Київський національний університет імені Тараса Шевченка

О. О. Безущак, О. Г. Ганюшкін

ЗАВДАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ З АЛГЕБРИ І ТЕОРІЇ ЧИСЕЛ (***ТЕОРІЯ КІЛЕЦЬ І ПОЛІВ***)

Київ - 2020

О. О. Безущак, О. Г. Ганюшкін. Завдання до практичних занять з алгебри і теорії чисел (теорія кілець і полів): для студентів університетів. – К. : Видавничо-поліграфічний центр “Київський університет”, 2020. – 137 с.

Рецензенти: д-р фіз.-мат. наук, проф. М. Ф. Городній
д-р фіз.-мат. наук, проф. Б. В. Олійник

Рекомендовано до друку вченою радою механіко-математичного факультету Київського національного університету імені Тараса Шевченка (протокол № 7 від 26 грудня 2019 року)

Зміст

Передмова

Навчальні завдання повністю охоплюють теми практичних занять, що проводяться при вивченні на другому курсі механіко-математичного факультету нормативного курсу алгебри і теорії чисел.

Кожне завдання складається з чотирьох частин. Спочатку наводяться приклади розв'язання типових задач. Друга й третя частини містять задачі, що розглядаються на практичних заняттях (задачі другої частини є обов'язковими, третьої — розраховані на сильніших студентів), а четверта — задачі для домашнього завдання. Важчі задачі позначено зірочками, причому кількість зірочок є мірою складності задачі. До задач наведено відповіді, а для багатьох з них — і вказівки до розв'язання.

При посиланні на задачу використовується подвійна нумерація: перша цифра — номер заняття, а друга — номер задачі.

Заняття 1. Кільця та спеціальні елементи в них

Необхідні поняття. Кільцем $(K;+,\cdot)$ називається непорожня множина K з двома бінарними діями — *додаванням* $+$ і *множенням* $\cdot$, які задовольняють такі умови:

1) щодо додавання K є абелевою групою (яка називається *адитивною групою* кільця K);

2) множення *асоціативне*: для довільних a,b,c $\;ab\cdot c=a\cdot bc$;

3) додавання і множення пов'язані *дистрибутивними* законами: для довільних $a,b,c\in K$

$$a(b+c)=ab+ac \quad \text{і} \quad (b+c)a=ba+ca\,.$$

У залежності від додаткових умов, які накладаються на множення, виділяють ті чи інші класи кілець. Найчастіше вимагають:

1) наявність *одиниці*: існує такий елемент $1\in K$, що $1\cdot a=a\cdot 1=a$ для довільного $a\in K$;

2) *комутативність* множення: для довільних a,b $\;ab=ba$.

Якщо якась із цих умов виконується, то говорять відповідно про кільця *з одиницею* і *комутативні* кільця.

Якщо K_1 і K_2 — кільця, то декартовий добуток

$$K_1\times K_2=\{(a,b)\mid a\in K_1, b\in K_2\}$$

множин K_1 і K_2 із додаванням і множенням, визначеними правилами:

$$(a_1,b_1)+(a_2,b_2):=(a_1+a_2,b_1+b_2),\quad (a_1,b_1)\cdot(a_2,b_2):=(a_1a_2,b_1b_2)\,,$$

буде кільцем, яке називається *прямою сумою* кілець K_1 і K_2 і позначається $K_1\oplus K_2$.

Елемент a кільця K з одиницею 1 називається *лівим* (*правим*) *дільником одиниці*, якщо існує такий елемент b, що $ab=1$ (відповідно $ba=1$). Елемент, який є одночасно і лівим і правим дільником одиниці, називають просто *дільником одиниці* (або *оборотним* елементом).

Неодноелементне кільце K з одиницею, в якому кожний ненульовий елемент є оборотним, називається *тілом* або *кільцем з діленням*. Комутативне тіло називається *полем*.

Елемент a називається *лівим* (*правим*) *дільником нуля*, якщо існує такий елемент $b\neq 0$, що $ab=0$ (відповідно $ba=0$). Елемент, який є

одночасно і лівим і правим дільником нуля, називають просто *дільником нуля*. Якщо в кільці K єдиним дільником нуля є 0, то кажуть, що K — *кільце без дільників нуля*.

Неодноелементне комутативне кільце з одиницею і без дільників нуля називається *областю цілісності*.

Елемент a кільця k називається *нільпотентним*, якщо $a^k = 0$ для деякого натурального числа k. Найменше таке k називається *класом нільпотентності* елемента a.

Елемент e кільця називається *ідемпотентом*, якщо $e^2 = e$.

Кільця K і P називаються *ізоморфними*, якщо існує таке взаємно однозначне відображення $\varphi : K \to P$, що для довільних $a, b \in K$ виконуються такі дві умови:

$$\varphi(a+b) = \varphi(a) + \varphi(b); \qquad \varphi(ab) = \varphi(a)\varphi(b)\,.$$

Відображення φ називаються *ізоморфізмом* кільця K на кільце P.

Необхідні твердження. **1.** Непорожня підмножина $A \subseteq R$ буде підкільцем кільця K тоді й лише тоді, коли A замкнена відносно додавання, множення і взяття протилежного елемента.

2. У кільці з одиницею множина K^* оборотних елементів утворює групу відносно множення.

3. У кільці можна скорочувати на елемент a справа (зліва) тоді й лише тоді, коли a не є правим (лівим) дільником нуля. Зокрема, скорочувати на довільний ненульовий елемент можна лише в кільці без дільників нуля.

Приклади розв'язання типових задач

Задача 1. *Чи утворює кільце відносно звичайних додавання і множення така числова множина*:
а) $K_1 = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$, *б)* $K_2 = \{m + n\sqrt[3]{2} \mid m, n \in \mathbb{Z}\}$*?*

Розв'язання. Обидві множини є підмножинами поля дійсних чисел. Тому щоб відповісти на питання задачі, досить перевірити замкненість цих множин відносно додавання, взяття протилежного елемента і множення.

а) Для довільних $x = m + n\sqrt{2}$, $y = p + q\sqrt{2}$ із K_1 маємо:
1) $x + y = (m + p) + (n + q)\sqrt{2}$. Позаяк $m + p$ та $n + q$ — цілі числа, то $x + y \in K_1$.

2) $-x = -(m + n\sqrt{2}) = (-m) + (-n)\sqrt{2} \in K_1$.
3) $xy = (m + n\sqrt{2})(p + q\sqrt{2}) = (mp + 2nq) + (mq + np)\sqrt{2} \in K_1$.
Отже, множина K_1 є замкненою відносно додавання, взяття протилежного елемента і множення, а тому є кільцем.

b) Для довільних $x = m + n\sqrt[3]{2}$, $y = p + q\sqrt[3]{2}$ із K_2 маємо:
1) $x + y = (m + p) + (n + q)\sqrt[3]{2} \in K_2$.
2) $-x = -(m + n\sqrt[3]{2}) = (-m) + (-n)\sqrt[3]{2} \in K_2$.
Отже, замкненість відносно додавання і взяття протилежного елемента є. Лишилося перевірити замкненість відносно множення:
3) $xy = (m + n\sqrt[3]{2})(p + q\sqrt[3]{2}) = mp + (mq + np)\sqrt[3]{2} + nq\sqrt[3]{4}$.
Із замкненості K_2 відносно додавання та взяття протилежного елемента і того, що $mp+(mq+np)\sqrt[3]{2} \in K_2$, випливає, що xy буде належати K_2 тоді й лише тоді, коли $nq\sqrt[3]{4} \in K_2$. Зокрема, множині K_2 повинно належати число $\sqrt[3]{4}$ (якщо взяти $n = q = 1$). Це означає, що існують такі цілі числа a і b, що $\sqrt[3]{4} = a + b\sqrt[3]{2}$. Але тоді $\sqrt[3]{2}$ буде коренем многочлена $x^2 - bx - a$ із цілими коефіцієнтами. Із другого боку, $\sqrt[3]{2}$ є коренем многочлена $x^3 - 2$. Тому з рівності

$$x^3 - 2 = (x^2 - bx - a)(x + b) + (a + b^2)x + (ab - 2)$$

випливає, що $\sqrt[3]{2}$ є коренем многочлена $(a + b^2)x + (ab - 2)$ із цілими коефіцієнтами. Але число $\sqrt[3]{2}$ — ірраціональне, тому цей многочлен повинен бути нульовим. Із системи рівнянь

$$a + b^2 = 0, \quad ab - 2 = 0$$

отримуємо: $b^3 = -ab = -2$. Але це суперечить тому, що число b є цілим.
Таким чином, припущення, що $\sqrt[3]{4} \in K_2$, приводить до суперечності. Отже, множина K_2 не замкнена відносно множення і не є кільцем. □

Задача 2. *Чи утворює кільце відносно звичайних додавання і множення матриць*
a) множина K_1 усіх вироджених матриць із $M_n(\mathbb{R})$;
b) множина K_2 усіх симетричних матриць із $M_n(\mathbb{R})$?

Розв'язання. Якщо $n = 1$, то $K_1 = \{0\}$, а $K_2 = \mathbb{R}$. Отже, в обох випадках отримуємо кільце.
Далі розглянемо випадок $n > 1$.

а) Легко бачити, що сума двох вироджених матриць із $M_2(\mathbb{R})$ може бути виродженою. Наприклад,

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

Приклад легко узагальнюється на довільне $n > 1$. Тому при $n > 1$ множина K_1 не є замкненою відносно додавання, а тому не є кільцем.

b) Якщо A і B — симетричні матриці, тобто $A^\top = A$ і $B^\top = B$, то $(A + B)^\top = A^\top + B^\top = A + B$ і $(-A)^\top = -A^\top = -A$. Отже, множина K_2 замкнена відносно додавання та взяття протилежного елемента.

Нехай тепер $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ і $B = \begin{pmatrix} x & y \\ y & z \end{pmatrix}$ — дві симетричні матриці із $M_2(\mathbb{R})$. Тоді

$$AB = \begin{pmatrix} ax + by & ay + bz \\ bx + cy & by + cz \end{pmatrix}.$$

Для симетричності матриці AB необхідно, щоб виконувалася рівність

$$ay + bz = bx + cy.$$

Але легко підібрати значення параметрів так, щоб рівність не виконувалась. Наприклад, можна взяти $b = 0$, $a = y = 1$, $c = 2$. Позаяк приклад легко узагальнюється на довільне $n > 1$, то при $n > 1$ множина K_2 не є замкненою відносно додавання, а тому не є кільцем. □

Задача 3. *Опишіть усі дільники нуля і всі дільники одиниці в кільці* $M_n(\mathbb{R})$.

Розв'язання. Дільники одиниці — це оборотні елементи. Тому в кільці $M_n(\mathbb{R})$ дільниками одиниці будуть усі невироджені матриці і тільки вони.

Нехай тепер матриця A вироджена і $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, …, $\boldsymbol{v}_n$ — її рядки. Виродженість A означає, що існують такі числа α_1, α_2, …, α_n, які не всі

дорівнюють 0, що $\alpha_1\boldsymbol{v}_1 + \alpha_2\boldsymbol{v}_2 + \cdots + \alpha_n\boldsymbol{v}_n = \mathbf{0}$. Але тоді

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \cdot A = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1\boldsymbol{v}_1 + \alpha_2\boldsymbol{v}_2 + \cdots + \alpha_n\boldsymbol{v}_n \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix} = 0.$$

Позаяк перша матриця ненульова, то A є правим дільником нуля. Аналогічно доводиться, що A є лівим дільником нуля. Таким чином, у кільці $M_n(\mathbb{R})$ кожна вироджена матриця є дільником нуля. □

Задача 4. *Покажіть, що в кільці всіх лінійних перетворень простору $P[x]$ многочленів з коефіцієнтами з поля P існують необоротні елементи φ і ψ, добуток $\varphi\psi$ яких є оборотним.*

Розв'язання. Ми покажемо навіть трохи більше: у кільці $P[x]$ існують необоротні лінійні перетворення φ і ψ, добуток $\varphi\psi$ яких є одиницею кільця $P[x]$ — тотожним перетворенням.

Як відомо з математичного аналізу, в кільці $P[x]$ оператор "інтегрування" $\varphi : \sum\limits_{k\geq 0} a_k x^k \mapsto \sum\limits_{k\geq 0} \frac{a_k}{k+1} x^{k+1}$ і оператор диференціювання $\psi : f(x) \mapsto f'(x)$ є лінійним перетвореннями. Перше перетворення не є сюр'єктивним (образ $\operatorname{Im} A$ не містить многочленів нульового степеня), а друге не є ін'єктивним (в ядро $\operatorname{Ker} B$ потрапляють усі многочлени нульового степеня). Тому обидва перетворення не є оборотними. Але їх добуток $\varphi\psi$ є тотожним перетворенням. Справді, для довільного многочлена $\sum\limits_{k\geq 0} a_k x^k$

$$\sum_{k\geq 0} a_k x^k \overset{A}{\mapsto} \sum_{k\geq 0} \frac{a_k}{k+1} x^{k+1} \overset{B}{\mapsto} \sum_{k\geq 0} a_k x^k.$$

□

Задача 5. *Доведіть, що в скінченному кільці з одиницею кожен елемент є або правим дільником одиниці, або правим дільником нуля.*

Розв'язання. Якщо відображення $x \mapsto xa$ є бієкцією, то існує таке b, що $ba = 1$. Отже, в цьому випадку a є правим дільником одиниці. Якщо ж відображення $x \mapsto xa$ не є бієкцією, то існують такі $x_1 \neq x_2$, що $x_1a = x_2a$. Але тоді $(x_1 - x_2)a = 0$ і a є правим дільником нуля. □

Зауваження. Зрозуміло, що аналогічна властивість виконується і для лівих дільників нуля та одиниці.

Задача 6. *Доведіть, що в кільці з* 1 *і без дільників* 0 *кожен елемент, який є оборотним з одного боку, буде оборотним і з другого боку.*

Розв'язання. Це випливає з такого ланцюжка імплікацій:

$$ab = 1 \Rightarrow bab = b \Rightarrow (ba - 1)b = 0 \Rightarrow ba = 1.$$ □

Задача 7. *Нехай* $n = p_1^{k_1} \cdots p_m^{k_m}$*, де* $p_1, \ldots, p_m$ *— попарно різні прості числа. Знайдіть у кільці* $\mathbb{Z}_n$ *усі нільпотентні елементи та підрахуйте їх кількість.*

Розв'язання. Якщо a не ділиться на просте число p, то й жоден степінь a не буде ділитися на p. Тому a може бути нільпотентним елементом кільця $\mathbb{Z}_n$ лише тоді, коли a ділиться на кожне з простих чисел $p_1, \ldots, p_m$. Позаяк ці числа попарно різні, то a повинно ділитись на їх добуток $p_1 \cdots p_m$. Із другого боку ця умова є й достатньою: якщо a ділиться на $p_1 \cdots p_m$ і $k = \max(k_1, \ldots, k_m)$, то a^k ділиться на число $p_1^k \cdots p_m^k$, яке кратне n. Але тоді $a^k \equiv \pmod n$, тобто a є нільпотентним елементом кільця $\mathbb{Z}_n$.

Таким чином, a нільпотентним елементом кільця $\mathbb{Z}_n$ тоді й лише тоді, коли ділиться на $p_1 \cdots p_m$. Тому загальна кількість нільпотентних елементів у кільці $\mathbb{Z}_n$ дорівнює

$$\frac{n}{p_1 \cdots p_m} = p_1^{k_1 - 1} \cdots p_m^{k_m - 1}.$$ □

Задача 8. *Нехай* $|M| = n$*. Підрахуйте кількість нільпотентних елементів у кільці функцій* $\mathrm{Map}(M, \mathbb{Z}_{36})$.

Розв'язання. Те, що функція $f : M \to K$ є нільпотентним елементом кільця $\mathrm{Map}(M, K)$, означає, що існує таке k, що для кожного $x \in M$ буде $f^k(x) = (f(x))^k = 0$. Тобто значеннями нільпотентної функції $f : M \to K$ можуть бути лише нільпотентні елементи кільця K.

У випадку кільця $\mathbb{Z}_{36}$ ця умова буде й достатньою. Справді, із розв'язання попередньої задачі випливає, що елемент a кільця $\mathbb{Z}_{36}$ буде нільпотентним тоді й лише тоді, коли він ділиться на 6. Але якщо a ділиться на 6, то a^2 ділиться на 36, тобто є нулем у кільці $\mathbb{Z}_{36}$. Тому для кожної функції $f : M \to \mathbb{Z}_{36}$, значеннями якої є нільпотентні елементи кільця $\mathbb{Z}_{36}$, виконується рівність $f^2 = 0$.

Таким чином, функція $f : M \to \mathbb{Z}_{36}$ буде нільпотентною тоді й лише тоді, коли вона відображає M у множину N нільпотентних елементів кільця $\mathbb{Z}_{36}$. Із розв'язання попередньої задачі випливає, що N містить 6 елементів. Тому кільце $\mathrm{Map}(M, \mathbb{Z}_{36})$ містить 6^n нільпотентних елементів. □

Задача 9. *Доведіть, що кільце верхніх трикутних матриць із $M_n(\mathbb{R})$ і кільце нижніх трикутних матриць із $M_n(\mathbb{R})$ ізоморфні.*

Розв'язання. Якщо $n = 1$, то ці кільця збігаються. Тому далі вважаємо, що $n > 1$.

Перше, що приходить на думку спробувати — це транспонування. І справді, при транспонуванні верхні трикутні матриці переходять у нижні трикутні, це відображення є взаємно однозначним, матриця, транспонована до суми, є сумою транспонованих, а транспонована до добутку — добутком транспонованих. Заважає лише одна "дрібниця": матриця, транспонована до добутку, є добутком транспонованих у зворотному порядку. А при ізоморфізмі порядок множників має зберігатися. Позаяк множення верхніх трикутних матриць не є комутативним (наприклад $\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}2 & 2\\ 0 & 2\end{pmatrix}$, а $\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix} = \begin{pmatrix}2 & 4\\ 0 & 2\end{pmatrix}$), то, на жаль, транспонування не є ізоморфізмом даних кілець.

