** або таблицею множення цієї множини називається таблиця яка складається з n стовпчиків та n рядків. У рядки і стовпчики таблиці послідовно нумеруються елементами $a_1,a_2,\ldots,a_n$ множини G. Якщо $(G,*)$ – група, то за елемент a_1, як правило, беруть нейтральний елемент e групи. На перетині рядка, поміченого елементом a_i, і стовпчика, поміченого елементом a_j, записують результат $a_i * a_j$.

Приклад 1. Таблиця Келі для множини $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$, з операціями додавання і множення мають відповідно вигляд

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

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

Приклад 2. Таблиця Келі для групи

$GL_2(Z_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ має вигляд:

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

Зауваження. а) якщо операція $(*)$ комутативна, то її таблиця Келі є симетричною відносно головної діагоналі.

b) якщо для операції $(*)$ існує нейтральний елемент e, то елемент a_i буде оборотним зліва (справа) тоді й лише тоді, коли у стовпчику (рядку), поміченому елементом a_i, зустрічається нейтральний елемент.

c) у випадку групи в кожному рядку і в кожному стовпчику таблиці Келі всі елементи групи зустрічаються по одному разу (немає повторів).

Завдання 2. Скласти табличку Келі групи

1. Z_7. 2. C_6. 3. D_3. 4. $T_2(Z_3)$. 5. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix} \right\rangle$.

6. Z_6. 7. C_8. 8. S_3. 9. $\langle (136)(45) \rangle$. 10. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \right\rangle$.

11. D_4. 12. Z_9^*. 13. Q_8. 14. $T_3(Z_2)$. 15. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \right\rangle$.

16. $\langle (154)(26) \rangle$. 17. Z_{15}^*. 18. Z_{20}^*. 19. Z_{30}^*. 20. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} \right\rangle$.

21. Z_{16}^*. 22. Z_7^*. 23. $\langle (1352)(46) \rangle$. 24. C_7.

25. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 4 & 6 & 1 \end{pmatrix} \right\rangle$. 26. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix} \right\rangle$.

27. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 1 & 4 \end{pmatrix} \right\rangle$. 28. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 6 & 1 \end{pmatrix} \right\rangle$.

29. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix} \right\rangle$. 30. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix} \right\rangle$.

1.3. Порядок елемента групи

Нехай G - мультиплікативна група. **Порядком елемента** a групи G називається найменше натуральне число n (найменший додатний показник n), для якого $a^n = e$. Якщо такого показника не існує, то a називається **елементом нескінченого порядку**.

Твердження 1: Порядок елемента дорівнює кількості різних степенів цього елемента.

Якщо елемент a має порядок n, то пишуть $|a| = n$.

Якщо a елемент n–ого порядку, то породжена ним циклічна підгрупа $\langle a \rangle$ складається з таких елементів: $e = a^0, a, a^2, \ldots, a^{n-1}$.

Приклади. 1. Елемент $i \in C^*$ має порядок 4.

2. Елемент $g = \cos\frac{5\pi}{8} + i\sin\frac{5\pi}{8}$ із C^* є елементом порядку 16, оскільки $g^8 = -1,\ g^{16} = 1$.

3. Елемент 2 з R^* є елементом нескінченного порядку (для довільного натурального n $2^n \neq 1$).

4. Елемент $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ із $GL_2(Z_2)$ є елементом порядку 2: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

5. Елемент $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in S_5$ є елементом порядку 4:

$$g^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix},\ g^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix},$$

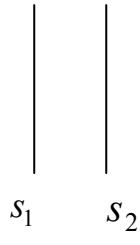
$$g^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Твердження 2: Порядок підстановки дорівнює найменшому спільному кратному довжин незалежних циклів цієї підстановки.

Зауважимо, що порядок добутку ab елементів a і b, взагалі кажучи, не визначаються порядками елементів a і b.

Приклади.

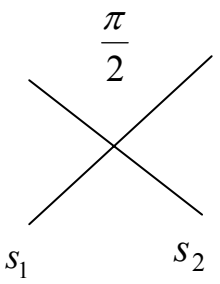
1. Розглянемо дві осьові симетрії з паралельними осями. Порядок кожної осьової симетрії дорівнює 2. Якщо ми розглянемо добуток $s_1 s_2$, то отримаємо паралельне перенесення, яке має нескінченний порядок.



$$|s_1| = |s_2| = 2,$$

$$|s_1 s_2| = \infty$$

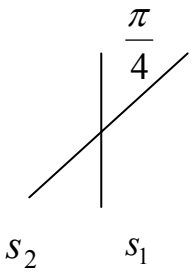
2. Розглянемо дві осьові симетрії з осями, що перетинаються під кутом 90°. Порядок кожної осьової симетрії дорівнює 2, тобто $|s_1| = |s_2| = 2$. Добуток $s_1 s_2$ є поворотом на кут 180° навколо точки перетину осей і має порядок 2.



$$|s_1| = |s_2| = 2,$$

$$|s_1 s_2| = 2.$$

3. Розглянемо дві осьові симетрії з осями, що перетинаються під кутом 45°. Порядок кожної осьової симетрії дорівнює 2. Але цього разу добуток $s_1 s_2$ є поворотом на 90° навколо точки перетину осей і має порядок 4.



$$|s_1| = |s_2| = 2,$$

$$|s_1 s_2| = 4.$$

4. Елемент $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 10 & 9 & 6 & 7 & 12 & 2 & 8 & 1 & 11 & 5 & 4 \end{pmatrix} \in S_{12}$ перепишемо у вигляді добутку незалежних циклів $g = (1\,3\,9)(2\,10\,11\,5\,7)(4\,6\,12)(8)$. Маємо чотири незалежних цикла та $HCK(3,5,3,1) = 15$. Отже, елемент має порядок 15.

Завдання 3. Знайти порядок елемента групи

1. a) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 6 & 1 & 5 & 8 & 7 \end{pmatrix} \in S_8$; b) $g = \frac{\sqrt{3}}{2} - \frac{1}{2} i \in C^*$.

2. a) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 6 & 2 & 5 & 8 & 7 \end{pmatrix} \in S_8$; b) $g = -\frac{\sqrt{3}}{2} + \frac{1}{2} i \in C^*$.

3. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&7&4&6&2&5&8&3\end{pmatrix}\in S_8$; b) $g=\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\in C^*$.

4. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\7&3&4&6&2&5&8&1\end{pmatrix}\in S_8$; b) $g=-\frac{\sqrt{3}}{2}-\frac{1}{2}i\in C^*$.

5. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&3&6&2&5&8&7\end{pmatrix}\in S_8$; b) $g=-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\in C^*$.

6. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&3&7&6&2&5&8&4\end{pmatrix}\in S_8$; b) $g=2-i\in C^*$.

7. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&5&4&6&2&3&8&7\end{pmatrix}\in S_8$; b) $g=-i\in C^*$.

8. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&3&4&6&1&5&2&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{6\pi}{5}+i\sin\frac{6\pi}{5}\in C^*$.

9. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&6&2&5&8&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{2\pi}{7}+i\sin\frac{2\pi}{7}\in C^*$.

10. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&6&4&2&5&3&1\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{pmatrix}\in GL_4(R)$.

11. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&6&2&5&3&7\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}0&i\\1&0\end{pmatrix}\in GL_2(C)$.

12. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&3&2&7&1&5&8&6\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}-1&a\\0&1\end{pmatrix}\in GL_2(R)$.

13. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&6&5&8&2&7\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\in GL_2(Z)$.

14. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&3&7&6&4&5&8&2\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}\in GL_2(Z)$.

15. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&1&6&7&5&8&4\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}-1&0&0\\0&0&1\\0&-1&0\end{pmatrix}\in GL_3(Z)$.

16. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&4&6&2&5&3&1\end{pmatrix}\in S_8$; b) $g=\frac{1-i\sqrt{3}}{2}\in C^*$.

17. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&6&3&5&2&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\in C^*$.

18. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&8&4&6&1&5&7&3\end{pmatrix}\in S_8$; b) $g=\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\in C^*$.

19. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&7&5&8&2&6\end{pmatrix}\in S_8$; b) $g=-\frac{1}{2}+\frac{\sqrt{3}}{2}i\in C^*$.

20. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&6&5&8&2&7\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}-1&0&0\\0&0&1\\0&1&0\end{pmatrix}\in GL_3(Z)$.

21. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&8&6&1&5&7&4\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}a&1\\-1&0\end{pmatrix}\in GL_2(R)$.

22. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&4&6&2&5&3&1\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\in GL_3(Z)$.

23. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&6&7&5&3&2\end{pmatrix}\in S_8$; b) $g=i\in C^*$.

24. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&4&3&6&1&5&8&7\end{pmatrix}\in S_8$; b) $g=\begin{pmatrix}1&0\\a&-1\end{pmatrix}\in GL_2(Z)$.

25. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&4&1&6&5&8&2&7\end{pmatrix}\in S_8$; b) $g=-\frac{1}{2}-\frac{\sqrt{3}}{2}i\in C^*$.

26. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&3&4&6&1&7&2&5\end{pmatrix}\in S_8$; b) $g=\cos\frac{3\pi}{5}+i\sin\frac{3\pi}{5}\in C^*$.

27. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\6&3&4&8&1&5&2&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{7\pi}{15}+i\sin\frac{7\pi}{15}\in C^*$.

28. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&3&4&6&1&5&2&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{6\pi}{15}+i\sin\frac{6\pi}{15}\in C^*$.

29. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&3&2&6&1&5&4&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{3\pi}{13}+i\sin\frac{3\pi}{13}\in C^*$.

30. a) $g=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&1&6&5&8&7\end{pmatrix}\in S_8$; b) $g=\cos\frac{\pi}{5}+i\sin\frac{\pi}{5}\in C^*$.

1.4. Група симетрій

Симетрія фігури (тіла) — це рух площини (простору), за яким фігура (тіло) в цілому, як множина, переходить у себе.

Теорема: Множина симетрій фігури (тіла) утворює групу відносно суперпозиції.

Цю групу називають групою симетрій фігури (тіла).

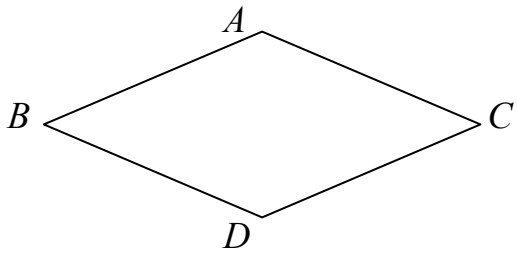
Приклад 1. Група симетрій ромба містить 4 елементи:

тотожне перетворення ε,

симетрію відносно діагоналі AD,

симетрію відносно діагоналі BC,

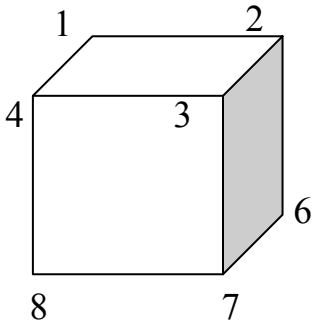
поворот на 180° навколо центра О.



Отже, порядок групи симетрій ромба дорівнює 4.

Приклад 2. Група симетрій кола містить усі повороти навколо центра кола і всі симетрії відносно осей, що проходять через центр кола. Зокрема, ця група нескінченна.

Приклад 3. Група поворотів куба містить :



а) тотожний поворот ;

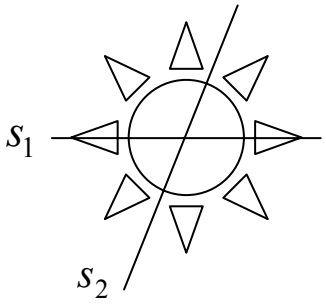
б) повороти навколо кожної з трьох осей, що з'єднують центри протилежних граней, на кути $\frac{\pi}{2}, \pi, \frac{3\pi}{2}$ (всього 9 поворотів);

в) по два повороти навколо кожної з чотирьох діагоналей (на кути $\frac{2\pi}{3}; \frac{4\pi}{3}$; всього 8 поворотів);

г) повороти на 180° навколо кожної з шести осей, що з'єднують середини протилежних ребер (6 поворотів).

Таким чином, група поворотів куба містить 24 елементи. Зауважимо, що група симетрій куба має порядок 48.

Приклад 4. Знайдемо порядок групи симетрій фігури, зображеної на рисунку.

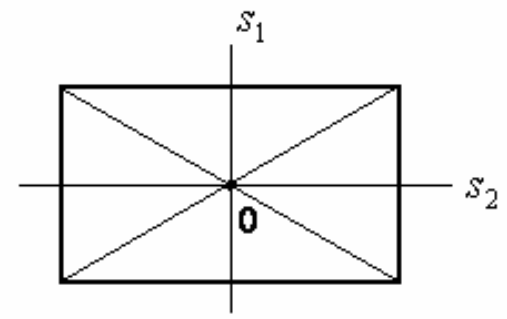


Як можна побачити, ця група містить 8 осьових симетрій (4 симетрії типу s_1 і 4 симетрії типу s_2) і 8 поворотів (на кути, кратні $\frac{\pi}{4}$).

Отже, порядок цієї групи дорівнює 16.

Приклад 5. Побудувати таблицю Келі для групи симетрій прямокутника.

Група симетрій прямокутника містить чотири елемента: два повороти на кути 0° і 180° навколо його центра та дві осьові симетрії відносно прямих s_1 та s_2, що проходять через середини протилежних сторін прямокутника. Бінарною операцією є суперпозиція. Таблиця Келі має такий вигляд:



$\circ$	0°	180°	s_1	s_2
0°	0°	180°	s_1	s_2
180°	180°	0°	s_2	s_1
s_1	s_1	s_2	0°	180°
s_2	s_2	s_1	180°	0°

Завдання 4. Знайти порядок групи симетрій

1. Рівностороннього трикутника.
2. Правильної чотирикутної піраміди.
3. Еліпса.
4. Правильної шестикутної піраміди.
5. Еліпсоїд із попарно різними півосями.
6. Гіперболи.
7. Цифри 0.
8. Правильного п'ятикутника.
9. Правильної трикутної піраміди.
10. Букви Х.
11. Виразу 00.
12. Правильної трикутної піраміди.
13. Прямого різностороннього паралелепіпеда.
14. Прямої призми з ромбом в основі.
15. Правильної п’ятикутної піраміди.
16. Квадрата.
17. Букви Ф.
18. Правильної восьмикутної піраміди.
19. Паралелограма.
20. Цифри 8.
21. Правильного шестикутника.
22. Правильної семикутної піраміди.
23. Букви Н.
24. Правильного восьмикутника.
25. Букви Ж.
26. Виразу 88.
27. Виразу ХХ.
28. Букви S.
29. Прямокутника.
30. Виразу $$.

1.5. Система твірних елементів групи. Циклічна група

Підмножина $A \subseteq G$ групи G називається **системою твірних** елементів групи G, якщо A не міститься в жодній власній підгрупі з G. Можна показати, що A буде системою твірних групи G тоді й лише тоді, коли кожен елемент $g \in G$ можна записати у вигляді $g = a_1 a_2 .... a_s$, де кожен множник a_i належить множині A або є оберненим до елемента з A. Група, для якої існує система твірних з одного елемента, називається циклічною. Зрозуміло, що множина всіх елементів групи G буде системою твірних для G, але це надлишкова система. Система твірних з якої неможна вилучити жодного елемента, називається незвідною. Якщо кількість елементів незвідної системи твірних групи є скінченною, то таку групу G називають **скінченопородженою**. В кожній скінченній групі

існують незвідні системи твірних, причому вони можуть складатися з різних елементів, тобто незвідна система твірних вибирається неоднозначно. Так наприклад, $Q_8 = \{\pm 1;\pm i;\pm j;\pm k\} =< i, j >=< i,k >=< j,k >$. Незвідні системи твірних групи G можуть містити навіть різну кількість елементів. Наприклад, група підстановок S_n може бути породжена як всіма транспозиціями з фіксованим елементом, тобто $S_n =< (1,2);(1,3);(1,4);...;(1,n) >$ ($n-1$ елемент) так і всього двома елементами $S_n =< (1,2);(1,2,3,...,n) >$. Нескінченні групи не обов'язково повинні мати незвідні системи твірних, наприклад, адитивна група раціональних чисел. З іншого боку, існують нескінченні групи зі скінченною незвідною групою твірних, наприклад адитивна група цілих чисел породженна одним елементом, а саме $(Z,+) =< 1 >=< -1 >$.