Наступну пропозицію підказує лінійна алгебра: якщо матриця лінійного перетворення $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^N$ у базі $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ є верхньою трикутною, то матриця цього ж перетворення у базі $\boldsymbol{e}_n, \boldsymbol{e}_{n-1}, \ldots, \boldsymbol{e}_1$ буде нижньою трикутною:

$$\text{якщо } [\mathcal{A}] = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{12} \\ 0 & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_{nn} \end{pmatrix}, \text{ то } [\mathcal{A}]' = \begin{pmatrix} a_{1n} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{2n} & a_{2,n-1} & \ldots & 0 \\ a_{1n} & a_{1,n-1} & \ldots & a_{11} \end{pmatrix}.$$

Матрицею переходу від бази $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ до бази $\boldsymbol{e}_n, \boldsymbol{e}_{n-1}, \ldots, \boldsymbol{e}_1$

є матриця

$$S = \begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 1 & \dots & 0 & 0 \end{pmatrix},$$

в якої на побічній діагоналі стоять одиниці, а всі інші елементи нульові. При переході до нової бази матриця A лінійного перетворення переходить у матрицю $S^{-1}AS$. Легко перевіряється, що відображення $\varphi : A \mapsto S^{-1}AS$ є ізоморфізмом кільця верхніх трикутних матриць на кільце нижніх трикутних матриць. Справді, φ є взаємно однозначним і

$$\varphi(A+B) = S^{-1}(A+B)S = S^{-1}AS + S^{-1}BS = \varphi(A) + \varphi(B),$$
$$\varphi(AB) = S^{-1}ABS = S^{-1}AS \cdot S^{-1}BS = \varphi(A) \cdot \varphi(B). \qquad \square$$

Основні задачі

10. Чи утворює кільце відносно звичайних додавання і множення така множина цілих чисел:
a) множина невід'ємних цілих чисел;
b) множина всіх тих цілих чисел, які діляться на 2 або 3;
c) множина всіх тих цілих чисел, у десятковому записі яких зустрічаються лише парні цифри?

11. Чи утворює кільце з одиницею відносно додавання і множення матриць така множина матриць із $M_n(\mathbb{R})$:
a) усі невироджені матриці;
b) усі діагональні матриці;
c) усі матриці з раціональним визначником?

12. Чи утворює кільце відносно звичайних додавання і множення така числова множина:
a) $\{m + \sqrt[3]{2}n + \sqrt[3]{4}k \mid m, n, k \in \mathbb{Z}\}$,
b) $\{m + \varepsilon n \mid m, n \in \mathbb{Z},\ \varepsilon$ — первісний корінь степеня 3 з 1$\}$?

13. Чи утворює кільце відносно звичайних додавання і множення многочленів множина тих многочленів $f(x)$ із $\mathbb{Z}[x]$,
a) в яких вільний член ділиться на 10;
b) в яких сума коефіцієнтів дорівнює 0;
c) в яких коефіцієнт при x дорівнює 0;
d) в яких коефіцієнт при x^2 дорівнює 0?

14. Доведіть, що множина 2^M всіх підмножин фіксованої множини M є комутативним асоціативним кільцем з одиницею, якщо як додавання взяти симетричну різницю

$$A \triangle B := (A \setminus B) \cup (B \setminus A)$$

підмножин, а як множення — перетин підмножин.

15. Нехай K_1 і K_2 — підкільця кільця K.
a) Доведіть, що перетин $K_1 \cap K_2$ також є підкільцем.
b) За яких умов об'єднання $K_1 \cup K_2$ буде підкільцем?

16. Опишіть усі дільники 0 і всі дільники 1 в кільці a) $\mathbb{Z}$; b) $\mathbb{Z}_n$.

17. З'ясуйте, чи є даний елемент кільця $\mathbb{Z}_{30}$ дільником 1, і в разі позитивної відповіді знайдіть обернений до нього:
a) $\overline{12}$; b) $\overline{13}$; c) $\overline{14}$; d) $\overline{15}$; e) $\overline{17}$.

18. Опишіть усі дільники 0 і всі дільники 1 в кільці: a) $\mathbb{R}[x]$; b) всіх функцій $\mathbb{R} \to \mathbb{R}$; c) всіх неперервних функцій $\mathbb{R} \to \mathbb{R}$.

19. Нехай P — підкільце кільця K і $a \in P$. Які з наступних імплікацій є правильними:
a) якщо a є дільником 0 у кільці P, то a є дільником 0 у кільці K;
b) якщо a є дільником 0 у кільці K, то a є дільником 0 у кільці P?

20. З'ясуйте, чи може в кільці
a) сума необоротних елементів бути оборотним елементом;
b) сума дільників нуля бути оборотним елементом;
c) сума оборотних елементів бути дільником нуля.

21. Нехай у кільці K для кожного ненульового елемента $a \in K$ існує єдиний такий елемент $b \in K$, що $aba = a$. Доведіть, кільце K не містить дільників нуля.

22. Доведіть, що кільце $\mathbb{Z}_n$ містить нетривіальні нільпотентні елементи тоді й лише тоді, коли n ділиться на квадрат якогось простого числа.

23. Нехай $|M| = n$. Підрахуйте кількість нільпотентних елементів у кільці функцій $\mathrm{Map}(M, \mathbb{Z}_{48})$.

24. Доведіть, що в кільці з одиницею для кожного ідемпотента e елемент $1 - e$ також буде ідемпотентом.

25. Нехай R — комутативне кільце і $e \in R$. Доведіть, що множина eR буде кільцем із одиницею e тоді й лише тоді, коли e — ідемпотент.

26. Нехай $n > 1$ — вільне від квадратів ціле число. Доведіть, що кільця $\{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$ і $\left\{\left(\begin{smallmatrix} x & y \\ ny & x \end{smallmatrix}\right) \mid x, y \in \mathbb{Z}\right\}$ ізоморфні.

27. Доведіть, що кільця $\mathbb{Z}[x]$ і $\mathbb{Q}[x]$ — не ізоморфні.

Додаткові задачі

28. З'ясуйте, для яких натуральних чисел k множина

$$\mathbb{Z}_{(k)} = \left\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}, k \nmid n\right\}$$

буде кільцем відносно звичайних дій додавання і множення.

29* Чи утворює кільце відносно звичайних додавання і множення функцій множина всіх дійсних періодичних функцій?

30. Чи утворює кільце множина $\mathbb{R}[x]$ всіх дійсних многочленів відносно звичайного додавання і суперпозиції $(f \circ g)(x) = g(f(x))$ в ролі множення? Якщо ні, то які саме аксіоми кільця не виконуються?

31. Доведіть, що множина $\operatorname{End} A$ ендоморфізмів абелевої групи A утворює кільце відносно додавання і множення, визначених правилами: для всіх $a \in A \quad (\varphi + \psi)(a) = \varphi(a) + \psi(a), \quad (\varphi \cdot \psi)(a) = \psi(\varphi(a))$.

32. Чи можна на множині $\mathbb{R}^+$ визначити таку бінарну дію $\circ$, щоб множина $\mathbb{R}^+$ зі звичайним множенням у ролі додавання і дією $\circ$ в ролі множення утворювала кільце?

33. a) Доведіть, що в кільцях з одиницею комутативність додавання є наслідком інших аксіом кільця.

b) Доведіть, що коли не вимагати існування одиниці, то комутативність додавання не випливає з решти аксіом кільця.

34. Опишіть усі підкільця з одиницею кільця $\mathbb{Q}$.

35. Доведіть, що кільце з циклічною адитивною групою є комутативним.

36. Опишіть усі дільники 0 і всі дільники 1 в кільці $M_n(\mathbb{Z})$.

37. Нехай K — скінченне кільце з 1. Доведіть, що
a) кожний елемент з K, який є оборотним з одного боку, буде оборотним і з другого боку;
b) кожний елемент з K, який є дільником 0 з одного боку, буде дільником 0 і з другого боку.

38. a) Доведіть, що в скінченному кільці з одиницею кожен елемент є або дільником одиниці, або дільником нуля.

b) Наведіть приклад нескінченного кільця з одиницею, в якому твердження із попереднього пункту не виконується.

39.* Нехай K — кільце з 1 і елемент $1 - ab$ — оборотний. Доведіть, що елемент $1 - ba$ — також оборотний.

40. Знайдіть у кільці $\mathbb{R}[[x]]$ степеневих рядів елемент, обернений до елемента: a) $1 - x$; b) $1 + 2x$; c)** $1 + x + x^2$.

41. Опишіть усі нільпотентні елементи в кільці $M_2(\mathbb{R})$.

42. Доведіть, що в скінченному кільці для кожного елемента a існує таке натуральне число n, що a^n є ідемпотентом.

43. Доведіть, що три кільця: K_1 — дійсних функцій, що перетворюються в 0 на даній підмножині $\varnothing \neq D \subseteq \mathbb{R}$, K_2 — тригонометричних многочленів, і $\mathbb{R}[x]$ — попарно неізоморфні.

44. Наведіть приклад такого ненульового кільця K з одиницею, яке ізоморфне кільцю $K[x]$.

45. Доведіть, що коли $n \neq m$, то $n\mathbb{Z} \not\supseteq m\mathbb{Z}$.

46. Нехай p — просте число.
a) Доведіть, що кожне кільце порядку p є комутативним.
b) Доведіть, що кожне кільце з одиницею порядку p^2 є комутативним.
c) Наведіть приклад некомутативного кільця порядку p^3.

Домашнє завдання

47. Чи утворює кільце множина тих раціональних чисел, у нескоротному записі яких
a) знаменник є парним числом;
b) чисельник є парним числом;
c) знаменник є непарним числом?

48. Чи утворює кільце з одиницею відносно звичайних додавання і множення функцій множина тих дійсних функцій $f(x)$, які задовольняють умову

a) $f(5) = 0$; b) $f(5) = 1$; c) $f(0) = f(1)$.

49. З'ясуйте, які з матриць

$$a)\begin{pmatrix}1 & 1 & 1\\ 1 & 2 & 2\\ 2 & 3 & 5\end{pmatrix};\quad b)\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix};\quad c)\begin{pmatrix}0 & 1 & 1\\ 1 & -1 & -1\\ 1 & -1 & -2\end{pmatrix};\quad d)\begin{pmatrix}1 & 1 & 1\\ 1 & -1 & 1\\ 0 & 1 & 1\end{pmatrix}$$

є дільниками 0 або дільниками 1 в кільці $M_3(\mathbb{Z})$.

50. Знайдіть усі дільники 0, дільники 1 і нільпотентні елементи в кільці із зад. 14.

51. Які елементи кільця $\mathbb{Z}_{24}$ будуть a) дільниками 0; b) дільниками 1; c) нільпотентними?

52. Доведіть, що множина дійсних матриць вигляду $\left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right)$ утворює кільце, ізоморфне полю $\mathbb{C}$.

Заняття 2. Ідеали, гомоморфізми, факторкільця

Необхідні поняття. Підкільце I кільця K називається *лівим ідеалом*, якщо $KI \subseteq I$ (тобто $ab \in I$ для довільних $a \in K$ і $b \in I$). Аналогічно, якщо $IK \subseteq I$, то I називається *правим ідеалом*. Якщо I є одночасно і лівим, і правим ідеалом, то I називається *двостороннім ідеалом*, або просто *ідеалом*.

Кожне кільце K має два *тривіальні* ідеали: саме кільце K (його називають *одиничним* ідеалом) і *нульовий ідеал* $\{0\}$ (який часто позначають просто 0). Неодиничні ідеали ще називають *власними*.

Найменший з лівих (правих, двосторонніх) ідеалів кільця, які містять даний елемент a, називається лівим (правим, двостороннім) *головним* ідеалом, породженим елементом a. Породжений елементом a двосторонній головний ідеал позначається (a).

Відображення $\varphi : K \to P$ з кільця K в кільце P називається *гомоморфізмом*, якщо для довільних $a, b \in K$ виконуються такі дві умови:

$$\varphi(a+b) = \varphi(a) + \varphi(b); \qquad \varphi(ab) = \varphi(a)\varphi(b)\,.$$

(тобто гомоморфізм кілець має бути як гомоморфізмом їх адитивних груп, так і мультиплікативних напівгруп).

Позаяк гомоморфізм кілець одночасно є гомоморфізмом їх адитивних груп, то $\varphi(0) = 0$ і $\varphi(-a) = -\varphi(a)$. Однак одиниця кільця K (якщо вона є) не зобов'язана переходити в одиницю кільця P.

Ядром гомоморфізму $\varphi : K \to P$ називається множина $\operatorname{Ker}\varphi = \{x \in K \mid \varphi(x) = 0\}$, а образом — множина $\operatorname{Im}\varphi = \{\varphi(x) \mid x \in K\}$.

Ін'єктивний (відповідно сюр'єктивний, бієктивний) гомоморфізм кілець називається *мономорфізмом* (відповідно *епіморфізмом*, *ізоморфізмом*). Гомоморфізм кільця в себе називається *ендоморфізмом*, а ізоморфізм на себе — *автоморфізмом*.

Для кожного двостороннього ідеалу I кільця K на K можна визначити так зване *відношення конґруентності за модулем ідеалу* I: елементи a і b конґруентні за модулем I тоді й лише тоді, коли $a - b \in I$ (записують $a \equiv b \pmod{I}$ або $a \equiv b\ (I)$). Відношення конґруентності за модулем I є відношенням еквівалентності. Клас еквівалентності, що містить елемент a, позначають $\overline{a}$ або $a + I$ і називають *класом лишків* за модулем ідеалу I. Він має вигляд $\overline{a} = a + I = \{a + x \mid x \in I\}$.

На множині K/I всіх класів лишків за модулем ідеалу I визначаються додавання і множення за такими правилами:

$$(a+I)+(b+I)=(a+b)+I, \qquad (a+I)\cdot(b+I)=ab+I.$$

Множина K/I із так визначеними додаванням і множенням буде кільцем, яке називається *факторкільцем* кільця K за ідеалом I.

Відображення $x \mapsto \overline{x}=x+I$ називається *канонічним епіморфізмом* кільця K на факторкільце K/I.

Необхідні твердження. **1.** Підмножина I кільця K буде лівим (правим) ідеалом кільця K тоді й лише тоді, коли вона є підгрупою адитивної групи кільця і витримує множення на елементи кільця зліва (справа).

2. У кільці K з одиницею породжений елементом a лівий (відповідно правий) головний ідеал має вигляд Ka (відповідно aK).

3. Якщо відображення $\varphi : K \to K'$ є гомоморфізмом кілець, то його образ $\varphi(K)$ є підкільцем кільця K'. Якщо K — кільце з одиницею, то $\varphi(K)$ також є кільцем з одиницею (яка, однак, може не збігатися з одиницею кільця K').

4. Якщо $\varphi : K \to P$ — гомоморфізм кілець, а $K' \subseteq K$ і $P' \subseteq P$ — підкільця, то $\varphi(K')$ є підкільцем в P, а повний прообраз $\varphi^{-1}(P')$ — підкільцем в K.

5. Нехай $\varphi : K \to R$ — гомоморфізм кілець. a) Якщо J — ідеал кільця R, то його повний прообраз $\varphi^{-1}(J)$ є ідеалом кільця K.
b) Якщо гомоморфізм φ є сюр'єктивним і I — ідеал кільця K, то його образ $\varphi(I)$ є ідеалом кільця R.

6. Нехай I — ідеал кільця K. Тоді для кожного підкільця $K \supseteq L \supseteq I$ факторкільце $\overline{L}=L/I$ є підкільцем факторкільця K/I для кожного ідеалу $K \supseteq J \supseteq I$ факторкільце $\overline{J}=J/I$ є ідеалом факторкільця K/I.

7. Основна теорема про гомоморфізм кілець. Якщо відображення $\varphi : K \to P$ є гомоморфізмом кілець, то ядро $\operatorname{Ker}\varphi$ гомоморфізму є двостороннім ідеалом кільця K, а образ $\operatorname{Im}\varphi$ ізоморфний факторкільцю $K/\operatorname{Ker}\varphi$.

Приклади розв'язання типових задач

Задача 1. *З'ясуйте, чи утворює ідеал у кільці $\mathbb{Z}[x]$ множина тих многочленів $f(x)=a_0+a_1x+\cdots+a_nx^n$ із $\mathbb{Z}[x]$, які задовольняють таку умову:*

a) a_0 *ділиться на* 5;
b) $a_1 = 0$;
c) $f(x)$ *є парним многочленом.*

Розв'язання. Кільце $\mathbb{Z}[x]$ комутативне, тому поняття лівого, правого й двостороннього ідеалів збігаються.

Перевіримо спочатку, чи утворює відповідна множина I многочленів підгрупу адитивної групи кільця $\mathbb{Z}[x]$. Для цього необхідно й достатньо, щоб вона була замкненою відносно додавання і взяття протилежного елемента. Нехай $f(x) = a_0 + a_1x + \cdots + a_nx^n$ і $g(x) = b_0+b_1x+\cdots+b_mx^m$ — два многочлени з I. Тоді $-f(x) = -a_0-a_1x-\cdots-a_nx^n$ і $f(x)+g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$.

a) Якщо a_0 і b_0 діляться на 5, то кожне з чисел $-a_0$ і $a_0 + b_0$ також діляться на 5.

b) Якщо $a_1 = 0$ і $b_1 = 0$, то $-a_1 = 0$ і $a_1 + b_1 = 0$.

c) Якщо многочлени $f(x)$ і $g(x)$ — парні, то $-f(x)$ і $f(x) + g(x)$ — також парні многочлени.