Можна також сказати, що група G називається **циклічною**, якщо вона складається зі степенів (кратних) одного із своїх елементів a. Елемент a називається **твірним елементом** циклічної групи. Циклічна група з твірним елементом a позначається $\langle a \rangle$. Кожна циклічна група абелева.

Приклад 1. Множина цілих чисел відносно додавання утворює нескінченну циклічну групу з твірним елементом одиниця (за твірний елемент можна також взяти елемент – "мінус одиниця").

Приклад 2. Група всіх комплексних коренів n-ого степеня з одиниці є скінченною циклічною групою з твірним елементом $\varepsilon_1 = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. Зауважимо, що за твірний елемент цієї групи можна взяти довільне число $\varepsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$, де k взаємно просте з n.

Нехай $G-$ мультиплікативна група з одиницею e. **Порядком елемента** $a \in G$ називається найменше натуральне число n, для якого $a^n = e$. Якщо елемент a є елементом скінченного порядку n (пишуть $|a| = n$), то порядок циклічної групи $\langle a \rangle$ збігається з порядком твірного елемента. Якщо елемент a є елементом нескінченного порядку, то циклічна група $\langle a \rangle$ нескінченна. Всі циклічні групи одного порядку n ізоморфні між собою. Всі циклічні групи нескінченного порядку ізоморфні між собою.

Нагадаємо, що через $\varphi(n)$ позначається кількість натуральних чисел, що не перевищують n і взаємно прості з числом n. Нехай $G = \langle a \rangle$, $|a| = n$. Тоді кількість елементів n-го порядку в $\langle a \rangle$ дорівнює $\varphi(n)$ (тобто кількість твірних елементів групи G дорівнює $\varphi(n)$).

Для кожного елемента b циклічної групи G порядку n його порядок $|b|$ є дільником числа n.

Приклад 3. У циклічній групі $G = \langle a \rangle$ порядку 560 знайти всі елементи g, які задовольняють умову $g^{30} = e$.

Потрібно знайти всі такі елементи $g = a^k$, що $g^{30} = e$. $g^{30} = \left(a^k\right)^{30} = a^{30k} = e$, тому $30k \vdots 560$, $3k \vdots 56$, отже $k \vdots 56$, $k = 0,56,112,168,224,280,336,392,448,504$. Відповідь: умову $g^{30} = e$ задовольняють елементи $e, a^{56}, a^{112}, a^{168}, a^{224}, a^{280}, a^{336}, a^{392}, a^{448}, a^{504}$.

Приклад 4. У циклічній групі G порядку 360 знайти всі елементи g порядку 30.

За означенням порядку елемента групи 30 найменша степінь, в якій $g^{30} = e$. Маємо $360 : 30 = 12$. Зрозуміло, що коли елемент має порядок 30, то він має порядок 2,3,4,5,6,…,15,…,28, тобто якщо ми хочемо знайти найменшу степінь, то нам потрібно вибрати взаємно прості числа для

числа 30. Числа взаємно прості з 30 будуть числа 1, 7, 11, 13, 17, 19, 23, 29. Тобто, нас цікавлять елементи $b, b^7, b^{11}, b^{13}, b^{17}, b^{19}, b^{23}, b^{29}$, тому елементи порядку 30 є елементи $a^{12}, a^{84}, a^{132}, a^{156}, a^{204}, a^{228}, a^{276}, a^{348}$.

Завдання 5. У циклічній групі $\langle a \rangle$ порядку n

1) знайти всі елементи g, які задовольняють умову $g^k = e$;

2) та знайти всі елементи порядку k, якщо :

1. $n = 24$, $k = 6$.
2. $n = 100$, $k = 20$.
3. $n = 24$, $k = 4$.
4. $n = 360$, $k = 60$.
5. $n = 100$, $k = 10$.
6. $n = 360$, $k = 12$.
7. $n = 234$, $k = 9$.
8. $n = 360$, $k = 45$.
9. $n = 250$, $k = 10$.
10. $n = 255$, $k = 15$.
11. $n = 36$, $k = 9$.
12. $n = 48$, $k = 6$.
13. $n = 36$, $k = 6$.
14. $n = 56$, $k = 8$.
15. $n = 28$, $k = 4$.
16. $n = 160$, $k = 8$.
17. $n = 125$, $k = 25$.
18. $n = 200$, $k = 8$.
19. $n = 250$, $k = 50$.
20. $n = 164$, $k = 4$.
21. $n = 150$, $k = 15$.
22. $n = 240$, $k = 12$.
23. $n = 150$, $k = 10$.
24. $n = 72$, $k = 8$.
25. $n = 150$, $k = 25$.
26. $n = 140$, $k = 35$.
27. $n = 105$, $k = 15$.
28. $n = 280$, $k = 14$.
29. $n = 275$, $k = 25$.
30. $n = 121$, $k = 11$.

1.6. Теореми Силова. Силовські підгрупи

За теоремою Лагранжа порядок довільної підгрупи є дільником порядка скінченої групи. На прикладі групи A_4 можна переконатися, що зворотне твердження не є правильним. Порядок групи A_4 дорівнює 12, але A_4 не містить підгруп шостого порядку. У знакозмінній групі A_5 порядку 60 не існує підгруп 30-го порядку, 20-го та 15-го порядків. Природно виникає питання: "для яких дільників d порядку n групи G існує підгрупа даного порядку d ?" Для випадку $n = p^s m$, де p - просте число, m - ціле число і m взаємно просте з p, відповідь дає теорема Силова

(зауважимо, що підгрупи порядку p^s називають силовськими p-підгрупами групи G)

Теорема Силова. Нехай G – група, p – просте число. Якщо $|G| = p^s m$, де $s \geq 1$ та p не є дільником m, то справедливі наступні твердження:

1. у групі G існують підгрупи порядку p^i для кожного $i = 1,2,...,s$;
2. якщо $0 \leq k \leq s-1$, то довільна підгрупа P' порядку p^k міститься в деякій підгрупі P'' порядку p^{k+1}.
3. довільні дві силовські підгрупи P і P_1 групи G є спряженими, тобто знайдеться елемент $a \in G$, для якого $P_1 = aPa^{-1}$.
4. кількість N_p всіх силовськіх p-підгруп групи G порядку $n = p^s m$ конгруентна одиниці за модулем p, причому N_p є дільником порядка групи.

Група S_3 порядку 6 містить три силовськи 2-підргупи: $\{e,(12)\}$, $\{e,(13)\}$, $\{e,(23)\}$ і одну силовські 3-підгрупу A_3. Група A_4 порядку $12 = 2^2 \cdot 3$ містить одну силовські 2-підгрупу K_4 та чотири силовських 3-підгрупи $\{e,(123),(132)\}$, $\{e,(124),(142)\}$, $\{e,(134),(143)\}$, $\{e,(234),(243)\}$.

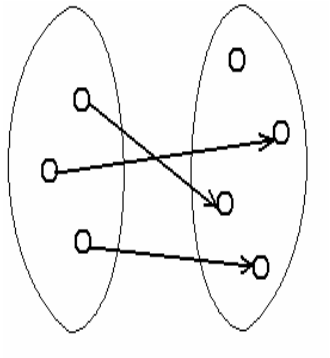
Вправа для самостійного опрацювання: Знайти всі силівські 5-підгрупи в групі A_5.

1.7. Морфізми груп

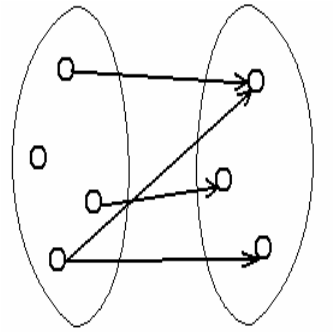
Розглянемо дві непорожні множини A і B. Кажуть, що множина A відображається **в** множину B, якщо кожному елементу множини A за деяким правилом φ поставлено у відповідність один і тільки один елемент множини B; записують $\varphi : A \to B$. Відображення $\varphi : A \to B$ називають **сюр'єктивним**, або відображення множини A **на** множину B, якщо кожний елемент множини B є образом деякого елемента множини A.

Відображення $\varphi : A \to B$ називають **ін'єктивним**, якщо воно різним елементам множини A зіставляє різні елементи множини B.

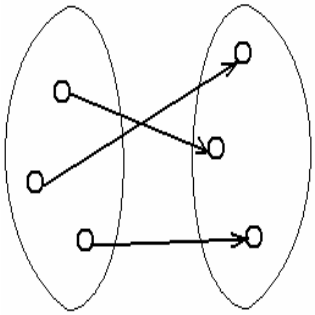
Відображення $\varphi : A \to B$ називають **бієктивним**, або взаємно однозначним, відображенням множини A на множину B, якщо кожний елемент множини B є образом єдиного елемента множини A (тобто відображення є ін'єктивним і сюр'єктивним одночасно).



Відображення "**в**"



Відображення "**на**"



Бієктивне відображення

Відображення $f : G \to G'$ групи $(G,*)$ в групу $(G',\circ)$ називається **гомоморфізмом**, якщо для довільних елементів a, b групи G виконується рівність $f(a * b) = f(a) \circ f(b)$.

Гомоморфізм $f : G \to G$ групи G в себе називається **ендоморфізмом**.

Гомоморфізм $f : G \to G'$ називається **епіморфізмом**, якщо відображення $f : G \to G'$ є сюр'єктивним.

Гомоморфізм $f : G \to G'$ називається **мономорфізмом**, якщо відображення $f : G \to G'$ є ін'єктивним.

Бієктивний гомоморфізм $f : G \to G'$ називається **ізоморфізмом** (тобто гомоморфізм $f : G \to G'$ є ізоморфізмом), якщо відображення f є ін'єктивним і сюр'єктивним одночасно.

Ізоморфізм групи G на себе називають **автоморфізмом**.

Властивості ізоморфізмів груп

Твердження. При кожному ізоморфізмі відображені $\varphi: G \to G_1$ групи $(G,*)$ в групу $(G_1,\circ)$:

1. нейтральний елемент e групи G відображається в нейтральний елемент e_1 групи G_1, тобто $\varphi(e) = e_1$;
2. образ оберненого елемента є оберненим до образу елемента, тобто $\varphi\left(g^{-1}\right) = (\varphi(g))^{-1}$;
3. порядки ізоморфних груп рівні.

Зауважимо також, що коли множина G_1 із визначеною бінарною операцією $\circ$, ізоморфна деякій групі $(G,*)$, то $(G_1,\circ)$ також є групою. Якщо група $(G,*)$ є абелевою (або циклічною) та відображення $\varphi: G \to G_1$ є ізоморфним, то $(G_1,\circ)$ також абелева (відповідно циклічна) група.

Приклад 1. З'ясувати, чи будуть ізоморфними група D_3 та група $GL_2(Z_2)$.

Група D_3 симетрій правильного трикутника складається з трьох поворотів на кути 0°, 120°, 240° відповідно та трьох осьових симетрій S_1, S_2, S_3 відносно прямих, що містять бісектриси кутів трикутника. Група невироджених матриць другого порядку з елементами поля Z_2 складається теж з шістьох елементів, а саме

$$GL_2(Z_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Позначимо елементи відповідних груп

$D_3 = \{a_0 = 0^\circ, a_1 = s_1, a_2 = s_2, a_3 = s_3, a_4 = 120^\circ, a_5 = 240^\circ\}$

$GL_2(Z_2) = \{b_0, b_1, b_2, b_3, b_4, b_5\}$ і складемо відповідні таблиці Келі:

$\circ$	a_0	a_1	a_2	a_3	a_4	a_5
a_0	a_0	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_0	a_4	a_5	a_2	a_3
a_2	a_2	a_5	a_0	a_4	a_3	a_1
a_3	a_3	a_4	a_5	a_0	a_1	a_2
a_4	a_4	a_3	a_1	a_2	a_5	a_0
a_5	a_5	a_2	a_3	a_1	a_0	a_4

$\circ$	b_0	b_1	b_2	b_3	b_4	b_5
b_0	b_0	b_1	b_2	b_3	b_4	b_5
b_1	b_1	b_0	b_4	b_5	b_2	b_3
b_2	b_2	b_5	b_0	b_4	b_3	b_1
b_3	b_3	b_4	b_5	b_0	b_1	b_2
b_4	b_4	b_3	b_1	b_2	b_5	b_0
b_5	b_5	b_2	b_3	b_1	b_0	b_4

З таблиць Келі видно, що відображення $\varphi : a_i \to b_i$, $i = \overline{0,5}$, буде ізоморфізмом.

Справедливі наступні твердження.

Твердження 1. Кожна нескінченна циклічна група ізоморфна адитивній групі Z цілих чисел.

Твердження 2. Кожна циклічна група порядку n ізоморфна групі поворотів C_n правильного n - кутника.

Наслідок з твердження 2. Циклічні групи одного порядку ізоморфні між собою.

Твердження 3 (теорема Келі). Кожна скінченна група порядку n ізоморфна деякій підгрупі H симетричної групи S_n.

Приклад 2. З'ясувати, чи будуть ізоморфними групи D_6, A_4, Z_{12}, C_6, Z_7^*, S_3.

Нагадаємо, що D_6 – група симетрій правильного шестикутника (шість симетрій + шість поворотів),

A_4 – група парних підстановок з 4-х елементів (12 парних підстановок),

Z_{12} – адитивна група кільця лишків за модулем 12 (порядок 12),

C_6 – група поворотів правильного шестикутника (шість поворотів на кути, кратні 60°, відносно центра шестикутника),

Z_7^* – мультиплікативна група кільця лишків за модулем 7 (містить 6 елементів),

S_3 – симетрична група степеня 3 (шість підстановок).

Оскільки порядки ізоморфних груп однакові, то жодна з перших трьох груп не може бути ізоморфною жодній з трьох останніх груп. Далі, в ізоморфних групах кількість елементів даного порядку однакова, тому $D_6 \ncong A_4$, оскільки D_6 має сім елементів другого порядку (180° та шість осьових симетрій), а група A_4 має лише три елемента другого порядку, а саме $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$. Група Z_{12} є циклічною, тому $Z_{12} \ncong D_6$, $Z_{12} \ncong A_4$ (ці групи не є циклічними). Отже, серед перелічених груп порядку 12 ізоморфних немає. Група S_3 не є циклічною, тому вона не може бути ізоморфною ні C_6, ні Z_7^*. Нарешті, групи C_6, Z_7^* є циклічними групами порядку 6, отже вони ізоморфні.

Приклад 3. З'ясувати, чи буде відображення $f : C^* \to C^*$, $f(z) = z^2$, гомоморфізмом? Чи буде воно ізоморфізмом?

Перевіримо умову гомоморфізму : $f(a * b) = f(a) \circ f(b)$. Візьмемо довільні два елемента $z_1, z_2 \in C^*$. Тоді

$$f(z_1 \cdot z_2) = (z_1 \cdot z_2)^2 = z_1^2 \cdot z_2^2 = f(z_1) \cdot f(z_2).$$

Отже, відображення є гомоморфізмом, але не є ізоморфізмом, оскільки $f(z) = f(\bar{z})$.

Завдання 6. З'ясувати, чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом?

1. $f: C^* \to R^*, \quad f(z) = |z|.$
2. $f: C^* \to R^*, \quad f(z) = 4|z|.$
3. $f: C^* \to R^*, \quad f(z) = \dfrac{3}{|z|}.$
4. $f: C^* \to R^*, \quad f(z) = \dfrac{1}{|z|}.$
5. $f: C^* \to R^*, \quad f(z) = 2 + |z|.$
6. $f: C^* \to C^*, \quad f(z) = \dfrac{z}{|z|}.$
7. $f: (Z,+) \to (Z,+), \quad f(n) = 3n.$
8. $f: R^* \to R^*, \quad f(x) = x^3.$
9. $f: R^+ \to R, \quad f(x) = log_2 x.$
10. $f: R \to R^+, \quad f(x) = 2^x.$
11. $f: C^* \to C^*, \quad f(z) = \dfrac{z^2}{|z|^2}.$
12. $f: (Z,+) \to (Z,+), \quad f(n) = -5n.$
13. $f: R \to R, \; f(x) = ax + b, \; a,b \in R.$
14. $f: (Z,+) \to (Z,+), \; f(n) = 2n^2 + n.$
15. $f: R \to R, \quad f(x) = sinx + cos2x.$
16. $f: (T,\cdot) \to (T,\cdot), \; f(z) = z^2,$ де $T = \{z \in C : |z| = 1\}.$
17. $f: R \to R^+, \quad f(x) = 3^x.$
18. $f: Q \to Q, \quad f(x) = ax, \quad a \neq 0.$
19. $f: C \to C, \quad f(z) = z \cdot \bar{z}.$
20. $f: R \to R, \quad f(x) = \sin x.$
21. $f: R \to R, \quad f(x) = x\sqrt{3}.$
22. $f: R^+ \to R, \quad f(x) = \ln x.$
23. $f: R^* \to R^*, \quad f(x) = 2\dfrac{x}{|x|}.$
24. $f: R \to Z, \quad f(x) = [x].$
25. $f: C^* \to R^+, \quad f(z) = |z|^3.$
26. $f: R^* \to R^*, \quad f(x) = x^4.$
27. $f: C^* \to R^+, \quad f(z) = |z|^2.$
28. $f: R^* \to R^*, \quad f(x) = \dfrac{1}{x}.$
29. $f: R \to R^+, \quad f(x) = e^x.$
30.. $f: R \to R, \quad f(x) = -|x|$

1.8. Кільце

Непорожня множина K, на якій введено дві бінарні операції $(*)$ і $(\circ)$, називається **кільцем**, якщо виконуються такі умови:

1) множина K є абелевою групою відносно операції $(*)$;

2) операція $(\circ)$– асоціативна на множини K;

3) операція $(\circ)$– дистрибутивна відносно операції $(*)$, тобто

$$\forall a,b,c \in K \quad (a*b)\circ c = a\circ c * b\circ c; \quad c\circ(a*b) = c\circ a * c\circ b.$$

Зауважимо, що операції $(*)$ і $(\circ)$ часто називають відповідно додаванням і множенням. Враховуючи це, можна дати таке означення: непорожня множина K з бінарними операціями додавання і множення називається **кільцем**, якщо відносно додавання вона є абелевою групою, відносно множення – напівгрупою, і має місце дистрибутивність множення відносно додавання як зліва, так і справа.

Абелева група $(K,+)$ називається адитивною групою кільця K. Зауважимо, що так визначені кільця називають асоціативними, за рахунок асоціативного множення. Поряд з цим існують і неасоціативні кільця (кільця Лі, альтернативні кільця, йорданові кільця тощо). Але ми розглядаємо лише асоціативні кільця, тому далі термін «кільце» означатиме «асоціативне кільце». Якщо операція множення комутативна, то кільце називають **комутативним**.

Елемент e кільця K називається **правою одиницею** цього кільця, якщо для довільного $a \in K$ має місце $ae = a$ (відповідно **лівою одиницею** кільця – якщо $ea = a$). Елемент e кільця K називається **одиницею** цього кільця, якщо він одночасно є лівою і правою одиницею. Ненульове кільце K, в якому існує одиничний елемент e відносно операції множення, називають **кільцем з одиницею**.

Приклад 1. Множина квадратних матриць даного порядку n з дійсними коефіцієнтами є кільцем з одиницею (одинична матриця) відносно операції додавання і множення.

Приклад 2. Множина парних чисел є комутативним кільцем відносно операції додавання і множення.

Приклад 3. Множина двічі диференційовних на проміжку (a,b) функцій є комутативним кільцем з одиницею відносно звичайних операції додавання і множення.

Справедливі таки **твердження:**

1. У кожному кільці K сума будь-яких його елементів $a_1, a_2, ..., a_n$ не залежить від способу розставлення дужок і порядку розміщення доданків.
2. У кожному кільці K здійсненна операція віднімання.
3. У кожному кільці K містяться кратні na будь-якого елемента a $(n \in Z)$.
4. Для будь-яких елементів a і b кільця K та довільних цілих чисел m і n справджуються таки рівності: $(m+n)a = ma + na$, $m(a+b) = ma + mb$, $m(na) = (mn)a$.
5. У кожному кільці K для будь-яких його елементів $a_1, a_2, ..., a_n$ справджується рівність $-(a_1 + a_2 + ... + a_n) = (-a_1) + (-a_2) + ... + (-a_n)$.
6. У кожному кільці K для будь-якого його елемента a і довільного натурального числа n справджується рівність $n(-a) = -(na)$.
7. У кожному кільці K для будь-яких його елементів a і b справджуються рівності $(-a)b = -ab$, $a(-b) = -ab$, $(-a)(-b) = ab$.
8. У кожному кільці нульовий елемент 0 єдиний.
9. У кожному кільці з одиницею одиничний елемент 1 єдиний.
10. У кожному кільці K для будь-якого його елемента a маємо $a \cdot 0 = 0 \cdot a = 0$.

Непорожня підмножина A кільця K називається **підкільцем**, якщо вона сама є кільцем відносно тих самих операцій, що введені на K. У кожному кільці K є такі підкільця: саме кільце K та нульове підкільце,

яке складається лише з нульового елемента – їх називають тривіальними. Всі інші підкільця називають нетривіальними. Для того щоб з'ясувати, чи є дана непорожня підмножина A кільця K його підкільцем, зручно використовувати **критерій підкільця**: Непорожня підмножина A кільця K буде підкільцем тоді й лише тоді, коли A є замкненою відносно операцій множення та віднімання.

Зрозуміло, що перетин довільної родини підкілець кільця K також буде підкільцем цього кільця та підкільце комутативного кільця є комутативним.

Приклад 4. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина $Z\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}:a,b\in Z\right\}$.

Зрозуміло, що дана множина є підмножиною кільця R. Нехай $x,y\in Z\left(\sqrt{2}\right)$. За критерієм підкільця потрібно показати, що $x-y\in Z\left(\sqrt{2}\right)$ та $x\cdot y\in Z\left(\sqrt{2}\right)$. Нехай $x=a_1+b_1\sqrt{2}$, $y=a_1+b_1\sqrt{2}$. Тоді маємо:

$$x-y=\left(a_1+b_1\sqrt{2}\right)-\left(a_2+b_2\sqrt{2}\right)=\left(a_1-a_2\right)+\left(b_1-b_2\right)\sqrt{2},$$

$$x\cdot y=\left(a_1+b_1\sqrt{2}\right)\left(a_2+b_2\sqrt{2}\right)=\left(a_1b_1+2b_1b_2\right)+\left(a_1b_2+a_2b_1\right)\sqrt{2}.$$

Оскільки кожне з чисел a_1-a_2, b_1-b_2, $a_1b_1+2b_1b_2$, $a_1b_2+a_2b_1$ є цілими, то множина $Z\left(\sqrt{2}\right)$ є підкільцем кільця дійсних чисел. Отже, буде кільцем.

Приклад 5. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина $M=\left\{a+b\sqrt[3]{2}:a,b\in Z\right\}$.

Зрозуміло, що множина M є підмножиною кільця R. Нехай $x,y\in M$. За критерієм підкільця достатньо показати, що $x-y\in M$ та $x\cdot y\in M$. Нехай $x=a_1+b_1\sqrt[3]{2}$, $y=a_1+b_1\sqrt[3]{2}$. Тоді,

$$x\cdot y=\left(a_1+b_1\sqrt[3]{2}\right)\left(a_2+b_2\sqrt[3]{2}\right)=a_1b_1+\left(a_1b_2+a_2b_1\right)\sqrt[3]{2}+a_2b_2\sqrt[3]{4}.$$

Покажемо, що $\sqrt[3]{4}\notin M$. Від супротивного, припустимо, що $\sqrt[3]{4}=c+d\sqrt[3]{2}$ для деяких цілих c і d. Це означає що $\sqrt[3]{2}$ є коренем многочлена

$f(x)=x^2-dx-c$. Поділимо многочлен x^3-2 на $f(x)$ в кільці $Z[x]$ з остачею: $x^3-2=f(x)q(x)+r(x)$, де остача $r(x)$ - многочлен не вище першого степеня з цілими коефіцієнтами. Підставляючи в обидва боки рівності $x^3-2=(x^2-dx-c)q(x)+r(x)$ значення $\sqrt[3]{2}$, отримаємо, що $r(\sqrt[3]{2})=0$. Тоді лінійний многочлен $q(x)$ не може бути з цілими коефіцієнтами, оскільки він містить радикал. Ця суперечність доводить, що $\sqrt[3]{4}\notin M$. Множина M не є кільцем, оскільки вона не замкнена відносно звичайного множення.

Приклад 6. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина $C_{[a,b]}$ всіх функцій, неперервних на відрізку $[a,b]$.

З курсу математичного аналізу відомо, що сума, різниця та добуток функцій, неперервних на відрізку $[a,b]$, є функцією, неперервною на цьому відрізку. Асоціативність і комутативність додавання та множення, а також дистрибутивності випливають із відповідних законів для додавання й множення дійсних чисел. Нейтральним елементом для операції додавання буде нульова функція 0, нейтральним елементом для операції множення буде одинична функція 1, протилежною функцією для $f(x)$ буде функція $-f(x)$. Отже, множина $C_{[a,b]}$ всіх функцій, неперервних на відрізку $[a,b]$ буде комутативним кільцем з одиницею.

Завдання 7. З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення

1. Множина дійсних чисел вигляду $x + y\sqrt{3}$, де $x, y \in Q$?
2. Множина дійсних функцій, неперервних на проміжку $[0,1]$?
3. Множина ненульових дійсних матриць вигляду $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, де число a – фіксоване?
4. Множина дійсних чисел вигляду $x + y\sqrt[3]{3}$, де $x, y \in Q$?
5. Множина всіх дійсних симетричних матриць порядку n?
6. Множина раціональних чисел, у нескоротному записі яких знаменники є дільниками фіксованого натурального числа n?
7. Множина всіх дійсних невироджених матриць порядку n.
8. Множина дійсних чисел, які можна подати у вигляді многочлена $a_0 + a_1\pi + a_2\pi^2 + \ldots + a_n\pi^n$ від числа π?
9. Множина комплексних чисел вигляду $x + iy$, де $x, y \in Z$?
10. Множина дійсних чисел вигляду $x + y\sqrt[3]{2}$, де $x, y \in Q$?
11. Множина всіх дійсних кососиметричних матриць порядку n?
12. Множина всіх тригонометричних многочленів вигляду $a_0 + \sum_{k=1}^{n} a_k \cos(kx)$ із дійсними коефіцієнтами?
13. Множина дійсних чисел вигляду $x + y\sqrt[3]{3} + z\sqrt[3]{9}$, де $x, y, z \in Q$?
14. Множина всіх дійсних верхніх трикутних матриць порядку n?
15. Множина дійсних функцій, неперервних на проміжку $(0,1)$?
16. Множина раціональних чисел, у нескоротному записі яких знаменники не діляться на фіксоване просте число p?
17. Множина дійсних чисел вигляду $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, де $x, y, z \in Q$?

18. Множина комплексних матриць вигляду $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$?

19. Множина всіх тригонометричних многочленів вигляду $a_0 + \sum_{k=1}^{n} a_k \cos(kx) + b_k \sin(kx)$ із дійсними коефіцієнтами?

20. Множина комплексних чисел вигляду $x + iy$, де $x, y \in Q$?

21. Множина дійсних чисел вигляду $x - y\sqrt{3}$, де $x, y \in Q$?

22. Множина раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p?

23. Множина дійсних чисел вигляду $x + y\sqrt{7}$, де $x, y \in Q$?

24. Множина всіх тригонометричних многочленів вигляду $\sum_{k=1}^{n} b_k \sin(kx)$ із дійсними коефіцієнтами?

25. Множина дійсних чисел вигляду $x + y\sqrt[3]{25}$, де $x, y \in Q$?

26. Множина всіх скалярних матриць порядку n?

27. Множина дійсних чисел вигляду $x + y\sqrt[3]{7} + z\sqrt[3]{49}$, де $x, y, z \in Q$?

28. Множина дійсних чисел вигляду $x + y\sqrt[4]{2}$, де $x, y \in Q$?

29. Множина дійсних функцій, неперервних на проміжку $(-1,1)$?

30. Множина всіх многочленів степінь яких не перевищує 2 від однієї змінної над полем Z_3?

1.9. Дільники нуля, дільники одиниці, оборотні та нільпотентні елементи. Поле

Нехай $(K,+,\cdot)$– кільце. Ненульовий елемент $a \in K$ називається **лівим дільником нуля**, якщо існує такий ненульовий елемент $b \in K$, що $ab = 0$. Ненульовий елемент $a \in K$ називається **правим дільником нуля**, якщо існує такий ненульовий елемент $b \in K$, що $ba = 0$. **Дільником нуля** називається такий елемент $a \in K$, який одночасно є лівим та правим дільником нуля. Зрозуміло, що в комутативному кільці лівий дільник нуля буде правими дільником нуля, і навпаки.

Комутативне кільце з одиницею без дільників нуля називається **областю цілісності**. Прикладами області цілісності є кільце цілих чисел Z та кільце многочленів $R[x]$. Зауважимо, що кільце квадратних матриць $M_n(R)$ при $n > 1$ не є областю цілісності, оскільки множення матриць не комутативне та кільце містить дільники нуля.

Елемент $a \in K$ називається **нільпотентним** елементом, якщо існує таке натуральне число n, що $a^n = 0$. Найменше таке n називається **ступенем нільпотентності** елемента a. Таким чином, кожний нільпотентний елемент є дільником нуля.

Нехай тепер K – кільце з одиницею. Елемент $a \in K$ називається **лівим** (відповідно правим) **дільником одиниці**, якщо існує такий неодиничний елемент $b \in K$, що $ab = 1$ (відповідно $ba = 1$). Якщо елемент одночасно є лівим і правим дільником одиниці, то його називають **дільником одиниці**. Дільники одиниці називають **оборотними елементами**, ліві дільники одиниці називають оборотними справа, праві дільники одиниці називають оборотними зліва. До необоротних елементів відносяться всі дільники нуля та сам нуль. У кільці Z_{20} дільниками нуля є $2,4,5,6,8,10,12,14,15,16,18$, необоротними елементами є $0,2,4,5,6,8,10,12,14,15,16,18$, оборотними елементами відповідно

1,3,7,9,11,13,17,19. У кільці цілих чисел Z дільників нуля немає, але всі елементи відмінні від ± 1 є необоротними.

Комутативне кільце з одиницею, в якому для кожного ненульового елемента існує обернений, називають **полем**. Поле називається скінченним, якщо кількість елементів у ньому скінченна. **Характеристикою поля** P з одиницею e і нулем θ називають найменше натуральне число p, для якого $pe = \theta$. Якщо рівність $pe = \theta$ виконується лише при $p = 0$, то вважають, що P є полем характеристики нуль. Всі числові поля мають характеристику нуль, всі скінченні поля мають скінченну характеристику p, причому p –просте число. Також зауважимо, що жодне поле не має дільників нуля.

Приклад 1. У полі Z_{331} знайти обернений елемент для елемента 173.

Розв'язування. Оскільки $(331,173) = 1$, то можна знайти лінійне зображення 1: $1 = 331a + 173b$.

В полі Z_{331} $331a = 0$, тому $1 = 173b$, й елемент b буде оберненим до елемента 173. Знайдемо лінійне зображення 1:

$$
\begin{array}{r|l}
331 & 173 \\
\hline
173 & 1
\end{array}
\qquad 158 = 331 - 173
$$

$$
\begin{array}{r|l}
173 & 158 \\
\hline
158 & 1
\end{array}
\qquad 15 = 173 - 158 = 2 \cdot 173 - 331
$$

$$
\begin{array}{r|l}
158 & 15 \\
\hline
150 & 10
\end{array}
$$

$$
\begin{array}{r|l}
15 & 8 \\
\hline
8 & 1
\end{array}
\qquad 8 = 158 - 15 \cdot 10 = 331 - 173 - 10(2 \cdot 173 - 331) = 11 \cdot 331 - 21 \cdot 173
$$

$$
\begin{array}{r|l}
8 & 7 \\
\hline
7 & 1
\end{array}
\qquad 7 = 15 - 8 = 2 \cdot 173 - 331 - (11 \cdot 331 - 21 \cdot 173) = 23 \cdot 173 - 12 \cdot 331
$$

$$
\begin{array}{r|l}
7 & \textcircled{1} \\
\hline
7 & 7
\end{array}
\qquad 1 = 8 - 7 = 11 \cdot 331 - 21 \cdot 173 - (23 \cdot 173 - 12 \cdot 331) = 23 \cdot 331 - 44 \cdot 173
$$

$$
\begin{array}{r}
0
\end{array}
$$

Отже, в полі Z_{331} $1 = -44 \cdot 173 = 287 \cdot 173$ і елемент 287 є оберненим до елемента 173 .

Приклад 2. У кільці Z_{150} знайти обернений елемент для елемента 31.