Таким чином, в усіх трьох випадках множина I є підгрупою адитивної групи кільця. Перевіримо тепер, чи витримує множина I множення на елементи кільця. Нехай $f(x)=a_0 + a_1x +\cdots+ a_nx^n$ належить I, а многочлен $g(x) = b_0 + b_1x + \cdots + b_mx^m$ — довільний. Тоді $f(x)g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots$.

a) Якщо a_0 ділиться на 5, то a_0b_0 також ділиться на 5.

b) Якщо a_0 ділиться на 5, але $a_1 = b_0 = 1$, то $a_1b_0 + a_0b_1$ при діленні на 5 дає в остачі 1, отже, на 5 не ділиться.

c) Якщо $f(x)$ — парний многочлен, то многочлен $x \cdot f(x)$ буде непарним.

Отже, у випадку a) множина I витримує множення на елементи кільця, а у випадках b) і c) — ні. Тому множина I буде ідеалом лише у випадку a). □

Задача 2. *a) Доведіть, що множина нільпотентних елементів комутативного кільця утворює ідеал.*
b) Наведіть приклад некомутативного кільця, в якому множина нільпотентних елементів не утворює ідеал.

Розв'язання. a) Нехай a і b — нільпотентні елементи, тобто для деяких натуральних n і m $a^n = b^m = 0$. Тоді $(-a)^n = 0$ і з комутативності

кільця випливає, що

$$(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}.$$

Але для кожного i добуток $a^i b^{n+m-i}$ дорівнює 0, бо або $i > 0$ (і тоді $a^i = 0$), або $n+m-i \geq m$ (і тоді $b^{n+m-i} = 0$). Тому $(a+b)^{n+m} = 0$ і $a+b$ є нільпотентним елементом.

Отже, множина нільпотентних елементів є замкненою відносно додавання і взяття протилежного елемента, а тому є підгрупою адитивної групи кільця.

Крім того в комутативному кільці для довільного елемента c маємо: $(ac)^n = a^n \cdot c^n = 0 \cdot c^n = 0$, тобто множина нільпотентних елементів витримує і множення на довільні елементи кільця. Тому ця множина є ідеалом.

b) Візьмемо у певному сенсі "найпростіше" некомутативне кільце: $M_2(\mathbb{R})$, а в ньому "найпростіші" нільпотентні матриці $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ і $B = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $A^2 = B^2 = 0$. Тоді для їх суми $C = A+B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ і довільного натурального n маємо: $C^{2n} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ і $C^{2n+1} = C$. Отже, матриця C не є нільпотентною, тобто множина нільпотентних матриць із $M_2(\mathbb{R})$ не замкнена відносно додавання і не є підгрупою адитивної групи кільця $M_2(\mathbb{R})$. А тому ця множина не є ідеалом. □

Задача 3. *З'ясуйте, для яких натуральних чисел n множина необоротних елементів із $\mathbb{Z}_n$ утворює ідеал.*

Розв'язання. Елемент a кільця $\mathbb{Z}_n$ буде необоротним тоді й лише тоді, коли a і n не є взаємно прості. Зокрема, буде необоротним кожен простий дільник числа n. Далі розглянемо два випадки.

1) n має принаймні два різні прості дільники p і q. Найбільший спільний дільник цих чисел дорівнює 1, а тому існують такі цілі числа u і v, що $up + vq = 1$. Це означає, що підгрупа адитивної групи кільця $\mathbb{Z}_n$, яка містить елементи p і q, повинна містити й оборотний елемент 1. А тому в цьому випадку множина необоротних елементів не є підгрупою адитивної групи кільця і не є ідеалом.

2) n має єдиний простий дільник p, тобто має вигляд $n = p^k$. У цьому випадку елемент $a \in \mathbb{Z}_n$ буде необоротним тоді й лише тоді, коли a ділиться на p. Але сума й різниця двох таких елементів і довільне кратне такого елемента також будуть ділитися на p. Отже, множина

необоротних елементів є підгрупою адитивної групи кільця і витримує множення на довільний елемент кільця, тобто є ідеалом. □

Задача 4. *Доведіть, що асоціативне кільце K із ненульовим множенням буде тілом тоді й лише тоді, коли воно не має нетривіальних односторонніх ідеалів.*

Розв'язання. Необхідність умови доводиться просто. Справді, нехай I — ненульовий лівий ідеал тіла K. Візьмемо в K довільний ненульовий елемент a. У тілі для нього існує обернений елемент a^{-1}. Але тоді I повинен містити елемент $a^{-1} \cdot a = 1$, а далі з $b \cdot 1 = b$ випливає, що I містить усі елементи $b \in K$. Отже, якщо лівий ідеал I — ненульовий, то $I = K$.

Для правих ідеалів доведення аналогічне.

Достатність. Припустимо, що кожен нетривіальний односторонній ідеал I кільця K збігається з K. Для довільного елемента $a \neq 0$ множина Ka буде лівим ідеалом. За умовою або $Ka = 0$, або $Ka = K$. Але в першому випадку множина $\{0, a\}$ також буде лівим ідеалом, причому ненульовим. Тому має бути $\{0, a\} = K$. Але тоді K є кільцем із ненульовим множенням, що суперечить умові. Отже, лишається лише випадок $Ka = K$. Аналогічно з відсутності нетривіальних правих ідеалів виводиться, що $aK = K$.

Із рівності $Ka = K$ випливає, що існує елемент 1_a, для якого $1_a \cdot a = a$. Далі із рівності $aK = K$ випливає, що для кожного $b \in K$ існує такий елемент c, що $ac = b$. Але тоді

$$1_a \cdot b = 1_a \cdot ac = 1_a a \cdot c = ac = b.$$

Отже, в K є ліва одиниця 1_a. Аналогічно доводиться, що в K є права одиниця. Але якщо в кільці є і ліва і права одиниці, то вони збігаються і дають двосторонню одиницю 1. Нарешті, з рівностей $Ka = K$ і $aK = K$ випливає існування таких елементів x і y, що $xa = 1$ і $ay = 1$, тобто лівого й правого обернених до a. Але тоді $x = y$ і є двостороннім оберненим до a.

Таким чином, K містить одиницю і для кожного ненульового елемента є обернений. Тому K є тілом. □

Задача 5. *Опишіть усі ідеали в кільці* $\mathrm{Map}(M, P)$ *функцій* $f : M \to P$, *де M — n-елементна множина, а P — поле, і підрахуйте їх кількість.*

Розв'язання. Нехай I — ідеал кільця $\mathrm{Map}(M,P)$. Якщо I містить функцію f, яка в точці $a \in M$ не дорівнює 0, то він містить і функцію f_a, яка в точці a дорівнює 1, а в усіх інших точках дорівнює 0. Справді, такою буде функція $f \cdot g$, де $g(a) = \big(f(a)\big)^{-1}$ і $g(x) = 0$ для всіх $x \neq a$.

Розгляньмо множину

$$A_I = \{a \in M \mid f(a) = 0 \text{ для всіх функцій } f \in I\}.$$

Неважко зрозуміти, що ідеал I складається з усіх тих і лише тих функцій, які в усіх точках множини A_I набувають значення 0. Те, що I містить лише такі функції, випливає безпосередньо з означення множини A_I. Покажемо, що I містить всі такі функції. Справді, нехай f — довільна функція, яка набуває ненульових значень лише в точках a_1, a_2, …, a_k, причому $\{a_1, a_2, \ldots, a_k\} \cap A_I = \varnothing$. Із означення множини A_I випливає, що для кожного i $(1 \leq i \leq k)$ ідеал I містить функцію f_i, яка в точці a_i не дорівнює 0, а тому містить і функцію f_{a_i}. Але тоді I містить і функцію $g = f_{a_1} + f_{a_2} + \cdots + f_{a_k}$, а разом із нею — і функцію $f \cdot g$. Позаяк функція g в усіх точках a_1, a_2, …, a_k дорівнює 1, то $f \cdot g = f$.

Таким чином, кожен ідеал кільця $\mathrm{Map}(M,P)$ має вигляд

$$\{f \in \mathrm{Map}(M,P) \mid f(x) = 0 \text{ для всіх } x \in A\},$$

де A — деяка фіксована підмножина множини M. Навпаки, множина всіх тих і лише тих функцій, які в усіх точках фіксованої підмножини $A \subseteq M$ набувають значення 0, є замкненою відносно додавання, віднімання і множення на довільну функцію, а тому утворює ідеал. Це дає нам взаємно однозначну відповідність між ідеалами кільця $\mathrm{Map}(M,P)$ і підмножинами множини M. Множина M має 2^n підмножин, тому кільце $\mathrm{Map}(M,P)$ має 2^n ідеалів. □

Задача 6. *Для яких натуральних чисел n і m відображення $k \,(\mathrm{mod}\, n) \mapsto k \,(\mathrm{mod}\, m)$ буде гомоморфізмом кільця $\mathbb{Z}_n$ в кільце $\mathbb{Z}_m$?*

Розв'язання. Спочатку з'ясуємо, коли правило $k(\mathrm{mod} n) \mapsto k(\mathrm{mod} m)$ коректно задає певне відображення φ із $\mathbb{Z}_n$ у $\mathbb{Z}_m$. Для цього потрібно, щоб елементи, які належать тому самому класові лишків за модулем n, переходили в той самий клас лишків за модулем m. Тобто якщо різниця двох чисел ділиться на n, то вона повинна ділитися і на m. А це рівносильне умові, що n ділиться на m.

Покажемо тепер, що коли відображення $k \,(\mathrm{mod}\, n) \mapsto k \,(\mathrm{mod}\, m)$ задане коректно, то воно є гомоморфізмом кілець. Нехай $\overline{p}$ і $\overline{q}$ — два довільні класи лишків із $\mathbb{Z}_n$, а p і q — їх представники. Тоді $p+q$ і pq будуть

представниками відповідно класів $\overline{p}+\overline{q}=\overline{p+q}$ і $\overline{p}\cdot\overline{q}=\overline{pq}$. Зокрема, кожне з чисел

$$p \pmod n + q \pmod n - (p+q) \pmod n$$

і

$$p \pmod n \cdot q \pmod n - (p\cdot q) \pmod n$$

ділиться на n. А позаяк n ділиться на m, то кожне з чисел

$$p \pmod m + q \pmod m - (p+q) \pmod m$$

і

$$p \pmod m \cdot q \pmod m - (p\cdot q) \pmod m$$

ділиться на m. Але

$$\varphi(\overline{p}) = \overline{p \pmod m}, \quad \varphi(\overline{q}) = \overline{q \pmod m},$$
$$\varphi(\overline{p}+\overline{q}) = \overline{(p+q) \pmod m}, \quad \varphi(\overline{p}\cdot\overline{q}) = \overline{(p\cdot q) \pmod m}.$$

Враховуючи попереднє зауваження, звідси випливає, що

$$\varphi(\overline{p}+\overline{q}) - (\varphi(\overline{p}) + \varphi(\overline{q})) = 0 \quad \text{і} \quad \varphi(\overline{p}\cdot\overline{q}) - (\varphi(\overline{p})\cdot\varphi(\overline{q})) = 0,$$

тобто

$$\varphi(\overline{p}+\overline{q}) = \varphi(\overline{p}) + \varphi(\overline{q}) \quad \text{і} \quad \varphi(\overline{p}\cdot\overline{q}) = \varphi(\overline{p})\cdot\varphi(\overline{q}).$$

Отже, φ є гомоморфізмом кілець.

Таким чином, відображення $k \pmod n \mapsto k \pmod m$ задає гомоморфізм кільця $\mathbb{Z}_n$ в кільце $\mathbb{Z}_m$ тоді й лише тоді, коли n ділиться на m. □

Задача 7. *Знайдіть усі гомоморфізми а) групи $(\mathbb{Z};+)$ в групу $(\mathbb{Q};+)$; б) кільця $\mathbb{Z}$ в кільце $\mathbb{Q}$.*

Розв'язання. а) Група $(\mathbb{Z};+)$ — циклічна, тому довільний гомоморфізм $\varphi : (\mathbb{Z};+) \to (\mathbb{Q};+)$ повністю визначається образом $\varphi(1)$ її твірного елемента. Зокрема, якщо $\varphi(1) = a$, то для довільного натурального n має бути

$$\varphi(n) = \varphi(1+1+\cdots+1) = \varphi(1)+\varphi(1)+\cdots+\varphi(1) = a+a+\cdots+a = a\cdot n.$$

Позаяк $\varphi(-n) = -\varphi(n)$, то рівність $\varphi(n) = an$ буде виконуватися для всіх $n \in \mathbb{Z}$.

Із другого боку, для довільного числа $a \in \mathbb{Q}$ відображення $\varphi_a : \mathbb{Z} \to \mathbb{Q}$, $n \mapsto n \cdot a$, є гомоморфізмом відповідних адитивних груп, бо

$$\varphi_a(n+m) = a(n+m) = an + am = \varphi_a(n) + \varphi_a(m).$$

Тому гомоморфізмами із $(\mathbb{Z}; +)$ в $(\mathbb{Q}; +)$ будуть відображення $\varphi_a : n \mapsto an$ і тільки вони.

b) Оскільки гомоморфізм кілець одночасно є гомоморфізмом їх адитивних груп, то потрібно лише з'ясувати, які з відображень φ_a із попереднього пункту зберігають множення. Зокрема, із $1 \cdot 1 = 1$ випливає, що має виконуватися рівність $\varphi(1) \cdot \varphi(1) = \varphi(1)$, тобто $a \cdot a = a$. Останню рівність задовольняють лише два числа з $\mathbb{Q}$: 0 і 1. Очевидно, що кожне з цих чисел справді визначає гомоморфізм із $\mathbb{Z}$ в $\mathbb{Q}$: $\varphi_0 : n \mapsto 0$ (нульовий гомоморфізм) і $\varphi_1 : n \mapsto n$ (занурення). □

Задача 8. *Нехай $\varphi : P \to K$ — епіморфізм комутативних кілець і $a \in P$. Чи будуть правильними наступні імплікації:*
a) якщо a є дільником нуля у кільці P, то $\varphi(a)$ є дільником нуля у кільці K;
b) якщо $\varphi(a)$ є дільником нуля у кільці K, то a є дільником нуля у кільці P?

Розв'язання. a) Елемент a є дільником нуля, якщо для деякого ненульового b виконується рівність $ab = 0$. При епіморфізмі φ вона переходить у рівність $\varphi(a)\varphi(b) = \varphi(0) = 0$. Але може трапитися так, що $\varphi(b) = 0$ для всіх таких b, що $ab = 0$.

Ці міркування підказують, як побудувати такий епіморфізм φ, який не зберігає властивість "бути дільником нуля". Наприклад, у кільці $\mathbb{Z}_6$ клас лишків $\overline{3}$ є дільником нуля, бо $\overline{3} \cdot \overline{2} = \overline{3} \cdot \overline{4} = \overline{0}$. Але при епіморфізмі $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2$, $n \bmod 6 \mapsto n \bmod 2$, кожен з елементів $\overline{2}$ і $\overline{4}$ переходить у нуль кільця $\mathbb{Z}_2$, а переходить в одиницю кільця $\mathbb{Z}_2$. Отже, $\varphi(\overline{3})$ не є дільником нуля і імплікація не є правильною.

b) Образ $\varphi(a)$ ненульового елемента a з P може стати дільником нуля у кільці K за рахунок того, що знайдеться такий елемент $b \in P$, що $ab \neq 0$, $\varphi(a) \neq 0$, $\varphi(b) \neq 0$, але $\varphi(ab) = 0$. Наприклад, кільце $\mathbb{Z}$ взагалі є кільцем без дільників нуля. Але образи $\overline{2}$ і $\overline{3}$ чисел 2 і 3 при канонічному епіморфізмі $\mathbb{Z} \to \mathbb{Z}_6$ є дільниками нуля, бо $\overline{2} \cdot \overline{3} = \overline{0}$. Тому імплікація не є правильною. □

Задача 9. *Нехай K — область цілісності і a — фіксований елемент із K. Доведіть, що відображення $\varphi_a : K[x] \to K$, $f(x) \mapsto f(a)$, є гомоморфізмом, знайдіть ядро* $\operatorname{Ker}\varphi_a$ *і опишіть класи суміжності за ядром.*

Розв'язання. Те, що відображення φ_a є гомоморфізмом, випливає із правил додавання і множення функцій:

$$\varphi_a(f+g) = (f+g)(a) = f(a) + g(a) = \varphi_a(f) + \varphi_a(g);$$
$$\varphi_a(f \cdot g) = (f \cdot g)(a) = f(a) \cdot g(a) = \varphi_a(f) \cdot \varphi_a(g).$$

У кільці $K[x]$ кожен многочлен $f(x)$ можна розділити на $x-a$ з остачею:

$$f(x) = (x-a)q(x) + r, \tag{1}$$

причому частка $q(x)$ і остача $r \in K$ визначені однозначно. Звідси отримуємо: $\varphi_a(f) = f(a) = r$. Тому $f(x) \in \operatorname{Ker}\varphi_a$ тоді й лише тоді, коли $r = 0$, тобто коли $f(x)$ ділиться на $x-a$. Отже, ядро $\operatorname{Ker}\varphi_a$ складається з усіх многочленів, кратних $x-a$, тобто збігається з головним ідеалом $(x-a)K[x]$.

Нарешті, із рівності (1) випливає, що многочлен $f(x)$ належить тому ж класу суміжності за ядром $\operatorname{Ker}\varphi_a$, що і його остача від ділення на $x-a$. Тому кожен клас суміжності має вигляд $r + (x-a)K[x]$, де $r \in K$. □

Задача 10. *Доведіть, що відображення $\varphi : \mathbb{Q}[x] \to \mathbb{C}$, при якому многочлену $f \in \mathbb{Q}[x]$ ставиться у відповідність його значення $f(1+i)$ в точці $1+i$, є гомоморфізмом. Знайдіть ядро і образ цього гомоморфізму.*

Розв'язання. Відображення φ є обмеженням на підкільце $\mathbb{Q}[x]$ гомоморфізму $\varphi_{1+i} : \mathbb{C}[x] \to \mathbb{C}$ із задачі 9. Тому φ також є гомоморфізмом.