Розв'язування. Оскільки $(150,31)=1$, то можна знайти лінійне зображення 1: $1=150a+31b$. В кільці Z_{150} маємо $150a=0$, тому $1=31b$, й елемент b буде оберненим до елемента 31. Знайдемо лінійне зображення 1:

$$\begin{array}{r|l} 150 & 31 \\ \underline{124} & \\ 31 & 26 \\ \underline{26} & 1 \\ 26 & 5 \\ \underline{25} & 5 \\ 5 & 1 \\ \underline{5} & 5 \\ 0 & \end{array} \qquad \begin{array}{l} n=150 \quad g=31 \\ 26 = n - g\cdot 4 \\ 5 = g - 1(n-4g) = 5g - n \\ 1 = 26 - 5\cdot 5 = (n-4g) - 5(5g-n) = 6n - 29g \end{array}$$

Отже, в кільці Z_{150} $1=6\cdot 150-29\cdot 31$ і елемент $-29\equiv 121 \pmod{150}$ 287 є оберненим до елемента 31.

Приклад 3. У полі $Q(\sqrt{5})$ розв'язати рівняння $x^2-(13-\sqrt{5})x+12+7\sqrt{5}=0$.

Розв'язування. $D=(13-\sqrt{5})^2-4(12+7\sqrt{5})=126-54\sqrt{5}$. З'ясуємо, чи можна дискримінант D подати у вигляді $D=(a-b\sqrt{5})^2$. Розв'язуючи систему рівнянь $\begin{cases}126=a^2+5b^2\\27=ab\end{cases}$, отримаємо $\begin{cases}a=9,\\b=3.\end{cases}$ Тому $x_{1,2}=\dfrac{13-\sqrt{5}\pm(9-3\sqrt{5})}{2}$, $\begin{array}{l}x_1=11-2\sqrt{5},\\x_2=2+\sqrt{5}.\end{array}$ Перевірку зробимо за теоремою Вієта:

$$\begin{cases}x_1\cdot x_2=\dfrac{C}{A},\\ x_1+x_2=\dfrac{-B}{A}\end{cases} \Rightarrow \begin{cases}(11-2\sqrt{5})\cdot(2+\sqrt{5})=22-10+11\sqrt{5}-4\sqrt{5}=12+7\sqrt{5},\\ 11-2\sqrt{5}+2+\sqrt{5}=13-\sqrt{5}.\end{cases}$$

Відповідь: у полі $Q(\sqrt{5})$ рівняння $x^2-(13-\sqrt{5})x+12+7\sqrt{5}=0$ має таки розв'язки $x_1=11-2\sqrt{5},\quad x_2=2+\sqrt{5}.$

Приклад 4. У полі $Q(\sqrt{13})$ розв'язати рівняння $x^2-(3-\sqrt{13})x+120+7\sqrt{13}=0$.

Розв'язування. $D=(3-\sqrt{13})^2-4(120+7\sqrt{13})=-458-34\sqrt{13}<0$. Зрозуміло, що дискримінант D не можна подати у вигляді $D=(a-b\sqrt{5})^2$. Отже, рівняння розв'язків не має.

Приклад 5. У полі $Q(\sqrt{3})$ розв'язати рівняння $x^2-(3+2\sqrt{3})x-22-\sqrt{3}=0$.

Розв'язування. $D=(3+2\sqrt{3})^2+4(22+\sqrt{3})=109+16\sqrt{3}$. З'ясуємо, чи можна дискримінант D подати у вигляді $D=(a-b\sqrt{3})^2, a,b\in Q$. Розв'язуючи систему рівнянь $\begin{cases}109=a^2+3b^2\\8=ab\end{cases}$, отримаємо $\begin{cases}a=\dfrac{8}{b}\\3b^4-109b^2+64=0\end{cases}$. Тому $b_{1,2}=\dfrac{109\pm\sqrt{11113}}{6}\notin Q$.

Відповідь: у полі $Q(\sqrt{3})$ рівняння $x^2-(3+2\sqrt{3})x-22-\sqrt{3}=0$ не має розв'язків.

Приклад 6. В кільці Z_{124} розв'язати систему рівнянь $\begin{cases}x+y=110,\\y-x=4.\end{cases}$

Розв'язування. Додавши рівняння, отримаємо: $2y=114$. Конгруенція $2y\equiv 114(\mathrm{mod}\,124)$ має два розв'язки $y_1=57,\ y_2=119$. Отже, початкова система має два розв'язки: $x_1=53, y_1=57,\quad x_2=115, y_2=119$.

Завдання 8. З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a

1. $M = Z_{179}$, $a = 96$.
2. $M = Z_{103}$, $a = 63$.
3. $M = Z_{157}$, $a = 121$.
4. $M = Z_{191}$, $a = 152$.
5. $M = Z_{233}$, $a = 199$.
6. $M = Z_{149}$, $a = 123$.
7. $M = Z_{173}$, $a = 96$.
8. $M = Z_{113}$, $a = 97$.
9. $M = Z_{163}$, $a = 57$.
10. $M = Z_{151}$, $a = 13$.
11. $M = Z_{111}$, $a = 16$.
12. $M = Z_{193}$, $a = 129$.
13. $M = Z_{293}$, $a = 123$.
14. $M = Z_{149}$, $a = 113$.
15. $M = Z_{164}$, $a = 97$.
16. $M = Z_{143}$, $a = 97$.
17. $M = Z_{199}$, $a = 111$.
18. $M = Z_{181}$, $a = 160$.
19. $M = Z_{197}$, $a = 115$.
20. $M = Z_{191}$, $a = 187$.
21. $M = Z_{167}$, $a = 117$.
22. $M = Z_{194}$,. $a = 107$.
23. $M = Z_{132}$, $a = 25$.
24. $M = Z_{150}$, $a = 101$.
25. $M = Z_{211}$, $a = 95$.
26. $M = Z_{229}$, $a = 99$.
27. $M = Z_{121}$, $a = 97$.
28. $M = Z_{173}$, $a = 101$.
29. $M = Z_{175}$, $a = 127$.
30. $M = Z_{281}$, $a = 100$.

Завдання 9. Розв'язати рівняння та систему рівнянь

1. $x^2 - (2+\sqrt{3})x - 6 - 2\sqrt{3} = 0$ у полі $Q(\sqrt{3})$; $\begin{cases} x + y = 7, \\ x - y = 5. \end{cases}$ в кільці Z_{20}.
2. $x^2 - (2+\sqrt{5})x + 2\sqrt{5} = 0$ у полі $Q(\sqrt{5})$; $\begin{cases} x - y = 7, \\ x + y = 21. \end{cases}$ в кільці Z_{22}.
3. $x^2 - x - 13 + 3\sqrt{11} = 0$ у полі $Q(\sqrt{11})$; $\begin{cases} x + y = 9, \\ x - y = 15. \end{cases}$ в кільці Z_{18}.
4. $x^2 + 2\sqrt{7}x - 25 - 8\sqrt{7} = 0$ у полі $Q(\sqrt{7})$; $\begin{cases} x + y = 17, \\ x - y = 3. \end{cases}$ в кільці Z_{18}.

5. $x^2+\left(2-\sqrt{3}\right)x-2\sqrt{3}=0$ у полі $Q\left(\sqrt{3}\right)$; $\begin{cases}x+y=11,\\ y-x=15.\end{cases}$ в кільці Z_{24}.

6. $x^2+\left(4-2\sqrt{7}\right)x+7-4\sqrt{7}=0$ у полі $Q\left(\sqrt{7}\right)$; $\begin{cases}x+y=11,\\ y-x=3.\end{cases}$ в кільці Z_{16}.

7. $x^2+\left(2+\sqrt{2}\right)x-4-2\sqrt{2}=0$ у полі $Q\left(\sqrt{2}\right)$; $\begin{cases}x+y=11,\\ y-x=5.\end{cases}$ в кільці Z_{20}.

8. $x^2+\left(\sqrt{5}-1\right)x+\dfrac{1-2\sqrt{5}}{4}=0$ у полі $Q\left(\sqrt{5}\right)$; $\begin{cases}x-y=21,\\ x+y=35.\end{cases}$ в кільці Z_{42}.

9. $x^2-2x-10=0$ у полі $Q\left(\sqrt{11}\right)$; $\begin{cases}x-y=10,\\ x+y=22.\end{cases}$ в кільці Z_{42}.

10. $x^2+\left(2+2\sqrt{11}\right)x+11+2\sqrt{11}=0$ у $Q\left(\sqrt{11}\right)$; $\begin{cases}x-y=8,\\ x+y=22.\end{cases}$ в кільці Z_{30}.

11. $x^2-\left(3+\sqrt{7}\right)x-70-26\sqrt{7}=0$ у полі $Q\left(\sqrt{7}\right)$; $\begin{cases}x+y=21,\\ x-y=11.\end{cases}$ в кільці Z_{42}.

12. $x^2+x\sqrt{3}-7+3\sqrt{3}=0$ у полі $Q\left(\sqrt{3}\right)$; $\begin{cases}x+y=17,\\ x-y=5\end{cases}$ в кільці Z_{28}.

13. $x^2-2\sqrt{3}x-1=0$ у полі $Q\left(\sqrt{3}\right)$; $\begin{cases}x+y=7,\\ x-y=3.\end{cases}$ в кільці Z_{12}.

14. $x^2+2\sqrt{5}x-19+8\sqrt{5}=0$ у полі $Q\left(\sqrt{5}\right)$; $\begin{cases}x+y=17,\\ x-y=19.\end{cases}$ в кільці Z_{28}.

15. $x^2-6x+6=0$ у полі $Q\left(\sqrt{3}\right)$; $\begin{cases}x-y=9,\\ x+y=21.\end{cases}$ в кільці Z_{42}.

16. $x^2-10x+20=0$ у полі $Q\left(\sqrt{5}\right)$; $\begin{cases}x+y=21,\\ x-y=25.\end{cases}$ в кільці Z_{38}.

17. $x^2+14x-28=0$ у полі $Q\left(\sqrt{77}\right)$; $\begin{cases}x-y=7,\\ y+x=13.\end{cases}$ в кільці Z_{22}.

18. $x^2+2x-1=0$ у полі $Q\left(\sqrt{2}\right)$; $\begin{cases}x+y=27,\\ x-y=13.\end{cases}$ в кільці Z_{42}.

19. $x^2-4x+2=0$ у полі $Q(\sqrt{2})$; $\begin{cases} x-y=1, \\ y+x=13. \end{cases}$ в кільці Z_{22}.

20. $x^2-4x+1=0$ у полі $Q(\sqrt{3})$; $\begin{cases} x-y=17, \\ x+y=23. \end{cases}$ в кільці Z_{46}.

21. $x^2-(3+3\sqrt{2})x+4+6\sqrt{2}=0$ у полі $Q(\sqrt{2})$; $\begin{cases} x+y=7, \\ x-y=15. \end{cases}$ в кільці Z_{18}.

22. $x^2-(4+\sqrt{2})x-1+5\sqrt{2}=0$ у полі $Q(\sqrt{2})$; $\begin{cases} x+y=11, \\ y-x=15. \end{cases}$ в кільці Z_{24}.

23. $x^2+(1-3\sqrt{2})x-2+\sqrt{2}=0$ у полі $Q(\sqrt{2})$; $\begin{cases} x+y=13, \\ x-y=7. \end{cases}$ в кільці Z_{24}.

24. $x^2+2x\sqrt{3}-13+8\sqrt{3}=0$ у полі $Q(\sqrt{3})$; $\begin{cases} x+y=11, \\ y-x=17. \end{cases}$ в кільці Z_{24}.

25. $x^2-2x-1-\sqrt{2}=0$ у полі $Q(\sqrt{2})$; $\begin{cases} x+y=10, \\ x-y=2. \end{cases}$ в кільці Z_{16}.

26. $x^2+(5+\sqrt{3})x+\sqrt{3}=0$ у полі $Q(\sqrt{3})$; $\begin{cases} x+y=33, \\ x-y=37. \end{cases}$ в кільці Z_{44}.

27. $x^2+(1-3\sqrt{5})x+4+\sqrt{5}=0$ у полі $Q(\sqrt{5})$; $\begin{cases} x+y=11, \\ x-y=27. \end{cases}$ в кільці Z_{30}.

28. $x^2-5x+4-\sqrt{2}=0$ у полі $Q(\sqrt{2})$; $\begin{cases} x+y=17, \\ x-y=27. \end{cases}$ в кільці Z_{38}.

29. $x^2+(1+\sqrt{3})x-12-7\sqrt{3}=0$ у полі $Q(\sqrt{3})$; $\begin{cases} x+y=24, \\ x-y=16. \end{cases}$ в кільці Z_{46}.

30. $x^2-(5+3\sqrt{5})x+16+7\sqrt{5}=0$ у полі $Q(\sqrt{5})$; $\begin{cases} x+y=33, \\ x-y=37. \end{cases}$ в кільці Z_{50}.

Завдання 10

1. Довести, що в групі Q/Z кожен елемент має скінченний порядок.
2. Довести, що кожна група порядку 6 або комутативна, або ізоморфна групі S_3.
3. Довести, що в кожній групі перетин довільного набору підгруп є підгрупою.
4. Довести, що в групі елементи xy і yx завжди мають однаковий порядок.
5. Нехай $R-$ скінченне кільце. Довести, що коли кільце R не має дільників нуля, то воно має одиницю та всі ненульові елементи кільця будуть оборотними.
6. Нехай елемент x групи G має порядок n. Довести, що $x^k = x^m$ тоді й лише тоді, коли $n \mid (k-m)$.
7. Довести, що в групі S_n порядок непарної підстановки є парне число.
8. Довести, що в будь–якій групі парного степеня є елемент порядку 2.
9. Нехай $R-$ скінченне кільце. Довести, що коли кільце R має одиницю, то будь–який лівий дільник нуля є правим дільником нуля.
10. Довести, що порядок скінченної групи ділиться на порядок кожної своєї підгрупи.
11. Довести, що об'єднання двох підгруп є підгрупою тоді й лише тоді, коли одна з підгруп міститься в іншій.
12. Довести, що в групі елементи x і yxy^{-1} мають однаковий порядок.
13. Довести, що кожна некомутативна група порядку 6 ізоморфна групі S_3.
14. Довести, що в групі Q/Z для кожного натурального n існує єдина підгрупа порядку n.
15. Нехай елемент x групи G має нескінченний порядок. Довести, що $x^k = x^m$ тоді й лише тоді, коли $k = m$.

16. Довести, що в групі S_n порядок підстановки є найменшим спільним кратним довжин незалежних циклів, що входять в її розклад.
17. Нехай $G-$ скінченна група, $a \in G$. Довести, що $G = \langle a \rangle$ тоді й лише тоді, коли елемент a має порядок $|G|$.
18. Довести, що в кільці з одиницею та без дільників нуля кожний елемент, що має односторонній обернений, є оборотним.
19. Довести, що група, в якій всі елементи мають порядок 2, комутативна.
20. Довести, що в групі C^* кожна скінченна підгрупа є циклічною.
21. Довести, що кільце цілих гаусових чисел $\{x + iy : x, y \in Z\}$ є евклідовим.
22. Довести, що в групі кожна скінченна піднапівгрупа є підгрупою.
23. Нехай елемент x групи G має порядок n. Довести, що $x^k = e$ тоді й лише тоді, коли $n|k$.
24. Нехай $G = \langle a \rangle$ – циклічна група порядку n. Довести, що елемент a^k є твірним елементом групи G тоді й лише тоді, коли числа k і n взаємно прості.
25. Довести, що в кільці дійсних функцій будь–який елемент, що не є дільником нуля, є оборотним.
26. Довести, що кільце комплексних чисел $\left\{\frac{x+iy}{2} : x, y \in Z, x \equiv y (\mathrm{mod}\, 2)\right\}$ є евклідовим.
27. Довести, що всі оборотні елементи кільця з одиницею утворюють групу відносно множення.
28. Довести, що кільце чисел $\left\{x + i\sqrt{3}y : x, y \in Z\right\}$ не є евклідовим.
29. Довести, що кожна група порядку p^2, де $p-$ просте число, є комутативною.
30. Довести, що порядок довільного елемента циклічної групи є дільником порядку твірного елемента цієї циклічної групи.

Розділ 2. КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД ОДНІЄЇ ЗМІННОЇ

2.1. Многочлени від однієї змінної. Схема Горнера

Розглянемо довільні многочлени $f(x)$ і $g(x)$ над полем P. **Найменшим спільним кратним** двох многочленів називається многочлен $q(x)$, який є спільним кратним многочленів $f(x)$ і $g(x)$ і ділить будь–яке спільне кратне цих многочленів. Многочлен $q(x)$ можна обчислити за формулою : $q(x)=\dfrac{f(x)\cdot g(x)}{(f(x),g(x))}$. Для знаходження найбільшого спільного дільника зручно використовувати **алгоритм Евкліда**.

Приклад 1. Знайти найменше спільне кратне многочленів

$f(x)=3x^5+5x^4-16x^3-6x^2-5x-6$, $g(x)=3x^4-4x^3-x^2-x-2$.

$$
\begin{array}{l|l}
3x^5+5x^4-16x^3-6x^2-5x-6 & 3x^4-4x^3-x^2-x-2 \\
\underline{-\,3x^5-4x^4-x^3-x^2-2x} & x+3 \\
-9x^4-15x^3-5x^2-3x-6 & \\
\underline{-\,9x^4-12x^3-3x^2-3x-6} & \\
3x^4-4x^3-x^2-x-2 & -3x^3-2x^2 \\
\underline{-\,3x^4+2x^3} & -x+2 \\
-6x^3-x^2-x-2 & \\
\underline{-\,-6x^3-4x^2} & \\
-3x^3-2x^2 & 3x^2-x-2 \\
\underline{-\,-3x^3+x^2+2x} & -x-1 \\
-3x^2-2x & \\
\underline{-\,-3x^2+x+2} & \\
3x^2-x-2 & -3x-2 \\
\underline{-\,3x^2+2x} & -x+1 \\
-3x-2 & \\
\underline{-\,-3x-2} & \\
0 &
\end{array}
$$

Найбільший спільний дільник цих многочленів дорівнює $(-3x-2)$. Отже, найменше спільне кратне

$$g(x)=\frac{\left(3x^5+5x^4-16x^3-6x^2-5x-6\right)\cdot\left(3x^4-4x^3-x^2-x-2\right)}{\left(-3x-2\right)},$$ або

$$g(x) = -3x^8 + x^7 + 23x^6 - 28x^5 + 14x^4 - 14x^3 - 13x^2 + x - 6.$$

Оскільки найменше спільне кратне і найбільший спільний дільник двох многочленів визначені лише з точністю до множника з поля P, то при знаходженні найбільшого спільного дільника остачу, частку і дільник можна на будь–якому кроку множити на довільне ненульове число (щоб уникнути дробових коефіцієнтів).

Найбільший спільний дільник можна знайти і за допомогою розкладу многочленів на незвідні многочлени.

Приклад 2. Знайти найбільший спільний дільник многочленів

$$f(x) = \left(x^3 - 1\right)\left(x^2 - 2x + 1\right) \qquad \text{і} \qquad g(x) = \left(x^2 - 1\right)^3.$$

Знайдемо розклад многочленів на незвідні множники над полем дійсних чисел:

$$f(x) = (x-1)^3\left(x^2 + x + 1\right), \qquad g(x) = (x-1)^3(x+1)^3.$$

Відповідь: $(f, g) = (x-1)^3$

Для обчислення значення многочлена $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ в точці $x_0 = c$ зручно користуватися **схемою Горнера**.

Приклад 3. Обчислити значення многочлена

$-3x^5 + 11x^3 - 13x^2 + x - 6$ у точці $x = -2$.

	-3	0	11	-13	1	-6
-2	-3	6	-1	-11	23	-52

Отже, значення многочлена $-3x^5 + 11x^3 - 13x^2 + x - 6$ в точці $x = -2$ дорівнює -52.

Схема Горнера має й інші застосування.

Приклад 4. Визначити кратність кореня $x=3$ для многочлена

$$f(x)=-x^6+9x^5-27x^4+28x^3-9x^2+27x-27.$$

	–1	9	–27	28	–9	27	–27
3	–1	6	–9	1	–6	9	0
3	–1	3	0	1	–3	0	
3	–1	0	0	1	0		
3	–1	–3	–9	–26			

Оскільки $-26\neq 0$, то корінь $x=3$ має кратність 3 для многочлена $f(x)=-x^6+9x^5-27x^4+28x^3-9x^2+27x-27$.

Приклад 5. Розкласти многочлен $f(x)=x^5-4x^3+6x^2-8x+10$ за степенями $x-2$.

	1	0	–4	6	–8	10
2	1	2	0	6	4	18
2	1	4	8	22	48	
2	1	6	20	62		
2	1	8	36			
2	1	10				
2	1					

Отже, розклад многочлена $f(x)$ за степенями $x-2$ має вигляд

$$f(x)=(x-2)^5+10(x-2)^4+36(x-2)^3+62(x-2)^2+48(x-2)+18.$$

Порівнюючи розклад многочлена за степенями $(x-x_0)$

$$f(x)=f(x_0)+a_1(x-x_0)+a_2(x-x_0)^2+a_3(x-x_0)^3+\ldots+a_n(x-x_0)^n$$

із розкладом $f(x)$ у ряд Тейлора за степенями $x-x_0$:

$$f(x)=f(x_0)+\frac{f'(x_0)}{1!}(x-x_0)+\frac{f''(x_0)}{2!}(x-x_0)^2+\ldots+\frac{f^{(n)}(x_0)}{n!}(x-x_0)^n+\ldots$$

Отримаємо: $f^{(k)}(x_0)=a_k\cdot k!$. Тому схему Горнера можна використовувати і для обчислення значень похідних многочлена.

Приклад 6. Знайти значення многочлена

$f(x) = -12x^4 + 2x^3 - 9x^2 + 7x - 2$ та значення усіх його похідних у точці $x = -1$.

	–12	2	–9	7	–2
–1	–12	14	–23	30	–32
–1	–12	26	–49	79	
–1	–12	38	–87		
–1	–12	50			
–1	–12				

Відповідь: $f^{(4)}(-1) = -12 \cdot 4!$, $f^{(3)}(-1) = 50 \cdot 3!$, $f''(-1) = -87 \cdot 2!$, $f'(-1) = 79 \cdot 1!$, $f(-1) = -32$.

Схему Горнера можна також використовувати для знаходження розкладу дробів вигляду $\frac{f(x)}{(x-c)^n}$ на елементарні дроби.

Приклад 7. Розкласти дріб $\frac{x^5 + 2x^2 - 4}{(x-4)^6}$ на найпростіші дроби над полем R.

Знайдемо розклад многочлена $f(x) = x^5 + 2x^2 - 4$ за степенями $x - 4$:

$$f(x) = (x-4)^5 + 20(x-2)^4 + 160(x-4)^3 + 642(x-4)^2 + 1296(x-4) + 1052.$$

Поділимо многочлен на $(x-4)^6$, після скорочення отримаємо:

$$\frac{1}{x-4} + \frac{20}{(x-4)^2} + \frac{160}{(x-4)^3} + \frac{642}{(x-4)^4} + \frac{1296}{(x-4)^5} + \frac{1052}{(x-4)^6}.$$

Завдання 11. Знайти найменше спільне кратне двох многочленів $f(x)$ та $g(x)$

1. $f(x)=x^4+2x^3-x^2-4x-2,\ g(x)=x^4+x^3-x^2-2x-2.$
2. $f(x)=x^4+2x^3+x+2,\ g(x)=x^5+3x^4+x^3+x^2+3x+1.$
3. $f(x)=2x^5+2x^4+x^3+3x^2+1, g(x)=2x^4-2x^3-x^2-x-1.$
4. $f(x)=2x^5+x^4+x^3-2x^2-x-1,\ \ g(x)=x^4-x^3-x+1.$
5. $f(x)=3x^5+5x^4-16x^3-6x^2-5x-6,\ \ g(x)=3x^4-4x^3-x^2-x-2.$
6. $f(x)=4x^4-2x^3-16x^2+5x+9,\ \ g(x)=2x^3-x^2-5x+4.$
7. $f(x)=3x^5-2x^2+x+2,\ \ g(x)=x^2-x+1.$
8. $f(x)=x^5-x^3-4x^2+4x+1,\ \ g(x)=x^3-x-1.$
9. $f(x)=x^5-5x^4-2x^3+12x^2-2x+12,\ \ g(x)=x^3-5x^2-3x+17.$
10. $f(x)=2x^4+3x^3-3x^2-5x+2,\ \ g(x)=2x^3+x^2-x-1.$
11. $f(x)=3x^4-5x^3+3x^2-2x+1,\ \ g(x)=3x^3-2x^2+x-1.$
12. $f(x)=x^5+5x^4+9x^3+7x^2+5x+3,\ \ g(x)=x^4+2x^3-2x^2+x+1.$
13. $f(x)=x^4-4x^3+1,\ \ g(x)=x^3-3x^2+1.$
14. $f(x)=x^5+2,\ \ g(x)=x^2-2x+1.$
15. $f(x)=x^5-7x+6,\ \ g(x)=(1-x)^4.$
16. $f(x)=(1-x)^3,\ g(x)=x^5-1.$
17. $f(x)=x^5+3x^4+x^3+x^2+3x+1,\ g(x)=x^4+2x^3+x+2.$
18. $f(x)=x^5+3x^3+2x^2+6,\ \ g(x)=x^5+x^4-x^3+2x^2+2x-2.$
19. $f(x)=3x^4-4x^3-x^2-x-2,\ g(x)=3x^5+5x^4-16x^3-6x^2-5x-6.$
20. $f(x)=x^4+7x^3+19x^2+23x+10,\ g(x)=x^4+7x^3+18x^2+22x+12.$
21. $f(x)=x^5+x^4+x^3+x^2+x+1,\ \ g(x)=x^4+2x^3+x^2-1.$
22. $f(x)=x^5-x^4+3x^3-4x^2-3,\ g(x)=x^4-x^3+2x^2-3x-3.$
23. $f(x)=x^5+2x^3+x^2+x+1,\ \ g(x)=x^4-x^3-2x^2-x-3.$
24. $f(x)=2x^4-3x^3-4x^2+4x+3,\ \ g(x)=x^2-x-1.$
25. $f(x)=3x^5+5x^4-16x^3-6x^2-5x-6,\ \ g(x)=3x^4-4x^3-x^2-x-2.$
26. $f(x)=x^5+x^4+3x^3-5x^2-5x-15,\ \ g(x)=x^5+x^4-x^3-5x^2-5x+5.$
27. $f(x)=x^5+x^4+2x^3+3x^2+3x+2,\ \ g(x)=x^4-3x^3+x^2-x-6.$
28. $f(x)=x^5+x^4+4x^2+2x-3,\ \ g(x)=x^4+2x^3+x^2+5x+6.$
29. $f(x)=2x^5+x^4+4x^3+3x^2+3x+2,\ \ g(x)=2x^4-x^3+2x^2+x-1.$
30. $f(x)=x^5+2x^4+2x^3-3x-2,\ \ g(x)=x^4-x^3+x^2-3x+2.$

Завдання 12. Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$

1. $f(x) = 3x^5 + 2x^4 + x^3 - 10x - 8,\ c = -1,\ x_0 = 2.$
2. $f(x) = x^5 - 6x^4 + 2x^3 + 36x^2 - 27x - 54,\ c = 3,\ x_0 = -1.$
3. $f(x) = x^5 + 5x^2 + 5x + 1,\ c = -1,\ x_0 = 2.$
4. $f(x) = 3x^4 - 4x^3 + 1,\ c = 1,\ x_0 = -2.$
5. $f(x) = x^4 + 4x^3 + 4x^2 - 1,\ c = -1,\ x_0 = -3$
6. $f(x) = x^4 + 5x^3 - 3x^2 - 13x + 10,\ c = 1,\ x_0 = 2.$
7. $f(x) = x^4 - 7x^3 + 15x^2 - 13x + 4,\ c = 1,\ x_0 = 3.$
8. $f(x) = x^4 + 2x^3 + x^2 + 2x + 2,\ c = -1,\ x_0 = 2.$
9. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24,\ c = -2,\ x_0 = -1.$
10. $f(x) = 3x^5 - 4x^4 + x,\ c = 1,\ x_0 = -2.$
11. $f(x) = x^5 + 4x^4 + 4x^3 - x,\ c = -1,\ x_0 = -3.$
12. $f(x) = 2x^4 + 4x^3 + 2x^2 + 2x + 2,\ c = -1,\ x_0 = -3.$
13. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8,\ c = 2,\ x_0 = -1.$
14. $f(x) = 2x^5 + 12x^4 + 21x^3 - 2x^2 - 36x - 24,\ c = -2,\ x_0 = 1.$
15. $f(x) = x^5 + 6x^4 + 11x^3 + 2x^2 - 12x - 8,\ c = -2,\ x_0 = -1.$
16. $f(x) = x^6 + 4x^5 + 3x^4 - 8x^3 - 17x^2 - 12x - 3,\ c = -1,\ x_0 = 1.$
17. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24,\ c = -2,\ x_0 = -1.$
18. $f(x) = 2x^5 - 12x^4 + 21x^3 + 2x^2 - 36x - 24,\ c = 2,\ x_0 = 1.$
19. $f(x) = x^6 - 4x^5 + 3x^4 + 8x^3 - 17x^2 + 12x - 3,\ c = 1,\ x_0 = -3.$
20. $f(x) = x^5 + 6x^4 + 13x^3 + 14x^2 + 12x + 8,\ c = -2,\ x_0 = 1.$
21. $f(x) = 2x^5 - 12x^4 + 27x^3 - 34x^2 + 36x - 24,\ c = 2,\ x_0 = 4.$
22. $f(x) = x^6 + 4x^5 + 9x^4 + 16x^3 + 19x^2 + 12x + 3,\ c = -1,\ x_0 = -3.$
23. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8,\ c = 2,\ x_0 = -1.$
24. $f(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16,\ c = -2,\ x_0 = 1.$
25. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8,\ c = 2,\ x_0 = -1.$

26. $f(x) = x^4 - x^3 + x^2 - 3x + 2,\ c = 1,\ x_0 = -1$.

27. $f(x) = x^5 - 3x^4 + 5x^3 - 7x^2 + 6x - 2,\ c = 1,\ x_0 = 3$.

28. $f(x) = x^5 + 3x^4 + 5x^3 + 7x^2 + 6x + 2,\ c = -1,\ x_0 = -3$.

29. $f(x) = x^5 - x^4 + x^3 - 3x^2 + 2x,\ c = 1,\ x_0 = -2$.

30. $f(x) = x^6 - 3x^5 + 5x^4 - 7x^3 + 6x^2 - 2x,\ c = 1,\ x_0 = 2$.

Завдання 13. Розкласти даний дріб на найпростіші дроби над полем дійсних чисел:

а) за допомогою схеми Горнера;

б) методом невизначених коефіцієнтів

1. а) $\frac{x^4}{(x-2)^6}$, б) $\frac{x^2}{x^4-16}$.

2. а) $\frac{9x^4+11x^2-1}{(x+1)^5}$, б) $\frac{x}{(x^2-1)^2}$.

3. а) $\frac{14x^3-3x+1}{(x-1)^4}$, б) $\frac{1}{x^4-16}$.

4. а) $\frac{6x^4+12x-3}{(x-2)^5}$, б) $\frac{x}{(x+1)(x^2+1)^2}$.

5. а) $\frac{x^3-10x+4}{(x+2)^5}$, б) $\frac{x^2}{x^4-16}$.

6. а) $\frac{5x^4+3x^3-1}{(x-3)^5}$, б) $\frac{x}{(x^2+1)^2}$.

7. а) $\frac{x^3}{(x+1)^5}$, б) $\frac{1}{(x+1)(x+2)(x+3)}$.

8. а) $\frac{2x^2-3x+1}{(x-2)^4}$, б) $\frac{2x-3}{(x^2+1)(x-2)}$.

9. а) $\frac{x^3-5x^2+17}{(x-3)^5}$, б) $\frac{x^3-3}{x^4+10x^2+25}$.

10. а) $\frac{3x^3-2x^2+x-1}{(x+1)^5}$, б) $\frac{3x+1}{(x^2+1)^2}$.

11. а) $\frac{2x^3+x^2-x-1}{(x-4)^5}$, б) $\frac{x^2}{x^4+5x^2+4}$.

16. а) $\frac{x^2-x-1}{(x-4)^4}$, б) $\frac{1}{x^4+4}$.

17. а) $\frac{3x^3-2x^2+x+2}{(x-2)^5}$, б) $\frac{1}{(x^2-1)^2}$.

18. а) $\frac{2x^3-x^2-5x+4}{(x+1)^5}$, б) $\frac{1}{x^3+1}$.