Ядро відображення φ складається з тих многочленів $f \in \mathbb{Q}[x]$, для яких число $1+i$ буде коренем. Але якщо комплексне число z_0 є коренем многочлена з дійсними (зокрема, раціональними) коефіцієнтами, то спряжене число $\overline{z_0}$ також буде його коренем. Отже, $f \in \operatorname{Ker}$ тоді й лише тоді, коли числа $1+i$ і $1-i$ є його коренями. Останнє рівносильне тому, що $f(x)$ ділиться на $(x-(1+i))(x-(1-i)) = x^2 - 2x + 2$. Таким чином, $\operatorname{Ker}\varphi = = (x^2-2x+2)\mathbb{Q}[x]$.

Якщо многочлен $f(x)$ має раціональні коефіцієнти, то його значення в точці $1+i$ є числом вигляду $a+bi$, де $a, b \in \mathbb{Q}$. Тому $\operatorname{Im}\varphi \subseteq \mathbb{Q}(i) = = \{a+bi \mid a, b \in \mathbb{Q}\}$. З іншого боку для довільного числа $a+bi \in \mathbb{Q}(i)$ маємо: $\varphi(bx+a-b) = a+bi$. Тому $\operatorname{Im}\varphi \supseteq \mathbb{Q}(i)$. Отже, $\operatorname{Im}\varphi = \mathbb{Q}(i)$. □

Задача 11. *Нехай P — поле, $f(x) = p_1^{k_1}(x) \cdots p_m^{k_m}(x)$ — розклад многочлена $f(x) \in P[x]$ у добуток незвідних многочленів.*
a) Опишіть усі дільники 0 у факторкільці $P[x]/\big(f(x)\big)$.
b) Доведіть, що кожен ненульовий елемент із $P[x]/\big(f(x)\big)$ є або дільником 0, або дільником 1.
c) Опишіть у факторкільці $P[x]/\big(f(x)\big)$ усі нільпотентні елементи.

Розв'язання. У кільці $P[x]$ кожен многочлен $g(x)$ можна розділити на $f(x)$ з остачею:

$$g(x) = f(x)q(x) + r(x), \tag{2}$$

причому частка $q(x)$ і остача $r(x)$ степеня, меншого за степінь $f(x)$, визначені однозначно. Многочлен $g(x)$ і його остача $r(x)$ від ділення на $f(x)$ належать тому самому класу суміжності за ідеалом $\big(f(x)\big)$, бо різниця $g(x) - r(x) = f(x)q(x)$ ділиться на $f(x)$. Тому далі *представниками класів суміжності за ідеалом $\big(f(x)\big)$ будемо брати многочлени із $P[x]$ степеня, меншого за степінь $f(x)$*. Зауважимо також, що різниця $r_1(x) - r_2(x)$ двох многочленів степеня, меншого за степінь $f(x)$, буде ділитися на $f(x)$ лише тоді, коли $r_1(x) = r_2(x)$. Тому такий представник визначений однозначно.

a) Нехай тепер $\overline{g(x)} \neq 0$, $\overline{h(x)} \neq 0$, але $\overline{g(x)} \cdot \overline{h(x)} = 0$. Позаяк нулем факторкільця $P[x]/\big(f(x)\big)$ є ідеал $\big(f(x)\big)$, то це означає, що добуток $g(x)h(x)$ ділиться на $f(x)$. Якби $g(x)$ і $f(x)$ були взаємно прості, то на $f(x)$ мав би ділитися многочлен $h(x)$. Але це неможливо, бо степінь $h(x)$ менший за степінь $f(x)$. Отже, $g(x)$ і $f(x)$ не є взаємно простими.

Навпаки, нехай $g(x)$ і $f(x)$ не є взаємно простими і $d(x)$ — їх найбільший спільний дільник. Тоді можемо записати: $g(x) = g_1(x)d(x)$, $f(x) = f_1(x)d(x)$. Оскільки степінь $f_1(x)$ менший за степінь $f(x)$, то $\overline{f_1(x)} \neq 0$. З іншого боку,

$$\overline{g(x)} \cdot \overline{f_1(x)} = \overline{g(x)f_1(x)} = \overline{g_1(x)d(x)f_1(x)} = \overline{g_1(x)f(x)} = 0,$$

тобто $\overline{g(x)}$ є дільником нуля.

Таким чином, $\overline{g(x)}$ є дільником нуля тоді й лише тоді, коли $g(x)$ і $f(x)$ не є взаємно простими, тобто коли $g(x)$ ділиться на якийсь із многочленів $p_1(x), \ldots, p_m(x)$. Зокрема, якщо многочлен $f(x)$ незвідний, то кожен многочлен меншого степеня буде з ним взаємно простим і факторкільце $P[x]/\big(f(x)\big)$ буде кільцем без дільників нуля.

b) Вище вже доведено, що коли $g(x)$ і $f(x)$ не є взаємно простими, то у факторкільці $P[x]/\big(f(x)\big)$ елемент $\overline{g(x)}$ є дільником нуля. Нехай тепер

$g(x)$ і $f(x)$ взаємно прості. Тоді існують такі многочлени $u(x)$ і $v(x)$, що $f(x)u(x) + g(x)v(x) = 1$. Переходячи до факторкільця $P[x]/\big(f(x)\big)$ і враховуючи, що $\overline{f(x)} = 0$, отримуємо:

$$1 = \overline{f(x)u(x) + g(x)v(x)} = \overline{f(x)} \cdot \overline{u(x)} + \overline{g(x)} \cdot \overline{v(x)} = \overline{g(x)} \cdot \overline{v(x)}.$$

Отже, в цьому випадку $\overline{g(x)}$ є дільником одиниці.

c) Нехай $g(x) = q_1^{k_1}(x) \cdots q_r^{k_r}(x)$ — розклад многочлена $g(x)$ у добуток незвідних многочленів. Елемент $\overline{g(x)}$ буде нільпотентним, якщо для для деякого натурального числа n матимемо $\overline{g(x)}^n = 0$, тобто якщо $g^n(x)$ ділиться на $f(x)$. Але $g^n(x) = q_1^{nk_1}(x) \cdots q_r^{nk_r}(x)$. Із однозначності розкладу на незвідні множники в кільці $P[x]$ випливає, що в розкладі многочлена $g^n(x)$ повинні зустрічатися усі незвідні дільники $p_1(x)$, …, $p_m(x)$ многочлена $f(x)$. Тому вони повинні зустрічатися і в розкладі многочлена $g(x)$. Отже, многочлен $g(x)$ повинен ділитися на добуток $p_1(x) \cdots p_m(x)$.

Із другого боку, якщо $g(x) = p_1(x) \cdots p_m(x)h(x)$, то $\overline{g^n(x)}$ буде ділитися на $f(x)$, якщо $n \geq \max(k_1, \ldots, k_m)$. Таким чином, $\overline{g(x)}$ буде нільпотентним елементом тоді й лише тоді, коли $g(x)$ ділиться на $p_1(x) \cdots p_m(x)$. □

Задача 12. *Для кожного многочлена $f(x) = x^2 + ax + b \in \mathbb{Z}_2[x]$ побудуйте табличку множення для факторкільця $\mathbb{Z}_2[x]/(f(x))$. Які з цих факторкілець будуть ізоморфними. Які з них будуть полями?*

Розв'язання. На початку розв'язання задачі 11 ми вже з'ясували, що представниками класів суміжності за модулем ідеалу $(f(x))$ можна брати многочлени степеня < 2. У кільці $\mathbb{Z}_2[x]$ таких многочленів лише 4: 0, 1, x і $x + 1$. Тому факторкільце $\mathbb{Z}_2[x]/(f(x))$ має 4 елементи (будемо позначати їх жирним шрифтом): $\mathbf{0} = 0 + (f(x))$, $\mathbf{1} = 1 + (f(x))$, $\mathbf{x} = x + (f(x))$, $\mathbf{x}+\mathbf{1} = (x+1) + (f(x))$. При цьому $\mathbf{0}$ і $\mathbf{1}$ будуть відповідно нулем і одиницею факторкільця $\mathbb{Z}_2[x]/(f(x))$.

Многочленів вигляду $x^2 + ax + b$ у кільці $\mathbb{Z}_2[x]$ також 4: $f_1(x) = x^2$, $f_2(x) = x^2 + 1$, $f_3(x) = x^2 + x$ і $f_2(x) = x^2 + x + 1$. Побудуємо табличку множення для факторкільця $\mathbb{Z}_2[x]/(f_3(x))$. Позаяк елементи $\mathbf{0}$ і $\mathbf{1}$ є відповідно нулем і одиницею, то частина таблички заповнюється одразу:

$f_3(x)$	**0**	**1**	**x**	**x+1**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**x**	**x+1**
x	**0**	**x**		
x+1	**0**	**x+1**		

.

Знайдемо вміст решти клітинок таблиці:

$x \cdot x = x^2 = x + (x^2 + x)$. Тому $\mathbf{x} \cdot \mathbf{x} = \mathbf{x}$.

$x \cdot (x + 1) = x^2 + x = 0 + (x^2 + x)$. Тому $\mathbf{x} \cdot (\mathbf{x+1}) = \mathbf{0}$.

$(x + 1) \cdot x = x^2 + x = 0 + (x^2 + x)$. Тому $(\mathbf{x+1}) \cdot \mathbf{x} = \mathbf{0}$.

$(x + 1) \cdot (x + 1) = x^2 + 2x + 1 = (x + 1) + (x^2 + x)$.

Тому $(\mathbf{x+1}) \cdot (\mathbf{x+1}) = \mathbf{x+1}$.

Таким чином, остаточно табличка множення набуває вигляду

$f_3(x)$	**0**	**1**	**x**	**x+1**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**x**	**x+1**
x	**0**	**x**	**x**	**0**
x+1	**0**	**x+1**	**0**	**x+1**

.

Для інших многочленів таблички множення для факторкілець $\mathbb{Z}_2[x]/(f(x))$ будуються аналогічно:

$f_1(x)$	**0**	**1**	**x**	**x+1**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**x**	**x+1**
x	**0**	**x**	**0**	**x**
x+1	**0**	**x+1**	**x**	**1**

,

$f_2(x)$	**0**	**1**	**x**	**x+1**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**x**	**x+1**
x	**0**	**x**	**1**	**x+1**
x+1	**0**	**x+1**	**x+1**	**0**

,

$f_4(x)$	**0**	**1**	**x**	**x+1**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**x**	**x+1**
x	**0**	**x**	**x+1**	**1**
x+1	**0**	**x+1**	**1**	**x**

.

Із табличок множення безпосередньо видно, що факторкільця $\mathbb{Z}_2[x]/(x^2)$, $\mathbb{Z}_2[x]/(x^2 + 1)$ і $\mathbb{Z}_2[x]/(x^2 + x)$ полями не будуть, бо містять дільники 0. У той же час із таблички множення для $\mathbb{Z}_2[x]/(x^2 + x + 1)$ видно, що кожен ненульовий елемент має обернений. Тому це факторкільце буде полем. Із кількості нулів у табличці множення видно також, що кожне з факторкілець $\mathbb{Z}_2[x]/(x^2 + x + 1)$ і $\mathbb{Z}_2[x]/(x^2 + x)$ не

ізоморфне жодному іншому. Нарешті, заміна $\mathbf{x}$ на $\mathbf{x}+\mathbf{1}$, а $\mathbf{x}+\mathbf{1}$ на $\mathbf{x}$ табличку множення для $\mathbb{Z}_2[x]/(x^2)$ переводить у табличку множення для $\mathbb{Z}_2[x]/(x^2+1)$. Тому ці факторкільця ізоморфні (адитивною групою кожного факторкільця є нециклічна група порядку 4, а в ній будь-яка перестановка ненульових елементів є автоморфізмом). □

Задача 13. *Доведіть, що факторкільце $\mathbb{Z}[x]/(x)$ ізоморфне кільцю $\mathbb{Z}$.*

Розв'язання. Розглянемо гомоморфізм $\varphi_0 : \mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(0)$, із задачі 9. Оскільки

$$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = a_0,$$

то очевидно, що $\operatorname{Im}\varphi_0 = \mathbb{Z}$. За основною теоремою про гомоморфізм $\operatorname{Im}\varphi_0 \simeq \mathbb{Z}[x]/\operatorname{Ker}\varphi_0$. Крім того, в розв'язанні задачі 9 показано, що $\operatorname{Ker}\varphi_0$ є ідеалом, породженим многочленом $x - 0$, тобто ідеалом (x). Отже,

$$\mathbb{Z} = \operatorname{Im}\varphi_0 \simeq \mathbb{Z}[x]/\operatorname{Ker}\varphi_0 = \mathbb{Z}[x]/(x).$$

□

Задача 14. *Доведіть, що факторкільця*
а) $\mathbb{Z}[x]/(x^2-2)$ і $\mathbb{Z}[x]/(x^2-3)$; б) $\mathbb{Q}[x]/(x^2-2)$ і $\mathbb{Q}[x]/(x^2-3)$ є неізоморфними.

Розв'язання. Щоб довести неізоморфність двох кілець, потрібно вказати властивість (яка залежить лише від операцій у кільці), яка в одному з кілець виконується, а в іншому — ні. Зауважимо також, що елементи кожного із даних факторкілець мають вигляд $\overline{ax+b} = (ax+b) + I$, де a і b належать кільцю $\mathbb{Z}$ (у випадку а) або полю $\mathbb{Q}$ (у випадку б), а I — відповідний ідеал.

а) У факторкільці $\mathbb{Z}[x]/(x^2-3)$ рівняння $y^2 - 3 = 0$ має очевидний розв'язок $\overline{x}$:

$$\overline{x}^2 - 3 = \overline{x^2 - 3} = 0.$$

З'ясуємо, чи має це рівняння розв'язок у факторкільці $\mathbb{Z}[x]/(x^2-2)$:

$$(\overline{ax+b})^2 - 3 = \overline{a^2x^2 - 2abx + b^2} - 3 = \overline{a^2x^2 - 2abx + b^2 - 3} =$$
$$= \overline{a^2(x^2-2) - 2abx + 2a^2 + b^2 - 3} = \overline{-2abx + 2a^2 + b^2 - 3}.$$

Таким чином, елемент $\overline{ax+b}$ факторкільця $\mathbb{Z}[x]/(x^2-2)$ буде розв'язком рівняння $y^2-3=0$ тоді й лише тоді, коли многочлен $-2abx+2a^2+b^2-3$ є нульовим. Це дає для цілих чисел a і b систему рівнянь

$$-2ab = 0, \qquad 2a^2 + b^2 - 3 = 0,$$

яка у свою чергу розпадається на такі дві системи:

$$a = 0, \quad b^2 = 3, \qquad \text{або} \qquad b = 0, \quad 2a^2 = 3. \tag{3}$$

Жодна з цих систем не має розв'язків у цілих числах, а тому рівняння $y^2 - 3 = 0$ у факторкільці $\mathbb{Z}[x]/(x^2-2)$ розв'язків не має. Отже, факторкільця $\mathbb{Z}[x]/(x^2-2)$ і $\mathbb{Z}[x]/(x^2-3)$ — не ізоморфні.

b) Міркування повністю аналогічні попереднім, тільки розв'язки систем (3) тепер треба шукати в полі $\mathbb{Q}$. Однак раціональних розв'язків ці системи також не мають, тому факторкільця $\mathbb{Q}[x]/(x^2-2)$ і $\mathbb{Q}[x]/(x^2-3)$ також не ізоморфні. □

Задача 15. *Доведіть, що коли a і b — різні елементи поля P, то факторкільце $P[x]/\big((x-a)(x-b)\big)$ ізоморфне кільцю $P \oplus P$.*

Розв'язання. Спробуємо використати основну теорему про гомоморфізм кілець. Для цього розглянемо відображення

$$\varphi : P[x] \to P \oplus P, \qquad f(x) \mapsto (f(a), f(b)).$$

Це відображення є гомоморфізмом. Справді.

$$\begin{aligned}
\varphi(f \pm g) &= \big((f \pm g)(a), (f \pm g)(b)\big) = \big(f(a) \pm g(a), f(b) \pm g(b)\big) = \\
&= \big(f(a), f(b)\big) \pm \big(g(a), (g(b)\big) = \varphi(f) \pm \varphi(g), \\
\varphi(f \cdot g) &= \big((f \cdot g)(a), (f \cdot g)(b)\big) = \big(f(a) \cdot g(a), f(b) \cdot g(b)\big) = \\
&= \big(f(a), f(b)\big) \cdot \big(g(a), (g(b)\big) = \varphi(f) \cdot \varphi(g).
\end{aligned}$$

Крім того, з теореми про інтерполяцію випливає, що коли $a \neq b$, то образ $(f(a), f(b))$ може бути довільним елементом кільця $P \oplus P$. Тому гомоморфізм φ є сюр'єктивним.