19. а) $\frac{x^5+x^2-x+1}{(x+2)^6}$, б) $\frac{x^2}{x^3-1}$.

20. а) $\frac{x^3-3x^2+1}{(x-2)^5}$, б) $\frac{3+x}{(x-1)(x^2+1)}$.

21. а) $\frac{x^4-4x^3+1}{(x+3)^5}$, б) $\frac{x^2}{x^4-1}$.

22. а) $\frac{x^4+22x+12}{(x-3)^5}$, б) $\frac{1}{(x^2+1)^2}$.

23. а) $\frac{3x^5+3x^2-7}{(x+1)^6}$, б) $\frac{1-x}{(x^2+4)^2}$.

24. а) $\frac{x^4-10x^2+1}{(x+1)^5}$, б) $\frac{x^3+4x^2-2}{x^4+x}$.

25. а) $\frac{x^3+x^2-x-1}{(x+2)^5}$, б) $\frac{3}{(x^3+x)}$.

26. а) $\frac{x^4-2x^2+3}{(x+1)^5}$, б) $\frac{x}{x^3-1}$.

12. a) $\frac{2x^4-3x^2+2}{(x+3)^5}$, b) $\frac{1}{(x^2+1)(x+3)}$.

13. a) $\frac{x^4-4x^3+1}{(x-3)^5}$, b) $\frac{x^2}{(x^2+1)(x-3)}$.

14. a) $\frac{2x^5+2x-7}{(x+3)^7}$, b) $\frac{2x-5}{(x^2+1)(x+3)}$.

15. a) $\frac{-2x^5+2x^2+3}{(x+3)^6}$, b) $\frac{3x^2+2x-1}{(x^2+1)^2}$.

27. a) $\frac{x^3-x^2+1}{(x-2)^5}$, b) $\frac{1-x^3}{(x^2+1)^2}$.

28. a) $\frac{x^3-x^2+1}{(x-2)^5}$, b) $\frac{1-x^3}{(x^2+1)^2}$.

29. a) $\frac{-x^3+3x-4}{(x+3)^7}$, b) $\frac{3x^2+5x-5}{(x^2+1)x}$.

30. a) $\frac{-3x^3+11}{(x-2)^5}$, b) $\frac{-4x+5}{(x^3+1)(x+1)}$.

2.2. Звідні та незвідні многочлени. Корені многочлена

Многочлен $f(x)$ степеня n називається **незвідним** над полем P, якщо його не можна подати у вигляді добутку многочленів степеня меншого за n. Над полем дійсних чисел незвідним може бути лише многочлен першого або другого степеня, над полем комплексних чисел незвідним може бути лише многочлен першого степеня. Над скінченним полем P і над полем раціональних чисел Q незвідним може бути многочлен як завгодно великого степеня. Для многочленів над полем раціональних чисел можна використовувати

критерій Айзенштайна: якщо для многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

із цілими коефіцієнтами знайдеться таке просте число p, що:

1) старший коефіцієнт a_0 не ділиться на p;

2) всі інші коефіцієнти a_i діляться на число p;

3) вільний коефіцієнт a_n не ділиться на p^2,

то многочлен $f(x)$ є незвідним над полем раціональних чисел.

Зауважимо, що критерій Айзенштайна є лише достатньою умовою незвідності многочлена над полем раціональних чисел. Незвідний над Q многочлен може цю ознаку не задовольняти (наприклад, многочлен $x+1$).

Кожний многочлен $f(x)$ з кільця $P[x]$ степеня $n \geq 1$ можна подати у вигляді добутку незвідних над полем P многочленів.

Приклад 1. *a*) многочлен x^2+1 є незвідним над полем дійсних чисел R, але над полем комплексних чисел його можна розкласти: $x^2+1=(x-i)(x+i)$.

b) многочлен $16x^4+81$ буде звідним і в кільці $R[x]$: $16x^4+81=$

$$=16x^4+72x^2-72x^2+81=\left(4x^2+9\right)^2-72x^2=\left(4x^2-\sqrt{72}x+9\right)\left(4x^2+\sqrt{72}x+9\right),$$

і в кільці $C[x]$: $16x^4+81=\left(4x^2-\sqrt{72}x+9\right)\left(4x^2+\sqrt{72}x+9\right)=$

$$=\left(x-\frac{3\sqrt{2}}{4}(1-i)\right)\left(x-\frac{3\sqrt{2}}{4}(1+i)\right)\left(x-\frac{3\sqrt{2}}{4}(-1-i)\right)\left(x-\frac{3\sqrt{2}}{4}(-1+i)\right).$$

c) многочлен $16x^{105}+7$ буде незвідним у кільці $Q[x]$ (він задовольняє критерію Айзенштайна для простого числа $p=7$).

Зауважимо, що над полем дійсних чисел кожний многочлен $f(x)$ степеня $n>2$ є звідним. Але дійсні корені многочлен $f(x)$ має лише в тому випадку, коли серед його незвідних множників є лінійні.

Для знаходження всіх раціональних коренів (якщо вони існують) многочлена $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ із цілими коефіцієнтами можна використати наступне **твердження**:

Кожний раціональний корінь многочлена $f(x)$ має вигляд $\frac{p}{q}$, де $p-$ дільник числа a_n, $q-$ дільник числа a_0, $p-mq$ ділить $f(m)$. Зокрема, якщо $a_0=1$, то раціональний корінь є цілим числом.

Приклад 2. Знайдемо всі раціональні корені многочлена

$$f(x)=x^4-2x^3-8x^2+13x-24.$$

Випишемо всі дільники числа 24: $\pm1;\ \pm2;\ \pm3;\pm4;\pm6;\pm8;\pm12;\pm24$.

Раціональні корені потрібно шукати серед цих дільників.

Візьмемо перше число $m=1$: $f(1)=-20\neq 0$. З'ясуємо, для яких дільників p числа 24 число $p-1$ ділить 20. $p\neq -2,+4,-6,\pm 8,\pm 12,\pm 24$. Тепер візьмемо число $m=-1$: $f(-1)=-42\neq 0$. З'ясуємо, для яких з дільників, що залишились $(+2,\pm 3,-4,+6)$, $p+1$ не ділить число 42. $p\neq 3$. Знайдемо $f(2)=-30\neq 0$. Число $p-2=6-2=4$ не ділить 30, $p\neq 6$, також $p\neq -4$. Знайдемо $f(-3)=0$ (тобто -3 є коренем). З'ясуємо кратність кореня $x=-3$:

	1	– 2	– 8	13	–24
– 3	1	– 5	7	– 8	0
– 3	1	– 8	31	$\neq 0$	

Корінь $x=-3$ простий.

Якщо многочлен має дійсні корені, то можна їх **відокремити,** тобто вказати проміжки, на яких многочлен буде мати по одному кореню. Встановити загальну кількість дійсних коренів та відокремити їх можна за допомогою **методу Штурма**. Нехай многочлен $f(x)$ з дійсними коефіцієнтами не має кратних коренів. Для многочлена $f(x)$ побудуємо **послідовність многочленів Штурма** за таким правилом:

$f:=f(x)$; $f_0:=f'(x)$; f_1- остача від ділення f на f_0, взята з протилежним знаком; f_2- остача від ділення f_0 на f_1, взята з протилежним знаком; f_3- остача від ділення f_1 на f_2, взята з протилежним знаком; … ; $f_{k+2}-$ остача від ділення f_{k+1} на f_k, взята з протилежним знаком; …. На деякому кроку ми отримаємо в остачі ненульове число, тобто $f_s:=const\neq 0$. Зауважимо, що на будь–якому етапі можна множити або ділити на довільне додатне число. Ці многочлени задовольняють наступним умовам:

1) останній многочлен f_s не має дійсних коренів та відмінний від нуля;
2) два сусідніх многочлена не мають спільних коренів (не дорівнюють нулю одночасно);
3) якщо многочлен $f_k(x_0)=0$, то в точці x_0 сусідні многочлени f_{k-1} та f_{k+1} мають значення, протилежні за знаком, тобто $f_{k-1}(x_0)\cdot f_{k+1}(x_0)<0$.

Якщо відомі многочлени Штурма, то вибираючи різні значення x_0 заповнюємо табличку. У табличці фіксується лише знак многочлена в даній точці; в останній стовпчик будемо записувати кількість змін знаку при фіксованому x_0 (якщо деякий многочлен у точці x_0 дорівнює нулю, то при підрахунку змін знаку ми на нього не звертаємо уваги):

	f	f_0	f_1	f_2	$\cdots$	f_{k+1}	f_{k+2}	$\cdots$	f_s	S
$-\infty$	$-$	$+$	$-$	$-$	$-$	$-$	$+$	$+$	$+$	$s(-\infty)$
$+\infty$	$+$	$+$	$+$	$-$	$-$	$-$	$-$	$+$	$+$	$s(+\infty)$
0	$+$	$+$	$+$	$+$	$-$	$-$	$+$	$+$	$+$	$s(0)$

Модуль різниці змін знаку $|s(a)-s(b)|$ на інтервалі (a,b) вказує на кількість дійсних коренів на цьому інтервалі. Наприклад, $|s(-\infty)-s(+\infty)|$ вказує на загальну кількість дійсних коренів; $|s(-\infty)-s(0)|$ вказує на кількість від'ємних дійсних коренів; $|s(0)-s(+\infty)|$ вказує на кількість додатних дійсних коренів. Якщо на деякому інтервалі $(a,a+1)$ є кілька коренів, то треба дробити інтервал $(a,a+1)$ далі.

Приклад 3. Відокремити дійсні корені многочлена $f(x)=x^4-6x^2-4x+2$.

$f=x^4-6x^2-4x+2$. $f'=4x^3-12x-4$, тому $f_0=x^3-3x-1$.

Знайдемо остачу від ділення многочлена f на многочлен f_0:

$$\begin{array}{r|l} x^4-6x^2-4x+2 & x^3-3x-1 \\ \underline{x^4-3x^2-x} & \hline x \\ -3x^2-3x+2 & \end{array}$$

Тому $f_1 = 3x^2 + 3x - 2$.

Знайдемо остачу від ділення многочлена f_0 на многочлен f_1:

$$\begin{array}{r|l} 3x^3-9x-3 & 3x^2+3x-2 \\ \underline{3x^3+3x^2-2x} & \hline x-1 \\ -3x^2-7x-3 & \\ \underline{-3x^2-3x+2} & \\ -4x-5 & \end{array}$$

Тому $f_2 = 4x + 5$.

Знайдемо остачу від ділення многочлена f_1 на многочлен f_2:

$$\begin{array}{r|l} 12x^2+12x-6 & 4x+5 \\ \underline{12x^2+15x} & \hline 3x-3 \\ -3x-6 & \text{(помножимо на 4)} \\ -12x-24 & \\ \underline{-12x-15} & \\ -9 & \end{array}$$

Тому $f_3 = 1$.

$f = x^4 - 6x^2 - 4x + 2$, $f_0 = x^3 - 3x - 1$, $f_1 = 3x^2 + 3x - 2$, $f_2 = 4x + 5$, $f_3 = 1$. Заповнюємо таблицю:

x_0	f	f_0	f_1	f_2	f_3	S
∞	+	+	+	+	+	0
$-\infty$	+	–	+	–	+	4
0	+	–	–	+	+	2
1	–	–	+	+	+	1
2	–	+	+	+	+	1
3	+	+	+	+	+	0
–1	+	+	–	+	+	2
–2	+	–	+	–	+	4
–1.5	–	+	+	–	+	3

На інтервалі $(-\infty,\infty)$ многочлен має 4 дійсних корені (різниця змін знаку дорівнює 4);

На проміжку $(-\infty,0)$ многочлен має 2 дійсних корені;

На проміжку $(0,+\infty)$ многочлен має 2 дійсних корені;

На проміжку $(0,+1)$ многочлен має 1 дійсний корінь;

На проміжку $(+1,+2)$ многочлен не має дійсних коренів;

На проміжку $(+2,+3)$ многочлен має 1 дійсний корінь;

На проміжку $(-1,0)$ многочлен не має дійсних коренів;

На проміжку $(-2,-1)$ многочлен має 2 дійсних корені;

На проміжку $\left(-\frac{3}{2},-1\right)$ многочлен має 1 дійсний корінь;

На проміжку $\left(-2,-\frac{3}{2}\right)$ многочлен має 1 дійсний корінь.

Отже, дійсні корені многочлена знаходяться на проміжках : $\left(-2,-\frac{3}{2}\right)$, $\left(-\frac{3}{2},-1\right)$, $(0,+1)$, $(+2,+3)$.

При розв'язування деяких задач доводиться користуватися методами, які застосовуються лише до многочленів, що не мають кратних множників (наприклад метод Штурма – відокремлення дійсних коренів многочлена). Тому розглянемо питання про розкладання многочленів $f(x)$, що має кратні множники, в добуток многочленів, що не мають кратні множники. Нехай $f(x)=a_0 p_1^{k_1}(x)\cdot p_2^{k_2}(x)\cdot\ldots\cdot p_m^{k_m}(x)$ є канонічний розклад многочлена $f(x)$, причому найвища кратність множників дорівнює s. Виберемо в цьому розкладі всі множники $p_i(x)$, кратність k_i яких дорівнює 1. Позначимо добуток всіх цих множників символом $\varphi_1(x)$. Виберемо двократні множники, тобто множники для яких $k_i=2$. Позначимо добуток всіх таких множників взятих у першому степені

символом $\varphi_2(x)$ і т.д. нарешті, виберемо всі множники кратності s, і добуток усіх їх, також узятих лише по одному разу, позначимо символом $\varphi_s(x)$. Якщо ж при цьому многочлен $f(x)$ не має множників кратності k, то вважатимемо, що $\varphi_k(x)=1$. Тоді многочлен $f(x)$ можна записати так: $f(x)=a_0\varphi_1(x)\cdot\varphi_2^2(x)\cdot\varphi_3^3(x)\cdot\ldots f_s^s(x)$. Задачу відшукання такого розкладу називають відокремленням кратних множників.

Зауважимо, що коли многочлен $f(x)$ має дійсні коефіцієнти, то $f'(x)$ та $НСД(f,f')$ також будуть мати дійсні коефіцієнти. Тому в цьому випадку всі обчислення будуть виконуватися в полі дійсних чисел (хоча неявно і використовується розклад на лінійні множники над полем C). Це дає нам наступний метод відокремлення кратних множників:

1. знайдемо похідну $f'(x)$.
2. знайдемо найбільший спільний дільник $НСД(f,f')=d_1$ (Відомо, що многочлен $f(x)$ не має кратних множників тоді й лише тоді, коли він є взаємно простим зі своєю похідною $f'(x)$). Якщо $d_1=1$, то многочлен немає кратних множників.
3. поділимо многочлен $f(x)$ на $d_1(x)$ та позначимо $V_1(x)=\dfrac{f(x)}{d_1(x)}$.
4. запишемо відповідь.

Приклад 4**.** Відокремити кратні множники многочлена

$$f(x)=x^6-6x^4-4x^3+9x^2+12x+4.$$

Розв'язування. Знайдемо спочатку похідну многочлена:

$f'(x)=6x^5-24x^3-12x^2+18x+12$. Тепер за алгоритмом Евкліда знайдемо найбільший спільний дільник многочленів $f(x)$ та $f'(x)$:

$$
\begin{array}{r|l}
x^6-6x^4-4x^3+9x^2+12x+4 & x^5-4x^3-2x^2+3x+12 \\
\hline
x^6-4x^4-2x^3+3x^2+2x & x \\
\hline
-2x^4-2x^3+6x^2+10x+4 & :(-2)
\end{array}
$$

$$
\begin{array}{r|l}
x^5-4x^3-2x^2+3x^2+12 & x^4+x^3-3x^2-5x-2 \\
\hline
x^5+x^4-3x^3-5x^2-2x & x-1 \\
\hline
-x^4-x^3+3x^2+5x+2 & \\
\hline
-x^4-x^3+3x^2+5x+2 & \\
\hline
0 &
\end{array}
$$

Маємо $НСД(f, f') = x^4 + x^3 - 3x^2 - 5x - 2 = d_1$. Далі $d_1' = 4x^3 + 3x^2 - 6x - 5$.

Тепер обчислюємо многочлен $V_1 = \dfrac{f}{d_1}$:

$$
\begin{array}{r|l}
x^6-6x^4-4x^3+9x^2+12x+4 & x^4+x^3-3x^2-5x-2 \\
\hline
x^6+x^5-3x^4-5x^3-2x^2 & x^2-x-2 \\
\hline
-x^5-3x^4+x^3+11x^2+12x+4 & \\
\hline
-x^5-x^4+3x^2+5x^2+2x & \\
\hline
-2x^4-2x^3+6x^2+10x+4 & \\
\hline
-2x^4-2x^3+6x^2+10x+4 & \\
\hline
0 &
\end{array}
$$

Таким чином, многочлен $V_1 = x^2 - x - 2$ немає кратних множників

Завдання 14. Розкласти даний многочлен на незвідні множники

а) над полем R; b) над полем C

1. $x^4 + 16$.
2. $x^4 - 10x^2 + 1$.
3. $x^4 - 81$.
4. $x^6 - 343$.
5. $x^4 + 27$.
6. $x^6 - 256$.
7. $x^4 + 25$.
8. $x^4 + 4$.
9. $x^6 + 1$.
10. $x^4 + 9$.
11. $x^6 - 64$.
12. $x^6 - 8$.
13. $x^6 + 27$.
14. $x^6 + 256$.
15. $x^4 - 625$.

16. $x^4 - 25$.
17. $x^4 + 81$.
18. $x^6 + 8$.
19. $x^4 - 16$.
20. $x^6 + 64$.
21. $x^6 + 125$.
22. $x^6 - 27$.
23. $x^6 + 81$.
24. $x^6 - 1$.
25. $x^6 - 81$.
26. $x^4 + 625$.
27. $x^4 + 121$.
28. $x^4 - 10x^2 + 9$.
29. $x^4 - 196$.
30. $x^6 + 1331$.

Завдання 15. Знайти всі раціональні корені многочлена

1. $8x^4 + 10x^3 + 5x^2 + 10x - 3$
2. $6x^4 - x^3 + 17x^2 - 3x - 3$
3. $8x^4 + 10x^3 + 13x^2 + 20x - 6$
4. $4x^4 + 4x^3 - x^2 + 5x + 3$
5. $8x^4 + 18x^3 + 15x^2 + 7x - 3$
6. $6x^4 + 5x^3 + 16x^2 - 4x - 3$
7. $4x^4 - 4x^3 + 3x^2 - 13x + 6$
8. $8x^4 + 2x^3 - 5x^2 + 13x - 3$
9. $8x^4 - 10x^3 + 5x^2 - 10x - 3$
10. $4x^4 + 8x^3 + 7x^2 + 8x + 3$
11. $6x^4 + x^3 + 17x^2 + 3x - 3$
12. $4x^4 + 8x^3 + 11x^2 + 16x + 6$
13. $8x^4 - 10x^3 + 13x^2 - 20x - 6$
14. $6x^4 + x^3 + 11x^2 + 2x - 2$
15. $8x^4 - 16x^3 + 10x^2 - 8x + 3$
16. $4x^4 - 8x^3 + 7x^2 - 8x + 3$
17. $4x^4 - 8x^3 + 11x^2 - 16x + 6$
18. $4x^4 - 4x^3 - x^2 - 5x + 3$
19. $8x^4 - 18x^3 + 15x^2 - 7x - 3$
20. $4x^4 + 4x^3 + 3x^2 + 13x + 6$
21. $8x^4 - 2x^3 - 5x^2 - 13x - 3$
22. $8x^4 + 10x^3 + 21x^2 + 30x - 9$
23. $4x^4 - 8x^3 + 15x^2 - 24x + 9$
24. $4x^4 - 12x^3 + 15x^2 - 11x + 3$
25. $6x^4 - 5x^3 + 16x^2 + 4x - 3$
26. $8x^4 - 10x^3 + 21x^2 - 30x - 9$
27. $4x^4 + 8x^3 + 15x^2 + 24x + 9$
28. $4x^4 + 12x^3 + 15x^2 + 11x + 3$
29. $8x^4 + 16x^3 + 10x^2 + 8x + 3$
30. $6x^4 - x^3 + 11x^2 - 2x - 2$

Завдання 16. Відокремити дійсні корені многочлена $f(x)$

1. $f(x) = 4x^4 - 12x^2 + 8x - 1$.
2. $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 1$.
3. $f(x) = 2x^5 - 10x^3 + 10x - 3$.
4. $f(x) = x^4 - 3x^2 + 1$.
5. $f(x) = x^4 + 6x^3 - 4x^2 + 4x + 2$.
6. $f(x) = x^4 - 7x^2 + 10$.
7. $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$.
8. $f(x) = x^4 - 6x^3 + 11x^2 - 6x$.
9. $f(x) = x^4 - 12x^2 - 16x - 4$.
10. $f(x) = -2x^5 + 10x^3 - 10x - 3$.

11. $f(x) = x^5 - 5x^3 + 5x^2 + 10x - 3$.
12. $f(x) = 3x^4 - 6x^2 + 1$.
13. $f(x) = x^4 - 5x^2 + 6$.
14. $f(x) = x^4 - 2x^3 - 3x^2 + 2x + 1$.
15. $f(x) = x^4 - 12x^2 + 16x - 4$.
16. $f(x) = x^4 - 8x^2 + 7$.
17. $f(x) = 2x^4 - 8x^3 + 8x^2 - 1$.
18. $f(x) = x^4 - 6x^2 + 1$.
19. $f(x) = x^4 - 4x^2 + x + 1$.
20. $f(x) = x^4 - 4x^2 + 2$.
21. $f(x) = x^4 - 2x^3 - 3x^2 + 2x + 1$.
22. $f(x) = x^4 - 5x^2 + 4$.
23. $f(x) = x^4 - 4x^3 - 4x^2 + 4x + 5$.
24. $f(x) = x^4 - 6x^2 - 4x + 2$.
25. $f(x) = 2x^4 - 6x^3 - 4x + 3$.
26. $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$.
27. $f(x) = x^4 - 10x^2 + 21$.
28. $f(x) = 3x^4 + 11x^2 + 2$.
29. $f(x) = x^4 - 6x^2 + 2$.
30. $f(x) = 4x^4 - x^2 - 4$.

Завдання 17

1. Довести, що для довільних натуральних чисел m, n і p многочлен $x^{3m} + x^{3n+1} + x^{3p+2}$ ділиться на $x^2 + x + 1$.
2. Визначити, для яких чисел A і B тричлен $Ax^4 + Bx^3 + 1$ ділиться на $(x-1)^2$.
3. Довести, що многочлен $f(x) = x^{10} - x^5$ ділиться на $x - a$ для довільного $a \in Z_5$ у кільці $Z_5[x]$.
4. Знайти суму квадратів коренів многочлена $x^n + a_1 x^{n-1} + \ldots + a_n$.
5. Для яких натуральних чисел m, n і p многочлен $x^{3m} + x^{3n+1} + x^{3p+2}$ ділиться на $x^4 + x^2 + 1$?

6. Для яких натуральних чисел m многочлен $x^{2m}+x^m+1$ ділиться на x^2+x+1?
7. Для яких натуральних чисел m многочлен $(x+1)^m-x^m-1$ ділиться на x^2+x+1?
8. Яку умову повинні задовольняти числа a і b, щоб многочлен x^5+ax^3+b мав подвійний корінь, відмінний від нуля.
9. Для яких натуральних чисел m многочлен $(x+1)^m-x^m-1$ ділиться на $(x^2+x+1)^2$?
10. Знайти всі такі трійки чисел (a,b,c), щоб коренями многочлена x^3-ax^2+bx-c були числа a,b,c.
11. Для яких значень a число -1 буде коренем многочлена x^5-ax^2-ax+1 кратності не менше 2?
12. Визначити, для яких A і B тричлен $Ax^{n+1}+Bx^n+1$ ділиться на $(x-1)^2$.
13. Для яких натуральних чисел m, n і p многочлен $x^{3m}+x^{3n+1}+x^{3p+2}$ ділиться на x^2+x+1?
14. Довести, що многочлен $f(x)=x^5-x$ ділиться на $x-a$ для довільного $a\in Z_5$ в кільці $Z_5[x]$.
15. Для яких натуральних чисел m многочлен $(x+1)^m+x^m+1$ ділиться на x^2+x+1?
16. Які умови повинні задовольняти числа a, b і c, щоб многочлен $x^5+10ax^3+5bx+c$ мав потрійний корінь, відмінний від нуля?
17. Для яких натуральних чисел m многочлен $(x+1)^m+x^m+1$ ділиться на $(x^2+x+1)^2$?
18. Яку умову повинні задовольняти числа a, b і c, щоб один із коренів многочлена x^3+ax^2+bx+c дорівнював сумі двох інших коренів.

19. Довести, що многочлен $f(x)=x^7-x$ ділиться на $x-a$ для довільного $a\in Z_7$ в кільці $Z_7[x]$.

20. Яку умову повинні задовольняти числа a, b, c, і d, щоб сума якихось двох коренів многочлена $x^4+ax^3+bx^2+cx+d$ дорівнювала сумі двох інших коренів.

21. Яку умову повинні задовольняти числа a, b, c, і d, щоб добуток якихось двох коренів многочлена $x^4+ax^3+bx^2+cx+d$ дорівнював добутку двох інших коренів.

22. Для яких цілих значень a один корінь многочлена $36x^3-12x^2-5x+a$ дорівнює сумі двох інших? Знайти ці корені.

23. Сума двох коренів многочлена $2x^3-x^2-7x+a$ дорівнює 1. Визначити параметр a.

24. Яку умову повинні задовольняти числа b і d, щоб для коренів x_1, x_2, x_3 многочлена x^3+bx+d виконувалось співвідношення $x_3=\frac{1}{x_1}+\frac{1}{x_2}$?

25. Довести, що многочлен $f(x)$ із цілими коефіцієнтами не має цілих коренів, якщо $f(0)$ і $f(1)$ – непарні числа.

26. Визначити многочлен найменшого степеня, який дає в остачі $2x$ при діленні на $(x-1)^2$ і $3x$ при діленні на $(x-2)^3$.

27. Визначити многочлен найменшого степеня, який дає в остачі x^2+x+1 при діленні на $x^4-2x^3-2x^2+10x-7$ і $2x^2-3$ при діленні на $x^4-2x^3-3x^2+13x-10$.

28. Чи утворюють корені многочлена $2x^4+8x^3+7x^2-2x-2$ арифметичну прогресію?

29. При яких значеннях a і b многочлен $f(x)=x^3+2x^2+ax+b$ ділиться на многочлен $g(x)=x^2+x+ab$ у кільці $Q[x]$?

30. Довести, що многочлен $f(x)=(x+a+b)^{2001}-x^{2001}-a^{2001}-b^{2001}$ ділиться на двочлени $f_1(x)=x+a$ та $f_2(x)=x+b$ у кільці $C[x]$.

Розділ 3. МНОГОЧЛЕНИ ВІД БАГАТЬОХ ЗМІННИХ

3.1. Симетричні многочлени

Многочлен $f(x_1, x_2, \ldots, x_n)$, що залежить від змінних $x_1, x_2, \ldots, x_n$, називають **симетричним**, якщо будь–яка підстановка множини $\{x_1, x_2, \ldots, x_n\}$ переводить цей многочлен у себе.

Приклад 1. Многочлени $x_1^3x_2 + x_1^3x_3 + x_2^3x_1 + x_2^3x_3 + x_3^3x_1 + x_3^3x_2$,

$x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5$, $(x_1 + x_2 - x_3)(x_1 + x_3 - x_2)(x_2 + x_3 - x_1)$

будуть симетричними.

Симетричні многочлени $\sigma_1 = x_1 + x_2 + \ldots + x_n$,

$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n \ ,$$

$$\ldots\ldots\ldots$$

$$\sigma_n = x_1x_2x_3 \ldots x_n$$

називають **елементарними симетричними многочленами.**

В силу того, що сума, різниця і добуток симетричних многочленів над довільним полем P є також симетричним многочленом над цим полем, симетричні многочлени над цім полем утворюють кільце.

Кожний симетричний многочлен $f(x_1, x_2, \ldots, x_n)$ можна подати, причому єдиним способом, у вигляді многочлена $g(\sigma_1, \sigma_2, \ldots, \sigma_n)$ від елементарних симетричних многочленів $\sigma_1, \sigma_2, \ldots, \sigma_n$. При цьому потрібно враховувати, що коли $ax_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}$ – старший член симетричного многочлена $f(x_1, x_2, \ldots, x_n)$ порядку m, тоді многочлен $f(x_1, x_2, \ldots, x_n)$ містить член $ax_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}$; для показників виконується умова

$k_1 \geq k_2 \geq k_3 \geq \ldots \geq k_n$, існує многочлен $h_i = c_i \sigma_1^{t_1 - t_2} \sigma_2^{t_2 - t_3} \ldots \sigma_n^{t_n}$, де c – якась стала, $t_1 \geq t_2 \geq t_3 \geq \ldots \geq t_n$, $t_1 + k_2 + t_3 + \ldots + t_n = m$, тоді $f = \sum h_i$.

Приклад 2. Виразити через основні симетричні многочлени многочлен

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

Старший член цього многочлена $x_1^3 x_2 x_3 x_4$. Випишемо показники старших членів многочленів:

t_1	t_2	t_3	t_4	Комбінація основних симетричних многочленів
3	1	1	1	$\sigma_1^2 \sigma_4$
2	2	2	0	$a\sigma_3^2$
2	2	1	1	$c\sigma_2 \sigma_4$

Нагадаємо, що $\sigma_1 = x_1 + x_2 + x_3 + x_4$,

$\sigma_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4$,

$\sigma_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4$,

$\sigma_4 = x_1 x_2 x_3 x_4$.

Многочлен f можна записати у вигляді $f = \sigma_1^2 \sigma_4 + a\sigma_3^2 + c\sigma_2 \sigma_4$. Визначимо числові коефіцієнти, надаючи окремі значення x_1, x_2, x_3, x_4:

x_1	x_2	x_3	x_4	f	σ_1	σ_2	σ_3	σ_4	f
1	1	1	0	1	3	3	1	0	$1 = a$
1	1	–1	–1	8	0	–2	0	1	$8 = -2c$

Розв'яжемо систему $\begin{cases} 1 = a \\ 8 = -2c \end{cases}$. Отже, $f = \sigma_1^2 \sigma_4 + \sigma_3^2 - 4\sigma_2 \sigma_4$.

Завдання 18. Виразити через основні симетричні многочлени заданий многочлен

1. $x_1^4x_2x_3 + x_1x_2^4x_3 + x_1x_2x_3^4$.
2. $x_1^5 + x_2^5 + x_3^5 + x_4^5$.
3. $x_1^2x_2^2x_3 + x_1^2x_2x_3^2 + x_1x_2^2x_3^2$.
4. $2x_1^3 + 2x_2^3 + 2x_3^3 + 2x_4^3 - x_1x_2x_3x_4$.
5. $x_1^3x_2 + x_1^3x_3 + x_2^3x_1 + x_2^3x_3 + x_3^3x_1 + x_3^3x_2$.
6. $x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5$.
7. $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$.
8. $(x_1^2 + x_2 + x_3)(x_1 + x_2^2 + x_3)(x_1 + x_2 + x_3^2)$.
9. $x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3$.
10. $x_1^2x_2^2 + x_1^2x_3^2 + x_1^2x_4^2 + x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2$.
11. $(x_1^2 + 2x_2x_3)(x_2^2 + 2x_1x_3)(x_3^2 + 2x_1x_2)$.
12. $x_1^2x_2x_3x_4 + x_1x_2^2x_3x_4 + x_1x_2x_3^2x_4 + x_1x_2x_3x_4^2$.
13. $x_1^4x_2 + x_1^4x_3 + x_2^4x_1 + x_3^4x_1 + x_2^4x_3 + x_3^4x_2$.
14. $(x_1 + x_2 - 3x_3)(x_1 + x_3 - 3x_2)(x_2 + x_3 - 3x_1)$.
15. $x_1^3x_2^2 + x_1^3x_3^2 + x_2^3x_1^2 + x_2^3x_3^2 + x_3^3x_1^2 + x_3^3x_2^2$.
16. $x_1^2x_2^2x_3^2 + x_1^2x_2^2x_4^2 + x_1^2x_3^2x_4^2 + x_2^2x_3^2x_4^2$.
17. $(x_1 + x_2 - x_3)(x_1 + x_3 - x_2)(x_2 + x_3 - x_1)$.
18. $x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4$.
19. $x_1^3x_2^3 + x_1^3x_3^3 + x_1^3x_4^3 + x_2^3x_3^3 + x_2^3x_4^3 + x_3^3x_4^3$.
20. $x_1^3 + x_2^3 + x_3^3 + x_4^3 - 5x_1x_2x_3x_4$.
21. $x_1^5 + x_2^5 + x_3^5 + 3x_1^2x_2^2 + 3x_1^2x_3^2 + 3x_2^2x_3^2$.
22. $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2x_1x_2x_3$.
23. $(2x_1 - x_2 - x_3)(2x_2 - x_1 - x_3)(2x_3 - x_2 - x_1)$.
24. $x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2$.
25. $x_1^3x_2x_3x_4 + x_1x_2^3x_3x_4 + x_1x_2x_3^3x_4 + x_1x_2x_3x_4^3$.
26. $x_1^3 + x_2^3 + x_3^3 - 2x_1^2x_2^2 - 2x_1^2x_3^2 - 2x_2^2x_3^2$.
27. $(x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2)$.
28. $(x_1^2 + 2x_2 + 2x_3)(2x_1 + x_2^2 + 2x_3)(2x_1 + 2x_2 + x_3^2)$.
29. $2x_1^4x_2 - 5x_1^2x_2 + 2x_1x_2^4 + 5x_1x_2^2$.
30. $(x_1 + x_2 - 2x_3)(x_1 + x_3 - 2x_2)(x_2 + x_3 - 2x_1)$.