Многочлен $f(x)$ належить ядру гомоморфізма φ тоді й лише тоді, коли $f(a) = f(b) = 0$. За теоремою Безу це буде тоді й лише тоді, коли $f(x)$ ділиться і на $x-a$, і на $x-b$. Останнє рівносильне тому, що $f(x)$ ділиться на $(x-a)(x-b)$, тобто що $f(x)$ належить ідеалу $\big((x-a)(x-b)\big)$. Отже, $\operatorname{Ker}\varphi = \big((x-a)(x-b)\big)$. Тому за основною теоремою про гомоморфізм

$$P \oplus P = \operatorname{Im}\varphi \simeq P[x]/\big((x-a)(x-b)\big).$$ □

Задача 16. *Доведіть, що з точністю до ізоморфізму існує рівно* 4 *кільця порядку* 4 *з одиницею.*

Розв'язання. Позначимо одиницю кільця символом e. Розглянемо спочатку випадок, коли адитивна група $(K;+)$ кільця K є циклічною. Якщо в цій групі одиниця e має порядок k, то для кожного $a \in K$ буде

$$\underbrace{a+\cdots+a}_{k} = a\cdot(\underbrace{e+\cdots+e}_{k}) = a\cdot 0 = 0,$$

тобто порядок кожного елемента буде $\le k$. Тому з циклічності групи $(K;+)$ випливає, що $k = 4$ і e є твірним елементом групи $(K;+)$. Тому кожен елемент $a \in K$ є кратним елемента e: $a = me$. Позаяк

$$me + ne = (m+n)e;$$
$$me\cdot ne = (\underbrace{e+\cdots+e}_{m})\cdot(\underbrace{e+\cdots+e}_{n}) = \underbrace{e+\cdots+e}_{mn} = mne,$$

то відображення $\mathbb{Z}_4 \to K$, $m \mapsto me$, буде ізоморфізмом кілець. Отже, в цьому випадку кільце K ізоморфне кільцю $\mathbb{Z}_4$.

Якщо ж адитивна група кільця K не є циклічною, то кожен ненульовий елемент групи $(K,+)$ має порядок 2 і можна вважати, що $(K,+) = \{0,1,a,a+1\}$. Зауважимо, що коли позначити $b = a+1$, то отримаємо $b+1 = a$, тобто перестановка елементів a і $a+1$ є автоморфізмом групи $(K,+)$.

Враховуючи дистрибутивний закон, для кожної з можливостей $a^2 = 0,1,a,a+1$ таблиця Келі мультиплікативної напівгрупи $(K,\cdot)$ заповнюється однозначно (зручно обмежитись лише множенням ненульових елементів):

$a^2=0$	1	a	$a+1$
1	1	a	$a+1$
a	a	0	a
$a+1$	$a+1$	a	1

,

$a^2=1$	1	a	$a+1$
1	1	a	$a+1$
a	a	1	$a+1$
$a+1$	$a+1$	$a+1$	0

,

$a^2=a$	1	a	$a+1$
1	1	a	$a+1$
a	a	a	0
$a+1$	$a+1$	0	$a+1$

,

$a^2=a+1$	1	a	$a+1$
1	1	a	$a+1$
a	a	$a+1$	1
$a+1$	$a+1$	1	a

.

Взагалі кажучи, потрібно ще перевірити, чи є визначене цими таблицями множення асоціативним і чи пов'язане воно з додаванням дистрибутивним законом. Однак є простіший шлях. Порівнюючи ці таблиці

із таблицями множення із задачі 68 для факторкілець $\mathbb{Z}_2[x]/(f)$, де f — многочлен степеня 2 із $\mathbb{Z}_2[x]$, бачимо, що перша, третя і четверта таблиці збігаються з таблицями множення у факторкільцях $\mathbb{Z}_2[x]/(x^2)$, $\mathbb{Z}_2[x]/(x^2+x)$ і $\mathbb{Z}_2[x]/(x^2+x+1)$ відповідно (із природною заміною a на $\mathbf{x}$). Отже, ці таблиці відповідають кільцям, причому неізоморфним. Нарешті, друга таблиця переходить у першу, якщо замінити a на $a+1$ і $a+1$ на a. Тому кільця, що відповідають цим таблицям, будуть ізоморфні.

Таким чином, із точністю до ізоморфізму маємо одне кільце із циклічною адитивною групою і три — із нециклічною. □

Основні задачі

17. З'ясуйте, чи утворює ідеал у кільці $\mathbb{Z}[x]$ множина тих многочленів $f(x) = a_0 + a_1x + \cdots + a_nx^n$ із $\mathbb{Z}[x]$, які задовольняють таку умову:
a) сума коефіцієнтів яких ділиться на 5;
b) $a_2 = 0$;
c) $f(0) + f(1) = 0$.

17. a — так; b,c — ні.

18. З'ясуйте, чи утворює ідеал у кільці K всіх неперервних дійсних функцій така множина дійсних функцій:
a) функції, які дорівнюють 0 на $[0,1]$;
b) функції, для яких $f(0) = f(1)$;
c) функції, для яких число $f(1/2)$ є раціональним?

19. З'ясуйте, чи утворюють ідеал усі необоротні елементи кільця:
a) $\mathbb{Z}_{16}$; b) $\mathbb{Z}_{36}$.

20. З'ясуйте, чи буде множина I ідеалом кільця $\mathbb{Z} \oplus \mathbb{Z}$. Якщо так, то опишіть факторкільце і з'ясуйте, чи буде воно областю цілісності (полем):
a) $I = \{(0,n) \mid n \in \mathbb{Z}\}$; b) $I = \{(n,n) \mid n \in \mathbb{Z}\}$;
c) $I = \{(2n,5n) \mid n \in \mathbb{Z}\}$; d) $I = \{(2n,5m) \mid n,m \in \mathbb{Z}\}$.

21. Доведіть, що підмножина $K = \{(m,n) \mid m+n \equiv 0 \pmod 2\}$ кільця $\mathbb{Z} \oplus \mathbb{Z}$ є підкільцем, але не є ідеалом.

22. Нехай K — кільце з одиницею. Доведіть, що коли ідеал $I \subseteq K$ містить оборотний елемент, то цей ідеал збігається з усім кільцем.

23. Доведіть, що кожен (лівий, правий) мінімальний ідеал є головним.

24. a) Доведіть, що в кільці K з одиницею об'єднання $\bigcup\limits_{n=1}^{\infty} I_n$ зростаючого ланцюга $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ власних ідеалів також буде власним ідеалом.
b)* Покажіть, що для кілець без одиниці попереднє твердження, взагалі кажучи, є хибним.

25. Опишіть усі ідеали кільця K і підрахуйте їх кількість, якщо:
a) $K = \mathbb{Z}$; b) $K = \mathbb{Z}_n$; c) $K = M_2(\mathbb{R})$.

26. З'ясуйте, чи буде гомоморфізмом кілець таке відображення із $M_2(\mathbb{Z})$ в $\mathbb{Z}$:
a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$; b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$; c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$.

27. Знайдіть усі гомоморфізми поля $\mathbb{R}$ в себе.

28. Доведіть, що при гомоморфізмі ідемпотент переходить в ідемпотент, а нільпотентний елемент — у нільпотентний.

29. Нехай P — поле. Доведіть, що кожний гомоморфізм $P \to K$ є або мономорфізмом, або нульовим гомоморфізмом.

30. Нехай $\varphi : P \to K$ — гомоморфізм кілець. Які з наступних тверджень є правильними:
a) образ $\varphi(I)$ ідеалу I кільця P буде ідеалом кільця K;
b) прообраз $\varphi^{-1}(J)$ ідеалу J кільця K буде ідеалом кільця P?

31. Знайдіть усі гомоморфізми з кільця $\mathbb{Z} \times \mathbb{Z}$ в кільце $\mathbb{Z}$. Для кожного з них знайдіть ядро і образ.

32. Опишіть елементи ідеалу $I = (x, 2)$ кільця $\mathbb{Z}[x]$ та факторкільце $\mathbb{Z}[x]/I$ за цим ідеалом.

33. Доведіть, що для довільних елементів a, b поля P факторкільця $P_a = P[x]/\big((x-a)^2\big)$ і $P_b = P[x]/\big((x-b)^2\big)$ ізоморфні.

34. Доведіть, що коли $a \neq b$ і $c \neq d$ — елементи поля P, то факторкільця $P[x]/\big((x-a)(x-b)\big)$ і $P[x]/\big((x-c)(x-d)\big)$ є ізоморфними.

35. Нехай P — поле, а многочлени f і g із $P[x]$ — взаємно прості. Доведіть, що $P[x]/(fg) \simeq P[x]/(f) \oplus P[x]/(g)$.

36. Нехай f — многочлен степеня 2 із комплексними коефіцієнтами.
a) Доведіть, що коли f має кратний корінь, то факторкільце $\mathbb{C}[x]/(f)$ ізоморфне факторкільцю $\mathbb{C}[x]/(x^2)$, а якщо f має 2 різні корені, то $\mathbb{C}[x]/(f) \simeq \mathbb{C} \oplus \mathbb{C}$.
b) Доведіть, що кільця $\mathbb{C}[x]/(x^2)$ і $\mathbb{C} \oplus \mathbb{C}$ неізоморфні.

37. Нехай f — дійсний многочлен степеня 2 із дискрімінантом D.
a) Доведіть, що коли $D < 0$, то $\mathbb{R}[x]/(f) \simeq \mathbb{C}$, коли $D = 0$, то $\mathbb{R}[x]/(f) \simeq \mathbb{R}[x]/(x^2)$, і коли $D > 0$, то $\mathbb{R}[x]/(f) \simeq \mathbb{R} \oplus \mathbb{R}$.
b) Доведіть, що кільця $\mathbb{C}$, $\mathbb{R}[x]/(x^2)$ і $\mathbb{R} \oplus \mathbb{R}$ попарно неізоморфні.

38. Нехай $x^2 + ax + b$ — дійсний квадратний тричлен із від'ємним дискримінантом. Доведіть, що факторкільце $\mathbb{R}[x]/(x^2 + ax + b)$ ізоморфне полю $\mathbb{C}$.

39. Знайдіть порядок факторкільця $P[x]/(f)$, якщо поле P має порядок q, а многочлен f має степінь n.

40. З'ясуйте, які з даних факторкілець ізоморфні:
a) $\mathbb{R}[x]/(x^2 + x + 1)$, b) $\mathbb{R}[x]/(x^2 + x - 1)$, c) $\mathbb{R}[x]/(x^2 - x + 1)$,
d) $\mathbb{R}[x]/(2x^2 - 3x + 1)$, e) $\mathbb{R}[x]/(x^2 + 4x + 4)$.

41. Побудуйте ізоморфізм факторкільця $\mathbb{R}[x, y]/(y)$ на факторкільце $\mathbb{R}[x, y]/(x)$.

42. Доведіть, що факторкільця $\mathbb{R}[x, y]/(x^2 - y)$ і $\mathbb{R}[x, y]/(x^2 - y^2)$ не ізоморфні.

Додаткові задачі

43. Нехай K — кільце всіх дійсних функцій $f : \mathbb{R} \to \mathbb{R}$.
a) Доведіть, що для кожної підмножини $A \subseteq \mathbb{R}$ множина

$$I_A = \{f \in K \mid f(x) = 0 \text{ для всіх } x \in A\}$$

є ідеалом кільця K.
b)* Чи правильно, що кожен ідеал кільця K має вигляд I_A для деякої підмножини $A \subseteq \mathbb{R}$?

44.* Нехай V — підпростір арифметичного простору $\mathbb{R}^n$. Доведіть, що
a) множина $I_V^l = \{A \in M_n(\mathbb{R}) \mid A\boldsymbol{x} = 0 \text{ для кожного } \boldsymbol{x} \in V\}$ буде лівим ідеалом кільця $M_n(\mathbb{R})$ і всі ліві ідеали з $M_n(\mathbb{R})$ мають такий вигляд;

b) множина $I_V^r = \{A \in M_n(\mathbb{R}) \mid \boldsymbol{x}^\top A = 0 \text{ для кожного } \boldsymbol{x} \in V\}$ буде правим ідеалом кільця $M_n(\mathbb{R})$ і всі праві ідеали з $M_n(\mathbb{R})$ мають такий вигляд.

45. Опишіть всі ідеали кільця $\mathbb{Z} \oplus \mathbb{Z}$.

46. Доведіть, що кожне кільце K з одиницею і без дільників нуля, в якому кожний спадний ланцюг лівих ідеалів обривається, є тілом.

47. Доведіть, що в комутативному кільці без нільпотентних елементів кожний мінімальний ідеал породжується ідемпотентом.

48. Нехай $P_1, \ldots, P_n$ — поля. Опишіть у кільці $P_1 \oplus \cdots \oplus P_n$ усі ідеали і знайдіть їх кількість.

49. a) Побудуйте епіморфізм $\mathbb{Z}[i] \to \mathbb{Z}_2$. b) Доведіть, що не існує епіморфізму $\mathbb{Z}[i] \to \mathbb{Z}$.

50. З'ясуйте, чи існує епіморфізм $\mathbb{Q} \to \mathbb{Z}$.

51. Доведіть, що для довільного кільця K з одиницею існує не більше одного гомоморфізму $\varphi : \mathbb{Q} \to K$, який одиницю переводить в одиницю.

52. Нехай $\varphi : P[x] \to P$ — такий гомоморфізм, що $\varphi(a) = a$ для всіх $a \in P$. Доведіть, що існує такий елемент $c \in P$, що $\varphi(f) = f(c)$ для всіх $f \in P[x]$.

53. Нехай K і R — кільця з одиницями 1_K і 1_R відповідно, а $\varphi : K \to R$ — гомоморфізм. Доведіть, що $\varphi(1_K)(1_R - \varphi(1_K)) = 0$.

54.* Доведіть, що факторкільця $\mathbb{R}[x, y]/(y)$ і $\mathbb{R}[x, y]/(x^2 - y)$ ізоморфні.

55. Доведіть, що кільце $\mathbb{Z}$ і факторкільце $\mathbb{Z}[x]/(2x-1)$ не ізоморфні.

56. Доведіть, що кожне кільце K з одиницею містить підкільце, ізоморфне $\mathbb{Z}$, або підкільце, ізоморфне $\mathbb{Z}_n$ для деякого n.

57. Опишіть із точністю до ізоморфізму всі кільця з одиницею
a) які не мають нетривіальних підкілець;
b) які не мають нетривіальних підкілець з одиницею.

58. Нехай P — поле. Доведіть, що для довільного многочлена $ax + b$ першого степеня із $P[x]$ факторкільце $P[x]/(ax + b)$ ізоморфне полю P.

59. Нехай φ — лінійне перетворення векторного простору V над полем P, а $\Pi_\varphi = \{f(\varphi) \mid f(x) \in P[x]\}$ — кільце всіх многочленів від φ. Доведіть, що $\Pi_\varphi \simeq P[x]/(m_\varphi(x))$, де $m_\varphi(x)$ — мінімальний многочлен перетворення φ.

60. Скільки є попарно неізоморфних кілець порядку 9 з одиницею?

61.* Для довільної матриці $A \in M_n(\mathbb{C})$ через $I_k(A)$ позначимо ідеал кільця $\mathbb{C}[\lambda]$, породжений усіма мінорами порядку k матриці $A - \lambda E$. Нехай $J(A)$ — жорданова нормальна матриці A. Доведіть, що $I_k(A) = I_k(J(A))$.

62.* a) Нехай M_n — множина шляхів довжини $2n$ із точки $(0, n)$ в точку $(n, 0)$, кожна ланка яких є зміщенням на 1 вправо або вниз і які не опускаються нижче прямої $x + y = n$. Доведіть, що існує взаємно однозначна відповідність між ідеалами кільця $T_n(\mathbb{R})$ і шляхами з множини M_{n+1}.

b) Підрахуйте кількість ідеалів у кільці $T_n(\mathbb{R})$.

c) Підрахуйте кількість нільпотентних ідеалів у кільці $T_n(\mathbb{R})$.

63.* Нехай K — кільце з одиницею. Доведіть, що кожен ідеал I кільця $M_n(K)$ має вигляд $M_n(J)$, де J — ідеал кільця K.

64. Нехай $C[a, b]$ — кільце неперервних на проміжку $[a, b]$, $a < b$, дійсних функцій.

a) Доведіть, що для кожної підмножини $A \subseteq [a, b]$ множина $I_A = \{f \in C[a, b] \mid f(x) = 0 \text{ для всіх } x \in A\}$ є ідеалом кільця $C[a, b]$.

b)* Доведіть, що ідеал I_A не є головним.

c)* Чи правильно, що для кожного ідеалу I кільця $C[a, b]$ існує така підмножина $A \subseteq [a, b]$, що $I = I_A$?

d)* Доведіть, що для кожного ідеалу $I \neq C[a, b]$ знайдеться така точка $x \in [a, b]$, що $f(x) = 0$ для всіх $f(x) \in I$.

e)* Доведіть, що ідеал I_A не є скінченнопородженим.

Домашнє завдання

65. З'ясуйте, чи утворює ідеал у кільці $\mathbb{Z}[x]$ множина тих многочленів $f(x) = a_0 + a_1x + \cdots + a_nx^n$ із $\mathbb{Z}[x]$, які задовольняють таку умову:

a) сума коефіцієнтів яких дорівнює 0;

b) a_3 ділиться на 5;

c) $f(x)$ є непарним многочленом.

66. З'ясуйте, чи буде підмножина I кільця $M_2(\mathbb{R})$ лівим, правим або двостороннім ідеалом:

a) $I = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \,\middle|\, a \in \mathbb{R} \right\}$; b) $I = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \,\middle|\, a \in \mathbb{R} \right\}$;

c) $I = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \,\middle|\, a \in \mathbb{R} \right\}$.

67. Нехай $\varphi : P \to K$ — сюр'єктивний гомоморфізм кілець з одиницею і $a \in P$. Які з наступних імплікацій є правильними:
a) якщо a є дільником 1 у кільці P, то $\varphi(a)$ є дільником 1 у кільці K;
b) якщо $\varphi(a)$ є дільником 1 у кільці K, то a є дільником 1 у кільці P?

68. Доведіть, що відображення $\varphi : \mathbb{Q}[x] \to \mathbb{R}$, $f(x) \mapsto f(\sqrt{2})$, є гомоморфізмом, і знайдіть його ядро і образ.

69. З'ясуйте, які з факторкілець: a) $\mathbb{Z}_2[x]/(x^2+1)$;
b) $\mathbb{Z}_7[x]/(x^2+x+2)$; c) $\mathbb{Z}_{11}[x]/(x^2+x)$; d) $\mathbb{Z}_3[x]/(2x^2+x+1)$ є областями цілісності.

70. З'ясуйте, які з факторкілець: a) $\mathbb{R}[x]/(x^2+1)$; b) $\mathbb{R}[x]/(x^2+x)$; c) $\mathbb{R}[x]/(x^2-1)$; d) $\mathbb{R}[x]/(x^2+x+1)$ є ізоморфними.

71. Нехай P — поле, а I — ідеал кільця $P[x,y]$, що складається з усіх многочленів без вільного члена. Доведіть, що $P[x,y]/I \simeq P$.

Заняття 3. Подільність

Необхідні поняття. Ідеал $I \subset K$ називається *максимальним*, якщо $I \neq K$ і для довільного ідеалу $J \subset K$ із включень $I \subseteq J \subseteq K$ випливає, що або $I = J$, або $J = K$.

Ідеал $I \subset K$ називається *простим*, якщо добуток ab двох елементів із K належить ідеалу I лише в тому випадку, коли принаймні один із множників належить I.

Областю цілісності називається неодноелементне комутативне кільце з одиницею і без дільників нуля.

Кажуть, що *елемент a ділить елемент b* (і записують $a \mid b$), якщо знайдеться такий елемент c, що $b = ac$. Синоніми: *a є дільником b*, *b ділиться на a*, *b є кратним a*.

Якщо $a \mid b$ і $b \mid a$, то елементи a і b називаються *асоційованими* (позначається $a \sim b$). Дільник b елемента a називається *власним*, якщо b не є асоційованим ні з a, ні з 1.

Елемент d називається *найбільшим спільним дільником* (коротко: НСД) елементів a і b, якщо d задовольняє дві умови: 1) $d \mid a$ і $d \mid b$; 2) якщо $c \mid a$ і $c \mid b$, то $c \mid d$. НСД елементів a і b позначається НСД(a, b).

Елементі a і b називаються *взаємно простими*, якщо НСД(a, b) існує і дорівнює 1.

Елемент m називається *найменшим спільним кратним* (коротко: НСК) елементів a і b, якщо m задовольняє дві умови: 1) $a \mid m$ і $b \mid m$; 2) якщо $a \mid n$ і $b \mid n$, то $m \mid n$.

Елемент p називається *нерозкладним* (або *незвідним*), якщо сам він не є дільником одиниці, але в кожному розкладі $p = ab$ один із множників є дільником одиниці. Іншими словами, елемент p є нерозкладним, якщо з точністю до асоційованості він має рівно 2 дільники: 1 і p.

Елемент p називається *простим*, якщо він не є дільником одиниці і з того, що $p \mid ab$, випливає, що $p \mid a$ або $p \mid b$.

Область цілісності, в якій кожний ненульовий елемент розкладається в добуток нерозкладних елементів, причому цей розклад є однозначним із точністю до порядку та асоційованості множників, називається *кільцем з однозначністю розкладу* або *факторіальним кільцем*.

Область цілісності K називається *евклідовим кільцем*, якщо існує функція $\sigma : K \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$, що задовольняє такі дві умови:
1) $\sigma(ab) \geq \sigma(a)$ для довільних ненульових елементів a і b;
2) для довільних елемента a і ненульового елемента b існують такі елементи q і r, що $a = qb + r$ і $\sigma(r) < \sigma(b)$ або $r = 0$.

Функція $\sigma(a)$ називається *нормою* елемента a, а q і r — відповідно *часткою* і *остачею* від ділення a на b.

Необхідні твердження. **1.** У кільці головних ідеалів для довільних елементів a і b НСД(a,b) і НСК(a,b) існують, причому для відповідних головних ідеалів виконуються рівності

$$\big(\text{НСД}(a,b)\big) = (a,b) = (a) + (b); \qquad \big(\text{НСК}(a,b)\big) = (a) \cap (b).$$

2. $a \mid b$ тоді й лише тоді, коли $b \in (a)$, або, що те саме, $(b) \subseteq (a)$. Таким чином, відношення подільності для елементів переходить у відношення включення для відповідних головних ідеалів. Зокрема, асоційованість елементів a і b означає, що $(a) = (b)$. Тому відношення асоційованості є відношенням еквівалентності і можна говорити про класи асоційованих елементів.

3. a є власним дільником b тоді й лише тоді, коли $(a) \supset (b)$.

4. Елементи a і b будуть асоційованими тоді й лише тоді, коли вони розрізняються дільником одиниці (точніше: $a \sim b$ тоді й лише тоді, коли існує такий елемент $\varepsilon \in K^*$, що $a = \varepsilon b$).

5. У кільці $\mathbb{Z}$ два цілих числа будуть асоційованими тоді й лише тоді, коли вони розрізняються щонайбільше знаком.

6. У кільці $P[x]$ многочленів з коефіцієнтами з поля P два многочлени будуть асоційованими тоді й лише тоді, коли вони розрізняються скалярним множником.

7. *Основні властивості відношення подільності*: а) $a \mid a$;
b) якщо $a \mid b$, то $a \mid bc$; c) якщо $a \mid b$ і $b \mid c$, то $a \mid c$;
d) на множині класів асоційованих елементів відношення подільності є відношенням часткового порядку;
e) якщо $a \mid b_1, \ldots, a \mid b_k$, то $a \mid (b_1c_1 + \cdots + b_kc_k)$ для довільних елементів $c_1, \ldots, c_k$.

8. Якщо НСД елементів a і b існує, то з точністю до асоційованості він визначений однозначно.

9. НСД$(a,b) = d$ тоді й лише тоді, коли (d) є найменшим серед головних ідеалів, що містять $(a) \cup (b)$.

10. Якщо НСК елементів a і b існує, то з точністю до асоційованості воно визначене однозначно.

11. НСК$(a,b) = m$ тоді й лише тоді, коли (m) є найбільшим серед головних ідеалів, що містяться в $(a) \cap (b)$.

12. Кільце $\mathbb{Z}[i]$ є евклідовим.

13. Із точністю до асоційованості в кільці $\mathbb{Z}[i]$ прості елементи вичерпуються числами таких трьох класів:

1) прості натуральні числа вигляду $p = 4k + 3$;

2) числа вигляду $a = m \pm ni$, де сума $m^2 + n^2$ є простим натуральним непарним числом;

3) число $a = 1 + i$.

14. Критерій факторіальності кільця: область цілісності, в якій кожний ненульовий елемент розкладається в добуток нерозкладних елементів, буде факторіальним кільцем тоді й лише тоді, коли всі нерозкладні елементи p будуть простими.

15. Кожне кільце головних ідеалів є факторіальним.

16. Кожне евклідове кільце є кільцем головних ідеалів.

17. В евклідовому кільці для довільних a і b за допомогою алгоритму Евкліда можна знайти такі u і v, що НСД$(a, b) = ua + vb$.

18. Кільце $\mathbb{Z}[i] = \{m + ni; m, n \in \mathbb{Z}\}$ цілих ґаусових чисел є евклідовим.

Увага! У задачах, пов'язаних із відношенням подільності, кільце завжди є областю цілісності.

Приклади розв'язання типових задач

Задача 1. *Для числа $z = n + m\sqrt{5}$ із кільця $\mathbb{Z}[\sqrt{5}]$ покладемо $N(z) = n^2 - 5m^2$. Доведіть, що в кільці $\mathbb{Z}[\sqrt{5}]$*

a) $N(z \cdot u) = N(z) \cdot N(u)$;

b) z є дільником одиниці в $\mathbb{Z}[\sqrt{5}]$ тоді й лише тоді, коли $N(z) = \pm 1$;

c) елемент $2 + \sqrt{5}$ є дільником одиниці;

d) елементи $3 + \sqrt{5}$ і $1 - \sqrt{5}$ — асоційовані;

e) якщо число $N(z)$ є простим цілим числом, то елемент z є нерозкладним;

f) не існує елемента z, для якого $N(z) = \pm 2$;

g) якщо $N(z) = \pm 4$, то елемент z є нерозкладним;

h) кожен із елементів 2, $\sqrt{5}+1$, $\sqrt{5}-1$, $3+\sqrt{5}$, $3-\sqrt{5}$ є нерозкладним;

i) елемент 2 не є асоційованим із жодним з елементів $\sqrt{5}+1$, $\sqrt{5}-1$, $3 + \sqrt{5}$ і $3 - \sqrt{5}$.

Розв'язання. а) Нехай $z = n + m\sqrt{5}$, $u = p + q\sqrt{5}$. Тоді

$$z \cdot u = (np + 5mq) + (nq + mp)\sqrt{5}.$$

Маємо:

$$N(z \cdot u) = (n^2 - 5m^2)(p^2 - 5q^2) =$$
$$= n^2p^2 - 5n^2q^2 - 5m^2p^2 + 25m^2q^2 =$$
$$(np + 5mq)^2 - 5(nq + mp)^2 = N(z) \cdot N(u).$$

b) Число $N(z)$ є цілим. Тому з a) та рівності $N(z) = 1$ випливає, що дільники одиниці мають норму ± 1. Отже, ця умова є необхідною.

Навпаки, якщо $N(n + m\sqrt{5}) = \pm 1$, то з рівності

$$(n + m\sqrt{5})(n - m\sqrt{5}) = n^2 - 5m^2 = \pm 1$$

випливає, що елемент $n + m\sqrt{5}$ є дільником одиниці.

c) Нехай

$$(2 + \sqrt{5})(x + y\sqrt{5}) = (2x + 5y) + (x + 2y)\sqrt{5} = 1.$$

Тоді $2x + 5y = 1$ і $x + 2y = 0$, звідки $x = -2$, $y = 1$. Отже, для $2 + \sqrt{5}$ існує обернений елемент $-2 + \sqrt{5}$.

d) Вони асоційовані, бо їх частка $\dfrac{3 + \sqrt{5}}{1 - \sqrt{5}} = -2 - \sqrt{5}$, як випливає з c), є дільником одиниці.

e) Нехай $N(z)$ є простим цілим числом і $z = uv$. Тоді з рівності $N(z) = N(u) \cdot N(v)$ випливає, що один із множників дорівнює ± 1. Без обмеження загальності можна вважати, що $N(u) = \pm 1$. Але тоді з b) випливає, що u є дільником одиниці. Отже, кожен розклад елемента z містить дільник одиниці, а тому z є нерозкладним.

f) Нехай $n^2 - 5m^2 = \pm 2$. Тоді $n^2 \pm 2 = 5m^2$, отже, $n^2 \pm 2$ ділиться на 5. Але квадрати цілих чисел при діленні на 5 дають в остачі лише 0, 1 і 4, тому $n^2 \pm 2$ не може ділитись на 5.

g) Нехай $N(z) = \pm 4$ і $z = uv$, причому жоден із множників не є дільником одиниці. Тоді з b) і a) випливає, що $N(u) = \pm 2$ і $N(v) = \pm 2$. Але це суперечить f).

h) Нерозкладність цих елементів випливає із g), бо

$$N(2) = N(3 + \sqrt{5}) = N(3 - \sqrt{5}) = 4,$$
$$N(\sqrt{5} + 1) = N(\sqrt{5} + 1) = -4.$$

i) якщо a — один із елементів $\sqrt{5} + 1$, $\sqrt{5} - 1$, $3 + \sqrt{5}$ або $3 - \sqrt{5}$, то частка $a/2$ не належить кільцю $\mathbb{Z}[\sqrt{5}]$. Тому 2 не є асоційованим із a. $\square$

Задача 2. *Знайдіть у кільці* $K = \mathbb{Z}[\sqrt{-6}]$ *усі (з точністю до асоційованості і порядку множників) розклади числа* 10 *у добуток нерозкладних елементів.*

Розв'язання. Кільце $\mathbb{Z}[\sqrt{-6}] = \{a + ib\sqrt{6} \mid a, b \in \mathbb{Z}\}$ є підкільцем поля $\mathbb{C}$ комплексних чисел. Тому можна розглядати норму $N(a+ib\sqrt{6})=a^2+6b^2$ його елементів, причому ця норма є мультиплікативною, тобто $N(uv) = N(u)N(v)$, і набуває лише цілих значень.

Міркуючи далі подібно як при розв'язанні попередньої задачі, спочатку знайдемо з точністю до асоційованості всі власні дільники числа 10. Позаяк $N(10) = 100$, то нормою такого дільника може бути одне з чисел 2, 4, 5, 10, 20, 25 або 50. Позаяк для кожного $t \in \{2, 5, 20.50\}$ рівняння $m^2 + 6n^2 = t$ не має цілих розв'язків, то в кільці K немає чисел із нормою 2, 5, 20 і 50. Норму 4 мають числа ± 2, норму 10 — числа $\pm 2 \pm \sqrt{6}i$, норму 25 — числа ± 5. Безпосередньо перевіряється, що 10 ділиться на кожне з цих чисел. А з того, що в K немає чисел із нормою 2 і 5, випливає, що всі ці числа є нерозкладними. Тому розклад числа 10 у добуток нерозкладних елементів містить або два множники із нормами 4 і 25 відповідно, або два множники із нормою 10. Із точністю до порядку це дає наступні 4 розклади:

$$10 = 2 \cdot 5 = (-2) \cdot (-5) = (2 + i\sqrt{6})(2 - i\sqrt{6}) = (-2 + i\sqrt{6})(-2 - i\sqrt{6}).$$

Враховуючи, що елементи, які розрізняються знаком, є асоційованими, остаточно отримуємо два розклади:

$$10 = 2 \cdot 5 = (2 + i\sqrt{6})(2 - i\sqrt{6}). \qquad \square$$

Задача 3. *Розкладіть у кільці* $\mathbb{Q}[x, y]$ *на незвідні множники многочлен a)* $x^3 - y^3$; *b)* $x^4 - y^2$; *c)* $x^7 + 2x^3y + 3x^2 + 9y$.

Розв'язання. а) Є очевидний розклад $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$. Доведемо, що обидва множники в правій частині є незвідними. Незвідність першого множника випливає з того, що він є многочленом першого степеня. Якщо другий множник є звідним, то його дільники є многочленами першого степеня, а розклад має вигляд

$$x^2 + xy + y^2 = (ax + by + c)(px + qy + r).$$

Позаяк множники в правій частині ми розглядаємо з точністю до асоційованості (а в кільці многочленів $\mathbb{Q}[x, y]$ це означає — з точністю до

скалярного множника), то можна вважати, що $a = p = 1$. Це дає рівність

$$x^2 + xy + y^2 = x^2 + (b+q)xy + bqy^2 + (c+r)x + (br+cq)y + cr.$$

Звідси, зокрема, випливає, що $b+q = 1$ і $bq = 1$. Тому за теоремою Вієта b і q мають бути коренями рівняння $z^2 - z + 1$. Але це рівняння не має раціональних коренів. Отже, множник $x^2 + xy + y^2$ також є незвідним.

b) Як і в попередньому випадку покажемо, що в очевидному розкладі $x^4 - y^2 = (x^2 + y)(x^2 - y)$ обидва множники є незвідними. Справді, якщо перший множник розкладається, то можна вважати, що цей розклад має вигляд

$$x^2 + y = (x + ay + b)(x + c).$$

Але тоді з рівності

$$(x + ay + b)(x + c) = x^2 + axy + acy + (b + c)x + bc = x^2 + y$$

випливає, що $a = 0$ і $ac = 1$, що неможливо.

Незвідність другого множника доводиться аналогічно.

c) Многочлен $x^7 + 2x^3y + 3x^2 + 9y$ відносно змінної y має степінь 1. Якщо він звідний, то він розкладається в добуток двох множників ненульового степеня, один з яких має бути многочленом $f(x)$ лише від змінної x, а другий має мати відносно змінної y степінь 1 (тому його можна записати у вигляді $g(x)y + h(x)$). Із рівності

$$x^7 + 2x^3y + 3x^2 + 9y = f(x)(g(x)y + h(x))$$

тоді випливає, що $f(x)g(x) = 2x^3 + 9$ і $f(x)h(x) = x^7 + 3x^2$. Зокрема, многочлени $2x^3 + 9$ і $x^7 + 3x^2$ мають спільний дільник $f(x)$ ненульового степеня. Але за допомогою алгоритму Евкліда легко перевіряється, що многочлени $2x^3+9$ і x^7+3x^2 є взаємно простими. Отримана суперечність доводить, що многочлен $x^7 + 2x^3y + 3x^2 + 9y$ є незвідним. □

Задача 4. *Чи правильно, що коли для довільного c виконується рівносильність $c \mid a \Leftrightarrow c \mid b$, то $a \sim b$?*

Розв'язання. Покладемо $c = a$. Тоді рівносильність набуває вигляду $a \mid a \Leftrightarrow a \mid b$. Позаяк ліва частина рівносильності є істинною, то $a \mid b$. Аналогічно у випадку $c = b$ отримаємо, що $b \mid a$. Отже, $a \sim b$, тобто твердження є правильним. □

Задача 5. *З'ясуйте, чи ділиться a на b в кільці $\mathbb{Z}[\sqrt{3}]$, якщо*
а) $a = 8 - \sqrt{3}$, $b = 3 + 2\sqrt{3}$; *б)* $a = 9 - \sqrt{3}$, $b = 5 - 2\sqrt{3}$.

Розв'язання. Кільце $\mathbb{Z}[\sqrt{3}]$ є підкільцем поля $\mathbb{R}$. Тому ми спочатку виконуємо ділення в полі $\mathbb{R}$, а потім з'ясовуємо, чи потрапляє результат у кільце $\mathbb{Z}[\sqrt{3}]$.

а) $\dfrac{8-\sqrt{3}}{3+2\sqrt{3}} = \dfrac{(8-\sqrt{3})(3-2\sqrt{3})}{(3+2\sqrt{3})(3-2\sqrt{3})} = \dfrac{30-19\sqrt{3}}{-3} = -10+\dfrac{19}{3}\sqrt{3}$. Число $-10 + \dfrac{19}{3}\sqrt{3}$ не належить кільцю $\mathbb{Z}[\sqrt{3}]$, тому a на b не ділиться.