Додаток 1. Питання колоквіуму

2 семестр

1. Бінарні операції, асоціативність, комутативність та дистрибутивність бінарних операцій, основні властивості бінарних операцій.
2. Означення групи, приклади груп.
3. Властивості груп. Довести:
   a) рівність $a^m \cdot a^n = a^{m+n}$;
   b) що кожне з рівнянь $ax = b$, $ya = b$ має єдиний розв'язок;
   c) що з $ab = ac$ випливає $b = c$.
4. Підгрупи та їх властивості. Критерії того, що підмножина групи є підгрупою.
5. Циклічна група; приклади циклічних груп. Теорема про будову підгруп циклічної групи.
6. Група підстановок, зображення підстановок у вигляді добутку транспозицій.
7. Ізоморфізм груп; показати, що відношення ізоморфізму є відношенням еквівалентності.
8. Довести, що при ізоморфізмі нейтральний елемент переходить в нейтральний елемент, а обернений елемент – в обернений.
9. Теорема, що коли множина з бінарною операцією ізоморфна групі, то вона є групою.
10. Теорема: кожна нескінченна циклічна група ізоморфна адитивній групі цілих чисел, кожна скінченна група порядку n ізоморфна групі поворотів правильного n - кутника.
11. Теорема Келі.
12. Розклад групи за підгрупою.
13. Теорема Лагранжа та наслідки з неї.
14. Кільця, приклади кілець, кільце лишків.
15. Основні властивості кілець, кільце з одиницею, дільники одиниці.

16. Дільники нуля. Область цілісності. Приклади областей цілісності.
17. Підкільце. Критерій того, що підмножина кільця є підкільцем.
18. Ізоморфізм кілець, властивості ізоморфних кілець.
19. Поле, властивості полів. Поле лишків Z_p. Довести, що поле не містить дільників нуля.
20. Характеристика поля, її властивості. Довести, що в полі характеристики p $(a+b)^p = a^p + +b^p$.
21. Підполе, розширення поля, ізоморфізм полів.

Додаток 2. Варіанти контрольних та самостійних робіт

Самостійна робота (2 семестр)

Варіант 1

1. Чи буде групою множина всіх комплексних коренів фіксованого степеня n з 1 відносно операції множення.
2. Чи буде операція $*$ асоціативна на множини Z, $x * y = x^2 + y^2$.
3. Знайти порядок елемента групи:

a) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 6 & 2 & 5 & 3 & 7 \end{pmatrix} \in S_8$; b) $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(Z)$.

4. Розв'язати рівняння та систему рівнянь :

a) $x^2 - \left(1+\sqrt{7}\right)x - 26 + 10\sqrt{7} = 0$ у полі $Q\left(\sqrt{7}\right)$; b) $\begin{cases} x + y = 11, \\ y - x = 15. \end{cases}$ в кільці Z_{24}.

5. Чи буде відображення гомоморфізмом? $f : R^* \to R^*$, $f(x) = -|x|$.
6. Чи буде кільце Z_{163} полем? Знайти обернений елемент до елемента $a = 57$.

Варіант 2

1. Чи буде групою множина всіх комплексних коренів усіх степенів з 1 відносно операції множення.
2. Чи буде операція $*$ асоціативна на множини N, $x * y = x^y y$.
3. Знайти порядок елемента групи:

a) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 7 & 6 & 4 & 5 & 8 & 2 \end{pmatrix} \in S_8$; b) $g = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(C)$.

4. Розв'язати рівняння та систему рівнянь :

a) $x^2 + \left(4 - 2\sqrt{7}\right)x + 7 - 4\sqrt{7} = 0$ у полі $Q\left(\sqrt{7}\right)$; b) $\begin{cases} x + y = 11, \\ y - x = 5. \end{cases}$ в кільці Z_{20}.

5. Чи буде відображення гомоморфізмом? $f : C^* \to C^*$, $f(z) = |z|$.
6. Чи буде кільце Z_{150} полем? Знайти обернений елемент до елемента $a = 101$.

Контрольна робота (2 семестр)

Варіант 1

1. Розкласти на незвідні множники над полем R многочлен $x^4 + 2x^2 + 25$.
2. Знайти раціональні корені многочлена $6x^6 + x^5 + 5x^4 + 6x^2 + x + 5$.
3. Знайти значення многочлена $-3x^6 - 11x^5 + 5x^4 - 2x^2 + 3x - 15$ та всіх його похідних при $x_0 = -2$.
4. Розв'язати рівняння $3x^2 + \left(5 - 9\sqrt{5}\right)x - 15\sqrt{5} = 0$ в полі $Q(\sqrt{5})$.
5. Знайти елемент, обернений до елемента 53 в кільці Z_{241}.
6. Розкласти в ланцюговий дріб $\frac{1811}{409}$.
7. Знайти остачу від ділення числа $\left(5284040^{175718} + 189679\right)^{521158}$ на число 81.

Варіант 2

1. Розкласти на незвідні множники над полем R многочлен $x^4 - 2x^2 + 36$.
2. Знайти раціональні корені многочлена $6x^6 - x^5 - 2x^4 + 6x^2 - x - 2$.
3. Знайти значення многочлена $2x^6 + 4x^5 - 5x^3 + 3x^2 - 17x + 35$ та всіх його похідних при $x_0 = -1$.
4. Розв'язати систему рівнянь $\begin{cases} \bar{x} + \bar{y} = \overline{97}, \\ \bar{y} - \bar{x} = \overline{25} \end{cases}$ в кільці Z_{168}.
5. Знайти елемент, обернений до елемента 59 в кільці Z_{367}.
6. Розкласти в ланцюговий дріб $\sqrt{125}$.
7. Знайти остачу від ділення числа $\left(2283658^{208563} + 12680\right)^{58247}$ на число 55.

Додаток 3. Цікаві задачі

1. Доведіть, що довільна скінченна підгрупа H групи C^* є циклічною.
2. Нехай p, q – прості числа та $p < q$. Доведіть, що кожна група порядку pq містить підгрупу порядку p (порядку q).
3. Доведіть, що кожна некомутативна група порядку 8 ізоморфна або групі D_4, або групі кватерніонів Q_8.
4. Доведіть, що кожна група порядку p^4 містить абелеву підгрупу порядку p^3.
5. Доведіть, що група A_5 не містить підгруп порядків 15, 20 і 30.
6. Знайдіть кількість силовських p – підгруп у групі S_{2p}.
7. Довести, що коли елемент x кільця $\Re$ є нільпотентним, то елемент $(1-x)$ є оборотним *(елемент a кільця $\Re$ називається нільпотентним, якщо для деякого натурального числа n маємо $a^n = 0$).*
8. Довести, що Z_m містить нільпотентні елементи тоді й лише тоді, коли m ділиться на квадрат натурального числа більшого за 1.
9. Довести: кожне п’яти елементне кільце або ізоморфне Z_5, або є кільцем з нульовим множенням.

Додаток 4. Умовні позначення

$НСД(a,b)$ – найбільший спільний дільник чисел a та b;

$НСК(a,b)$ – найменше спільне кратне чисел a та b;

A^T – матриця, транспонована до матриці A;

$|A|$ – потужність множини A;

$|a|$ – порядок елемента a;

$\langle a,b,...,c \rangle$ – група породжена елементами $a,b,...,c$;

$A \subseteq B$ – A є підмножиною B;

$A \subset B$ – A є власною підмножиною B (тобто $A \subseteq B$ і $A \neq B$);

A_n – знакозмінна група всіх парних підстановок степеня n;

C – множина, або адитивна група, або поле комплексних чисел;

C^* – мультиплікативна група поля комплексних чисел;

C_n – група за множенням усіх комплексних коренів степеня n з 1 або група поворотів правильного n-кутника;

$C(a)$ – клас спряженості елемента a;

D_n – група симетрій правильного n-кутника;

E_n – одинична матриця порядку n (матриця порядку n, в якій на головній діагоналі стоять одиниці, а решта елементів – нулі);

$GL_n(P)$ – повна лінійна група степеня n – група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P;

$GL_n(Z)$ – група за множенням усіх невироджених цілочисельних матриць порядку n, обернені до яких також є цілочисельними;

G/H – фактор-група групи G за нормальною підгрупою H;

$H \lhd G$ – H є нормальною підгрупою H;

K_4 – четверна група Кляйна – група підстановок $\{e,(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$;

$M_{n\times m}(P)$ – адитивна група матриць розміру $n \times m$ з коефіцієнтами з поля P;

$M_n(P)$ – адитивна група квадратних матриць порядку n з коефіцієнтами з поля P;

N_0 – множина цілих невід'ємних чисел;

$P[x]$ – кільце многочленів від x з коефіцієнтами з поля P;

$P_n[x]$ – множина всіх многочленів від x степеня не більшого ніж n з коефіцієнтами з поля P;

$P_n[x_1,...,x_k]$ – множина всіх многочленів степеня не більшого ніж n від змінних $x_1,...,x_k$ з коефіцієнтами з поля P;

Q_8 – група кватерніонів;

Q^+ – мультиплікативна група всіх додатних раціональних чисел;

Q^* – мультиплікативна група поля раціональних чисел;

R^+ – мультиплікативна група всіх додатних дійсних чисел;

R^* – мультиплікативна група поля дійсних чисел;

$SL_n(P)$ – спеціальна лінійна група степеня n – підгрупа матриць із $GL_n(P)$, визначник яких дорівнює 1;

S_n – симетрична група всіх підстановок степеня n;

$T_n(P)$ – група за множенням усіх невироджених верхніх трикутних матриць порядку n з коефіцієнтами з поля P;

U_n – група комплексних коренів степеня n з 1;

Z_n – множина, або адитивна група, або кільце класів лишків за модулем натурального числа n;

Z_n^* – мультиплікативна група оборотних класів лишків за модулем числа n;

$\tau(n)$ – кількість всіх натуральних дільників числа n;

$S(n)$ – сума всіх кількість всіх натуральних дільників числа n;

$\varphi(n)$ – функція Ойлера – кількість натуральних чисел менших за n та взаємно простих з ним.

Додаток 5. Таблиця простих чисел для $n \le 4861$

2	233	547	877	1229	1597	1993	2371	2749	3187	3583	4003	4421
3	239	557	881	1231	1601	1997	2377	2753	3191	3593	4007	4423
5	241	563	883	1237	1607	1999	2381	2767	3203	3607	4013	4441
7	251	569	887	1249	1609	2003	2383	2777	3209	3613	4019	4447
11	257	571	907	1259	1613	2011	2389	2789	3217	3617	4021	4457
13	263	577	911	1277	1619	2017	2393	2791	3221	3623	4027	4463
17	269	587	919	1279	1621	2027	2399	2797	3229	3631	4049	4481
19	271	593	929	1283	1627	2029	2411	2801	3251	3637	4051	4483
23	277	599	937	1289	1637	2039	2417	2803	3253	3643	3307	4493
29	281	601	941	1291	1657	2053	2423	2819	3257	3659	4057	4507
31	283	607	947	1297	1663	2063	2437	2833	3259	3671	4073	4513
37	293	613	953	1301	1667	2069	2441	2837	3271	3673	4079	4517
41	307	617	967	1303	1669	2081	2447	2843	3299	3677	4091	4519
43	311	619	971	1307	1693	2083	2459	2851	3301	3691	4093	4523
47	313	631	977	1319	1697	2087	2467	2857	3313	3697	4099	4547
53	317	641	983	1321	1699	2089	2473	2861	3319	3701	4111	4549
59	331	643	991	1327	1709	2099	2477	2879	3323	3709	4127	4561
61	337	647	997	1361	1721	2111	2503	2887	3329	3719	4129	4567
67	347	653	1009	1367	1723	2113	2521	2897	3331	3727	4133	4583
71	349	659	1013	1373	1733	2129	2531	2903	3343	3733	4139	4591
73	353	661	1019	1381	1741	2131	2539	2909	3347	3739	4153	4597
79	359	673	1021	1399	1747	2137	2543	2917	3359	3761	4157	4621
83	367	677	1031	1409	1753	2141	2549	2927	3361	3767	4159	4637
89	373	683	1033	1423	1759	2143	2551	2939	3371	3769	4177	4639
97	379	691	1039	1427	1777	2153	2557	2953	3373	3779	4201	4643
101	383	701	1049	1429	1783	2161	2579	2957	3389	3793	4211	4649
103	389	709	1051	1433	1787	2179	2591	2963	3391	3797	4217	4651
107	397	719	1061	1439	1789	2203	2593	2969	3407	3803	4219	4657
109	401	727	1063	1447	1801	2207	2609	2971	3413	3821	4229	4663
113	409	733	1069	1451	1811	2213	2617	2999	3433	3823	4231	4673
127	419	739	1087	1453	1823	2221	2621	3001	3449	3833	4241	4679
131	421	743	1091	1459	1831	2237	2633	3011	3457	3847	4243	4691
137	431	751	1093	1471	1847	2239	2647	3019	3461	3851	4253	4703
139	433	757	1097	1481	1861	2243	2657	3023	3463	3853	4259	4721
149	439	761	1103	1483	1867	2251	2659	3037	3467	3863	4261	4723
151	443	769	1109	1487	1871	2267	2663	3041	3469	3877	4271	4451
157	449	773	1117	1489	1873	2269	2671	3049	3491	3881	4273	4729
163	457	787	1123	1493	1877	2273	2677	3061	3499	3889	4283	4733
167	461	797	1129	1499	1879	2281	2683	3067	3511	3907	4289	4751
173	463	809	1151	1511	1889	2287	2687	3079	3517	3911	4297	4759
179	467	811	1153	1523	1901	2293	2689	3083	3527	3917	4327	4783
181	479	821	1163	1531	1907	2297	2693	3089	3529	3919	4337	4787
191	487	823	1171	1543	1913	2309	2699	3109	3533	3923	4339	4789
193	491	827	1181	1549	1931	2311	2707	3119	3539	3929	4349	4793
197	499	829	1187	1553	1933	2333	2711	3121	3541	3931	4357	4799
199	503	839	1193	1559	1949	2339	2713	3137	3547	3943	4363	4801
211	509	853	1201	1567	1951	2341	2719	3163	3557	3947	4373	4813
223	521	857	1213	1571	1973	2347	2729	3167	3559	3967	4391	4817
227	523	859	1217	1579	1979	2351	2731	3169	3571	3989	4397	4831
229	541	863	1223	1583	1987	2357	2741	3181	3581	4001	4409	4861

Основна література

1. Завало С.Т., Костарчук В.Н., Хацет Б.І . Алгебра і теорія чисел. В 2–х ч. –К.: Вища шк., 1974, 1977, 1980.
2. Завало С.Т. Курс алгебри. К.: Вища шк., 1985.
3. Курош А.Г. Курс высшей алгебры. М., Наука, 1971.
4. Ван дер Варден Б.Л. Алгебра. – М.: Наука, 1976.
5. Калужнин Л.А. Введение в общую алгебру. – М.: Наука, 1973.
6. Кострикин А.И. Введение в алгебру. – М.: Наука, 1977.
7. Скорняков Л.А. Элементы алгебры. – М.: Наука, 1965.
8. Фаддеев Д.К. Лекции по алгебре. – М.: Наука, 1984.
9. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. М.: Наука, 1977.
10. Проскуряков И.В. Сборник задач по линейной алгебре. – М.: Наука, 1965.