б) $\dfrac{9-\sqrt{3}}{5-2\sqrt{3}} = \dfrac{(9-\sqrt{3})(5+2\sqrt{3})}{(5-2\sqrt{3})(5+2\sqrt{3})} = \dfrac{39-13\sqrt{3}}{13} = 3+\sqrt{3}$. Позаяк частка $3 + \sqrt{3}$ належить кільцю $\mathbb{Z}[\sqrt{3}]$, то a на b ділиться. □

Задача 6. *Знайдіть у кільці* $K = \left\{ \dfrac{m+n\sqrt{3}i}{2} \,\middle|\, m \equiv n \pmod 2 \right\}$ *усі елементи, асоційовані з елементом* $a = 3 - \sqrt{3}i$.

Розв'язання. Асоційовані елементи розрізняються дільником одиниці. Тому спочатку знайдемо в кільці K усі дільники одиниці. Норма $N(z)$ комплексного числа $z = \dfrac{m+n\sqrt{3}i}{2}$ дорівнює $\dfrac{m^2+3n^2}{4}$. Позаяк $m \equiv n \pmod 2$, то можемо вважати, що $m = n + 2k$. Але тоді

$$\frac{m^2+3n^2}{4} = \frac{(n+2k)^2+3n^2}{4} = \frac{n^2+4nk+4k^2+3n^2}{4} = n^2+nk+k^2.$$

Отже, норма кожного елемента з K є цілим числом. Позаяк при множенні комплексних чисел їх норми також перемножаються, а $N(1) = 1$, то в кільці K усі дільники одиниці мають норму 1.

Усі розв'язки рівняння

$$(m^2 + 3n^2)/4 = 1$$

легко знаходяться безпосередньо: $n = 0$, $m = \pm 2$ або $n = \pm 1$, $m = \pm 1$. Це дає нам 6 елементів із нормою 1:

$$\varepsilon_1 = 1, \quad \varepsilon_2 = -1,$$
$$\varepsilon_3 = \frac{1+\sqrt{3}i}{2}, \quad \varepsilon_4 = \frac{1-\sqrt{3}i}{2}, \quad \varepsilon_5 = \frac{-1+\sqrt{3}i}{2}, \quad \varepsilon_6 = \frac{-1-\sqrt{3}i}{2}.$$

Усі вони є дільниками одиниці, бо $\varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_3\varepsilon_4 = \varepsilon_5\varepsilon_6 = 1$. Тому елементами, асоційованими з елементом a, будуть:

$$\varepsilon_1 a = a, \quad \varepsilon_2 a = -a, \quad \varepsilon_3 a = 3 + \sqrt{3}i, \quad \varepsilon_4 = 2\sqrt{3}i,$$
$$\varepsilon_5 = -\varepsilon_4 a = -2\sqrt{3}i, \quad \varepsilon_6 a = -\varepsilon_3 a = -3 - \sqrt{3}i. \qquad \square$$

Задача 7. *Нехай*

$$K = \{a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid n \neq 1;\ a_0, a_2, a_3, \ldots, a_n \in \mathbb{Z}\}$$

— кільце тих многочленів із цілими коефіцієнтами, які не містять лінійного члена.
a) Доведіть, що K є областю цілісності.
b) Знайдіть в K елемент, який є нерозкладним, але не є простим.
c) Знайдіть в K елемент, для якого є розклади в добуток нерозкладних різної довжини.
d) Доведіть, що для елементів x^2 і x^3 найбільший спільний дільник існує, а найменше спільне кратне — ні.
e) Доведіть, що для елементів x^5 і x^6 не існує ні найбільшого спільного дільника, ні найменшого спільного кратного.

Розв'язання. a) K містить одиницю і є підкільцем області цілісності $\mathbb{Z}[x]$. Тому K також є областю цілісності.

b) Розклад на множники в K є одночасно і розкладом на множники в $\mathbb{Z}[x]$. Але K не містить многочленів першого степеня. Тому многочлени другого і третього степеня з K будуть в K нерозкладними. Зокрема, нерозкладним елементом буде x^3. Крім того, x^3 ділить в K добуток $x^2 \cdot x^4$, але не ділить жоден із множників x^2 і x^4. Тому x^3 не є простим елементом.

c) Ми вже з'ясували, що многочлени x^2 і x^3 є нерозкладними в K. Тому потрібний елемент знайти легко. Наприклад, для x^6 маємо: $x^6 = x^3x^3 = x^2x^2x^2$.

d) Із однозначності розкладу на незвідні множники у більшому кільці $\mathbb{Q}[x]$ випливає, що з точністю до асоційованості в кільці K дільниками многочлена x^2 будуть лише 1 і x^2, а дільниками x^3 — лише 1 і x^3. Тому $\text{НСД}(x^2, x^3) = 1$.

З іншого боку, кожен із многочленів x^5 і x^6 є спільним кратним x^2 і x^3. Якщо $\text{НСК}(x^2, x^3)$ існує, то воно має бути спільним дільником многочленів x^5 і x^6. Але з точністю до асоційованості спільними дільниками x^5 і x^6 є лише 1, x^2 і x^3, жоден із яких не є спільним кратним x^2 і x^3. Тому найменше спільне кратне многочленів x^2 і x^3 не існує.

е) Ми вже з'ясували, що з точністю до асоційованості спільними дільниками x^5 і x^6 є лише 1, x^2 і x^3. Але жоден із дільників не ділиться на два інших. Тому НСД(x^5, x^6) не існує.

З іншого боку, кожен із многочленів x^8 і x^9 є спільним кратним x^5 і x^6. Якщо многочлен $f(x)$ є найменшим спільним кратним x^5 і x^6, то $f(x)$ має степінь ≥ 6 (бо ділиться на x^6) і ≤ 8 (бо ділить x^8). Але x^5 не має кратних степеня 6, а x^6 не має кратних степеня 7. Тому $f(x)$ має степінь 8. Але x^9 не має дільників степеня 8. Отже, припущення про існування НСК(x^5, x^6) приводить до суперечності. □

Задача 8. *З'ясуйте, чи існує в кільці $\mathbb{Z}[\sqrt{-3}]$ найбільший спільний дільник чисел 4 і $2 + 2\sqrt{-3}$.*

Розв'язання. Кільце $\mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} \mid a, b \in \mathbb{Z}\}$ є підкільцем поля $\mathbb{C}$ комплексних чисел. Тому можна розглядати норму $N(a+ib\sqrt{3}) = a^2+3b^2$ його елементів. Ця норма набуває лише цілих значень і є мультиплікативною: $N(uv) = N(u)N(v)$. Позаяк $N(4) = N(2 + 2\sqrt{-3}) = 16$, то норма нетривіальних дільників цих чисел може дорівнювати лише 2, 4 і 8. Рівняння $a^2 + 3b^2 = 2$ і $a^2 + 3b^2 = 8$ не мають цілих розв'язків, тому в кільці $\mathbb{Z}[\sqrt{-3}]$ елементів із нормою 2 або 8 нема. Розв'язками рівняння $a^2 + 3b^2 = 4$ є $(\pm 2, 0)$ і $(\pm 1, \pm 1)$, що дає нам 6 елементів ± 2 і $\pm 1 \pm \sqrt{-3}$ із нормою 4. Легко перевіряється, що вони справді є спільними дільниками чисел 4 і $2 + 2\sqrt{-3}$. Однак у кільці $\mathbb{Z}[\sqrt{-3}]$ жодне з чисел $\pm 1 \pm \sqrt{-3}$ не ділиться на 2, а жодне з чисел ± 2 не ділиться на $1 + \sqrt{-3}$. Тому найбільшого спільного дільника чисел 4 і $2 + 2\sqrt{-3}$ не існує. □

Задача 9. *Доведіть, що кільце $\mathbb{Z}[\sqrt{5}]$ не є факторіальним.*

Розв'язання. У кільці $\mathbb{Z}[\sqrt{5}]$ маємо такі розклади числа 4:

$$4 = 2 \cdot 2 = (\sqrt{5} + 1)(\sqrt{5} - 1) = (3 + \sqrt{5})(3 - \sqrt{5}).$$

У розв'язанні задачі 1 показано, що всі множники цих розкладів є нерозкладними елементами кільця $\mathbb{Z}[\sqrt{5}]$, але число 2 не є асоційованим із жодним із множників двох останніх розкладів. Тому кільце $\mathbb{Z}[\sqrt{5}]$ не є факторіальним. □

Задача 10. *Доведіть, що кільце дійсних степеневих рядів*

$$\mathbb{R}[[x]] = \Big\{ \sum_{n=0}^{\infty} a_n x^n \mid a_0, a_1, \ldots \in \mathbb{R} \Big\}$$

має єдиний, з точністю до асоційованості, нерозкладний елемент і є факторіальним.

Розв'язання. Спочатку з'ясуємо, який вигляд мають у кільці $\mathbb{R}[[x]]$ дільники одиниці. Очевидно, що умова $a_0 \neq 0$ є необхідною для оборотності елемента $a = \sum_{n=0}^{\infty} a_n x^n$. Виявляється, що ця умова є і достатньою. Справді, рівність

$$(a_0 + a_1 x + a_2 x^2 + \cdots)(b_0 + b_1 x + b_2 x^2 + \cdots) = 1$$

рівносильна такій нескінченній системі рівнянь

$$\begin{gathered} a_0 b_0 = 1, \\ a_0 b_1 + a_1 b_0 = 0, \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{gathered}$$

відносно невідомих коефіцієнтів b_0, b_1, b_2, $\ldots$.

Але якщо $a_0 \neq 0$, то ця система легко розв'язується:

$$b_0 = \frac{1}{a_0}, \quad b_1 = \frac{1}{a_0}(-a_1 b_0), \quad b_2 = \frac{1}{a_0}(-a_1 b_1 - a_2 b_0), \ \ldots \ .$$

Спробуємо тепер розкласти у добуток елемент x:

$$x = (c_0 + c_1 x + c_2 x^2 + \cdots)(d_0 + d_1 x + d_2 x^2 + \cdots). \tag{4}$$

Позаяк $c_0 d_0 = 0$, то можна вважати, що $c_0 = 0$. Але тоді з рівності $1 = c_0 d_1 + c_1 d_0 = c_1 d_0$ випливає, що $d_0 \neq 0$, тобто другий множник в (4) є дільником одиниці. Це означає, що елемент x є нерозкладним.

Нехай $a = \sum_{n=0}^{\infty} a_n x^n$ — довільний ненульовий елемент кільця $\mathbb{R}[[x]]$ і a_k — ненульовий коефіцієнт із найменшим індексом. Тоді a можна записати у вигляді

$$a = x^k (a_k + a_{k+1} x + a_{k+2} x^2 + \cdots). \tag{5}$$

Оскільки $a_k \neq 0$, то множник у дужках є дільником одиниці. Це означає, що з точністю до асоційованості, кожен ненульовий елемент кільця $\mathbb{R}[[x]]$ є степенем x. Тому x є єдиним нерозкладним елементом кільця $\mathbb{R}[[x]]$. Факторіальність кільця $\mathbb{R}[[x]]$ тепер випливає з того, що показник k у розкладі (5) визначений однозначно. $\square$

Задача 11. *Доведіть, що в кільці многочленів K із задачі* 7 множина $I = \{a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid a_2, \ldots, a_n \in \mathbb{Z}\}$ *утворює ідеал, який не є головним.*

Розв'язання. Очевидно, що множина I замкнена відносно додавання й віднімання. Крім того, кратне довільного многочлена з I також належить I. Тому I є ідеалом.

Припустимо, що ідеал I є головним і породжується многочленом $f(x) = a_2x^2 + a_3x^3 + \cdots + a_nx^n$. Добуток $f(x)K$ повинен містити многочлен x^2, тому $a_3 = \cdots = a_n = 0$ і $f(x) = a_2x^2$. Але тоді для довільного $g(x) = b_0 + b_2x^2 + \cdots + b_mx^m$ із K маємо:

$$f(x)g(x) = a_2b_0x^2 + a_2b_2x^4 + \cdots + a_2b_mx^{m+2}.$$

Отже, добуток $f(x)K$ не містить многочленів із ненульовим коефіцієнтом при x^3. А в I такі многочлени є. Тому $f(x)K \neq I$ і I не є головним ідеалом. □

Задача 12. *Доведіть, що кільце* $\mathbb{Z}[\sqrt{-3}] = \{m + ni\sqrt{3} \mid m, n \in \mathbb{Z}\}$ *не є евклідовим, а кільце* $K = \left\{ \dfrac{m + in\sqrt{3}}{2} \,\middle|\, m \equiv n \pmod 2 \right\}$ *— евклідове.*

Розв'язання. Для комплексного числа $z = x + iy$ через $N(z)$ позначимо його норму $x^2 + y^2$. Із рівності $N(z) = |x|^2$ випливає мультиплікативність норми: $N(uv) = N(u)N(v)$. У кожному з кілець $\mathbb{Z}[\sqrt{-3}]$ і K норма ненульового елемента є натуральним числом: для $\mathbb{Z}[\sqrt{-3}]$ це очевидно, а для K випливає з того, що коли $n = m + 2k$, то

$$N\Big(\frac{m + in\sqrt{3}}{2}\Big) = \frac{m^2}{4} + \frac{3n^2}{4} =$$
$$= \frac{m^2}{4} + \frac{3(m^2 + 4mk + 4k^2)}{4} = m^2 + 3mk + 3k^2.$$

У кільці $\mathbb{Z}[\sqrt{-3}]$ норму 1 мають лише елементи 1 і -1, а елементів із нормою 2 взагалі нема, бо рівняння $m^2 + 3n^2 = 1$ не має цілих розв'язків. Тому в кільці $\mathbb{Z}[\sqrt{-3}]$ асоційовані елементи можуть розрізнятися щонайбільше знаком, а елементи з нормою 4 є нерозкладними. Звідси випливає, що два розклади числа 4

$$4 = 2 \cdot 2 = (1 + i\sqrt{3}) \cdot (1 - i\sqrt{3})$$

є розкладами в добуток нерозкладних елементів, причому множники першого розкладу не є асоційованими із множниками другого. Це означає, що кільце $\mathbb{Z}[\sqrt{-3}]$ не є факторіальним. А тому воно не є і евклідовим.

Перейдемо тепер до кільця K. Легко пересвідчитись, що корені шостого степеня з одиниці 1, $\varepsilon = \dfrac{1+i\sqrt{3}}{2}$, $\varepsilon - 1 = \dfrac{-1+i\sqrt{3}}{2} = \varepsilon^2$, -1, $-\varepsilon = \dfrac{-1-i\sqrt{3}}{2}$ і $1-\varepsilon = \dfrac{1-i\sqrt{3}}{2} = -\varepsilon^2$ належать кільцю K. На комплексній площині цим числам відповідають вершини правильного шестикутника, що лежать на колі радіуса 1 із центром у початку координат.

Кожен елемент $\dfrac{m+in\sqrt{3}}{2}$ кільця K можна записати у вигляді $\dfrac{m-n}{2} + n\dfrac{1+i\sqrt{3}}{2} = m' + n\varepsilon$, де $m' = \dfrac{m-n}{2}$ і n — цілі. Зрозуміло, що m' і n можуть бути довільними. Це означає, що на комплексній площині елементам кільця K будуть відповідати вершини решітки з правильних трикутників із стороною 1. Множення на фіксоване число $b \neq 0$ (тобто перехід від K до множини bK) поверне цю решітку на кут $\arg b$ і розтягне в $|b|$ разів.

Розглянемо тепер довільний елемент $a \in K$. Якщо точка a є одним із вузлів решітки bK, то це означає, що в кільці K a ділиться на b націло. У противному разі точка a потрапляє на сторону або всередину одного з трикутників решітки. Але в правильному трикутнику для будь-якої його точки, відмінної від вершини, віддаль від цієї точки до кожної вершини менша за довжину сторони трикутника. Кожна з вершин трикутника є кратним числа b. Вибираючи одну з вершин, одержуємо рівність

$$a = qb + (a - qb), \tag{6}$$

де $q \in K$ і $|a - qb| < |b|$. Звідси $N(a-qb) = |a-qb|^2 < |b|^2 = N(b)$.

Таким чином, у кільці K є можливим ділення з остачею. Тому воно є евклідовим. □

Задача 13. *Користуючись алгоритмом Евкліда*
a) у кільці $\mathbb{Z}_{359}$ *обчисліть елемент, обернений до* 245;
b) у факторкільці $\mathbb{Z}_2[x]/I$, *де* $I = (x^4 + x^3 + x^2 + x + 1)$, *обчисліть елемент, обернений до* $(x^3 + x + 1) + I$.

Розв'язання. a) Спочатку за допомогою алгоритму Евкліда знайдемо НСД чисел 359 і 245 (зручно дані числа і остачі, які виникатимуть у процесі застосування алгоритму, виділити жирним шрифтом):

$$\mathbf{359} = 1 \cdot \mathbf{245} + \mathbf{114}, \tag{7}$$
$$\mathbf{245} = 2 \cdot \mathbf{114} + \mathbf{17}, \tag{8}$$
$$\mathbf{114} = 6 \cdot \mathbf{17} + \mathbf{12}, \tag{9}$$
$$\mathbf{17} = 1 \cdot \mathbf{12} + \mathbf{5}, \tag{10}$$
$$\mathbf{12} = 2 \cdot \mathbf{5} + \mathbf{2}, \tag{11}$$
$$\mathbf{5} = 2 \cdot \mathbf{2} + \mathbf{1}. \tag{12}$$

Отже, числа 359 і 245 є взаємно простими, а тому в кільці $\mathbb{Z}_{359}$ елемент, обернений до 245, існує. Щоб знайти його, "прокручуємо" рівності (7)–(12) знизу вгору:

$$\mathbf{1} = \mathbf{5} - 2 \cdot \mathbf{2} = \mathbf{5} - 2 \cdot (\mathbf{12} - 2 \cdot \mathbf{5}) = 5 \cdot \mathbf{5} - 2 \cdot \mathbf{12} =$$
$$= 5 \cdot \mathbf{17} - 7 \cdot \mathbf{12} = 47 \cdot \mathbf{17} - 7 \cdot \mathbf{114} = 47 \cdot (\mathbf{245} - 2 \cdot \mathbf{114}) - 7 \cdot \mathbf{114} =$$
$$= 47 \cdot \mathbf{245} - 101 \cdot \mathbf{114} = 47 \cdot \mathbf{245} - 101 \cdot (\mathbf{359} - 1 \cdot \mathbf{245}) =$$
$$= 148 \cdot \mathbf{245} - 101 \cdot \mathbf{359}.$$

Таким чином, ми знайшли зображення НСД чисел 359 і 245 у вигляді лінійної комбінації цих чисел: $1 = 148 \cdot 245 - 101 \cdot 359$. За модулем 359 остання рівність набуває вигляду $1 \equiv 148 \cdot 245$. Тому в кільці $\mathbb{Z}_{359}$ елементом, оберненим до 245, буде 148.

b) Аналогічно попередньому, спочатку за допомогою алгоритму Евкліда знайдемо НСД многочленів $f(x) = x^4 + x^3 + x^2 + x + 1$ і $g(x) = x^3 + x + 1$:

$$f(x) = (x+1) \cdot g(x) + \boldsymbol{x}, \tag{13}$$
$$g(x) = (x^2+1) \cdot \boldsymbol{x} + \mathbf{1}. \tag{14}$$

"Прокручуючи" рівності (13)–(14) знизу вгору, знаходимо зображення НСД цих многочленів у вигляді їх лінійної комбінації (зауважимо, що в кільці $\mathbb{Z}_2$ додавання збігається з відніманням):

$$\mathbf{1} = g(x) + (x^2+1) \cdot \boldsymbol{x} = g(x) + (x^2+1) \cdot (f(x) + (x+1) \cdot g(x)) =$$
$$= (x^2+1) \cdot f(x) + (x^3 + x^2 + x) \cdot g(x).$$

Добуток $(x^2+1)\cdot f(x)$ належить ідеалу I і за модулем цього ідеалу отримана рівність набуває вигляду $1 \equiv (x^3+x^2+x)\cdot g(x)$. Тому у факторкільці $\mathbb{Z}_2[x]/I$ елементом, оберненим до $(x^3+x+1)+I$, буде $(x^3+x^2+x)+I$. □

Задача 14. *Знайдіть у кільці $\mathbb{Z}[i]$ НСД чисел $a = 62-7i$ і $b = 19+25i$.*

Розв'язання. Позаяк кільце $\mathbb{Z}[i]$ є евклідовим, то для знаходження НСД можна використати алгоритм Евкліда. Спочатку ділимо з остачею a на b:

$$\frac{62-7i}{19+25i} = \frac{1098-1808i}{986} = (1-2i) + \frac{112+164i}{986}.$$

Норма другого доданка менша 1, тому за частку від ділення можна взяти перший доданок $1-2i$. Отримуємо:

$$62-7i = (1-2i)\cdot(19+25i) + (-7+6i).$$

Далі ділимо b на першу остачу $r_1 = -7+6i$:

$$\frac{19+25i}{-7+6i} = \frac{17-289i}{85} = -3i + \frac{17-34i}{85}.$$

Норма другого доданка менша 1, тому за частку від ділення можна взяти перший доданок $-3i$. Отримуємо:

$$19+25i = (-3i)\cdot(-7+6i) + (1+4i).$$

Тепер ділимо r_1 на другу остачу $r_2 = 1+4i$:

$$\frac{-7+6i}{1+4i} = \frac{17+34i}{17} = 1+2i.$$

Ділення відбулося націло. Останньою ненульовою остачею є число $r_2 = 1+4i$. Воно й буде НСД чисел $a = 62-7i$ і $b = 19+25i$. □

Задача 15. *Розкладіть у кільці $\mathbb{Z}[i]$ на нерозкладні множники число $14+8i$.*

Розв'язання. Норма числа $14+8i$ дорівнює $14^2+8^2 = 260$. Тому норми дільників числа $14+8i$ повинні бути дільниками числа 260. Найменшим неодиничним дільником числа 260 є 2. У кільці $\mathbb{Z}[i]$ норму 2 мають числа

$\pm 1 \pm i$. Вони є асоційованими, тому з точністю до асоційованості можемо обмежитися лише числом $1+i$. У кільці $\mathbb{Z}[i]$ воно є нерозкладним. Перевіримо, чи є воно дільником числа $14+8i$:

$$\frac{14+8i}{1+i} = 11-3i, \quad \frac{11-3i}{1+i} = 4-7i, \quad \frac{4-7i}{1+i} = -\frac{3}{2} - \frac{11}{2}i \notin \mathbb{Z}[i].$$

Таким чином, $14+8i = (1+i)^2(4-7i)$. Далі будемо розкладати на множники число $4-7i$. Його норма дорівнює $4^2+7^2 = 65 = 5 \cdot 13$. Розв'язучи рівняння $a^2+b^2=5$, знаходимо, що в кільці $\mathbb{Z}[i]$ норму 5 мають числа $\pm 1 \pm 2i$ і $\pm i \pm i$. Із точністю до асоційованості можемо обмежитися лише числами $2+i$ і $1+2i$. Позаяк їх норма є простим числом, то вони нерозкладні. Перевіримо, чи є вони дільниками числа $4-7i$:

$$\frac{4-7i}{2+i} = \frac{1}{5} - \frac{18}{5}i \notin \mathbb{Z}[i], \quad \frac{4-7i}{1+2i} = -2-3i.$$

Таким чином, дільником є лише число $1+2i$. Позаяк нормою частки $-2-3i$ є просте число 13, то частка також є нерозкдадним елементом.

Враховуючи, що кільце $\mathbb{Z}[i]$ є евклідовим, а тому з точністю до асоційованості і порядку множників розклад на нерозкладні множники є єдиним, одержуємо:

$$14+8i = -(1+i)^2(1+2i)(2+3i). \qquad \square$$

Основні задачі

16. Доведіть, що a) 1 є дільником кожного елемента кільця; b) 0 ділиться на будь–який елемент кільця.

17. Доведіть, що елемент a буде дільником одиниці тоді й лише тоді, коли a ділить кожен елемент кільця.

18. Доведіть, що елемент, асоційований з нерозкладним, сам є нерозкладним.

19. Нехай $a \sim a'$ і $b \sim b'$.
a) Чи випливає звідси, що $ab \sim a'b'$?
b) Чи випливає звідси, що $a+b \sim a'+b'$?

20. Чи правильно, що коли для довільного c виконується рівносильність $a|c \Leftrightarrow b|c$, то $a \sim b$?

21. Доведіть, що всі ненульові класи асоційованих елементів мають однакову потужність.

22. Нехай K — область цілісності, $K_1 \subseteq K$ — підкільце і $a \in K_1$. З'ясуйте, які з наступних імплікацій є правильними:
a) якщо a є простим в K_1, то a є простим в K;
b) якщо a є простим в K, то a є простим в K_1.

23. З'ясуйте, чи ділиться a на b в кільці $\mathbb{Z}[\sqrt{2}]$:
a) $a = 7 + 2\sqrt{2}$, $b = 3 - \sqrt{2}$;
b) $a = 6 - \sqrt{2}$, $b = 5 + 2\sqrt{2}$;
c) $a = 11\sqrt{2} - 5$, $b = 1 + 4\sqrt{2}$.

24. Знайдіть у кільці $\mathbb{Z}[\sqrt{-3}]$ усі (з точністю до асоційованості) власні дільники і всі (з точністю до асоційованості і порядку множників) розклади в добуток нерозкладних елементів числа a) 4; b) $5 - i\sqrt{3}$; c) $3 + 2i\sqrt{3}$.

25. Доведіть, що в кільці $\mathbb{Z}[\sqrt{-5}]$ елементи $2 + \sqrt{-5}$ і $2 - \sqrt{-5}$ є нерозкладними, але не є простими.

26. З'ясуйте, чи буде звідним у кільці $\mathbb{R}[x, y]$ многочлен a) $x^2 + y^2$; b) $x^3 + y^3$; c) $x^4 + y^4$; d) $x^3 + x^2y + xy^2 + y^3$; e) $x^4 + x^3y + x^2y^2 + xy^3 + y^4$.

27. Доведіть, що для довільних елементів a, b, c виконується рівність $\text{НСД}(a, b) = \text{НСД}(a, ac + b)$.

28. Доведіть, що у факторіальному кільці для довільних елементів a, b, c
a) $\text{НСД}(a, b, c) = \text{НСД}(a, \text{НСД}(b, c)) = \text{НСД}(\text{НСД}(a, b), c)$;
b) $\text{НСК}(a, b, c) = \text{НСК}(a, \text{НСК}(b, c)) = \text{НСК}(\text{НСК}(a, b), c)$.

29. Знайдіть у кільці K із задачі 7 такі елементи a, b, c, для яких не виконується рівність $\text{НСД}(a, \text{НСД}(b, c)) = \text{НСД}(\text{НСД}(a, b), c)$.

30. Доведіть, що в кільці K із задачі 7 $\text{НСД}(x^3, x^4)$ існує, а $\text{НСК}(x^3, x^4)$ не існує.

31. Нехай у факторіальному кільці елемент a розкладається в добуток $a = bc$ взаємно простих множників b і c. Доведіть, що
a) коли a є квадратом, то кожен із множників b і c є квадратом;
b) коли a є кубом, то кожен із множників b і c є кубом.

32. Доведіть, що кільце $\mathbb{Z}[\sqrt{-5}] = \{m + ni\sqrt{5} \mid m, n \in \mathbb{Z}\}$ не є факторіальним.

33. Нехай $\varphi : K \to R$ — епіморфізм кілець.
a) Чи правильно, що образ $\varphi(I)$ головного ідеалу кільця K буде головним ідеалом кільця R?
b) Чи правильно, що повний прообраз $\varphi^{-1}(J)$ головного ідеалу кільця R буде головним ідеалом кільця K?
c) Чи правильно, що R буде кільцем головних ідеалів, якщо таким є кільце K?

34. Доведіть, що кожне з наступних кілець не є кільцем головних ідеалів: a) $\mathbb{Z}[x]$; b) $P[x, y]$, де P — поле.

35. Нехай a і b — взаємно прості елементи з кільця K головних ідеалів. Доведіть, що $K/(ab) \simeq K/(a) \times K/(b)$.

36. Нехай $a_1, \ldots, a_n$ і $b_1, \ldots, b_m$ — елементи кільця головних ідеалів K. Доведіть, що коли кожен a_i є взаємно простим із кожним b_j, то елементи $a_1 \cdots a_n$ і $b_1 \cdots b_m$ також є взаємно простими.

37. За допомогою алгоритму Евкліда знайдіть НСД d чисел a і b і його лінійне зображення $d = ua + vb$:
a) $a = 180$, $b = 252$; b) $a = 2873$, $b = 6643$; c) $a = 4148$, $b = 7684$; d) $a = 1001$, $b = 6654$.

38. Користуючись алгоритмом Евкліда, обчисліть у кільці $\mathbb{Z}_n$ елемент, обернений до a, якщо a) $n = 433$, $a = 315$; b) $n = 863$, $a = 666$; c) $n = 2003$, $a = 1234$;

39. З'ясуйте, чи має дана конґруенція розв'язок, і якщо має, то знайдіть його: a) $25x \equiv 14 \pmod{36}$; b) $26x \equiv 14 \pmod{36}$;
c) $27x \equiv 14 \pmod{36}$.

40. Користуючись алгоритмом Евкліда, обчисліть у факторкільці $\mathbb{Z}_2[x]/I$ елемент, обернений до $g + I$, якщо
a) $I = (x^5 + x^4 + x^3 + x^2 + 1)$, $g = x^4 + x^3 + 1$;
b) $I = (x^5 + x^4 + x^2 + x + 1)$, $g = x^3 + x^2 + x + 1$;
c) $I = (x^5 + x^3 + 1)$, $g = x^4 + x^2 + x$.

41. Доведіть, що кільце $\mathbb{Z}[\sqrt{-2}]$ є евклідовим.

42. Знайдіть у кільці $\mathbb{Z}[i]$ НСД елементів a і b, якщо:
a) $a = 13 + 19i$, $b = 7 - 19i$; b) $a = 23 - 9i$, $b = 2 - 21i$;
c) $a = 24 + 5i$, $b = 12 - 7i$; d) $a = -2 + 29i$, $b = 25 - 5i$.

43. З'ясуйте, які з елементів a) 2; b) 3; c) $2 + i$; d) 5; e) $2 + 3i$ кільця $\mathbb{Z}[i]$ будуть нерозкладними.

44. Розкладіть у кільці $\mathbb{Z}[i]$ на нерозкладні множники число a) $7 + i$; b) $5 - 5i$; c) $1 + 13i$; d) $9 + 7i$; e) $11 + 3i$; f) $5 + i$; g) $7 + 3i$; h) $14 - 2i$.

45. Знайдіть у кільці $\mathbb{Z}[i]$ кількість дільників (з точністю до асоційованості) числа a) 16; b) 20; c) $10 + 10i$; d) $20 + 10i$; e) $26 - 78i$; f) $-28 + 96i$; g) $210 + 30i$.

46. Доведіть, що для кожного ненульового ідеала I кільця $\mathbb{Z}[i]$ факторкільце $\mathbb{Z}[i]/I$ буде скінченним.

47. Підрахуйте кількість елементів у факторкільці $\mathbb{Z}[i]/(a)$ і з'ясуйте, чи буде воно полем, якщо: a) $a = 1 + i$; b) $a = 2$; c) $a = 3$; d) $a = 5$.

Додаткові задачі

48. Доведіть, що в області цілісності кожен простий елемент є нерозкладним.

49. Доведіть, що коли многочлени $f(x)$ і $g(x)$ із $\mathbb{R}[x]$ є взаємно простими, то многочлен $f(x) + yg(x)$ із $\mathbb{R}[x, y]$ є незвідним.

50. Нехай p — просте число. Доведіть, що многочлен $x^2 + y^2 + z^2$ із $\mathbb{Z}_p[x, y, z]$ буде звідним тоді й лише тоді, коли $p = 2$.

51. a) Доведіть, що у факторіальному кільці для довільних елементів a, b, c виконується рівність НСД$(ca, cb) = c$НСД(a, b).

b) Знайдіть у кільці $K = \mathbb{Z}[\sqrt{-3}]$ елементи a, b, c, для яких рівність НСД$(ca, cb) = c$НСД(a, b) не виконується.

52. Доведіть, що підкільце

$$K = \{a_1 x^{\alpha_1} + \cdots + a_n x^{\alpha_n} \mid n \in \mathbb{N}, a_i \in \mathbb{R}, \alpha_i \geq 0\}$$

кільця Map$(\mathbb{R}^+, \mathbb{R})$ є областю цілісності, але не є факторіальним.

53. Нехай $\mathbb{Z}[1/2]$ — найменше підкільце поля $\mathbb{Q}$, яке містить $\mathbb{Z}$ і число $1/2$.

a) Доведіть, що кільце $\mathbb{Z}[1/2]$ є факторіальним.

b) Опишіть у кільці $\mathbb{Z}[1/2]$ всі дільники одиниці і всі нерозкладні елементи.

c) Доведіть, що кільце $\mathbb{Z}[1/2]$ є евклідовим.

54. Нехай $p_1, \ldots, p_k$ — прості числа. Доведіть, що кільце

$$\mathbb{Z}_{(p_1,\ldots,p_k)} := \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; n \text{ не ділиться на жодне з чисел } p_1, \ldots, p_k \right\}$$

— факторіальне, і $p_1, \ldots, p_k$ — з точністю до асоційованості усі нерозкладні елементи кільця $\mathbb{Z}_{(p_1,\ldots,p_k)}$.

55. Доведіть, що коли факторіальне кільце K має мінімальний ідеал, то воно є полем.

56. Доведіть теорему про існування розкладу на нерозкладні елементи для кожного з наступних кілець:
a) $\mathbb{Z}[\sqrt{-3}]$; b) $\mathbb{Z}[\sqrt{-5}]$; c) $\mathbb{Z}[\sqrt{-7}]$; d) $\mathbb{Z}\big[\frac{1+\sqrt{-3}}{2}\big]$; e) $\mathbb{Z}\big[\frac{1+\sqrt{-7}}{2}\big]$.

57. Доведіть, що коли область цілісності K не є полем, то кільце $K[x]$ є областю цілісності, але не є кільцем головних ідеалів.

58. Нехай P — поле. Доведіть, що в кільці $M_n(P)$ всі односторонні ідеали є головними.

59. Доведіть, що в кільці головних ідеалів рівняння $a_1x_1 + \cdots + a_nx_n = a$ має розв'язок тоді й лише тоді, коли a ділиться на найбільший спільний дільник коефіцієнтів $a_1, \ldots, a_n$.

60. Знайдіть у кільці $\mathbb{Z} \oplus \mathbb{Z}$ ненульовий простий ідеал, який не є максимальним.

61. Доведіть, що факторкільце скінченного кільця за простим ідеалом є тілом.

62.** Нехай K — кільце головних ідеалів. Доведіть, що для кожної матриці $A \in M_n(K)$ існують такі оборотні матриці $B, C \in M_n(K)$, що $BAC = \operatorname{diag}(a_1, a_2, \ldots, a_k, 0, \ldots, 0)$, причому $a_1 | a_2$, $a_2 | a_3$, $\ldots$, $a_{k-1} | a_k$.

63.* Доведіть для кільця $\mathbb{Z}[i]$ аналог теореми Ферма: якщо q — ґаусове просте число і a не ділиться на q, то $a^{N(q)-1} - 1$ ділиться на q.

64.** Доведіть, що для кожного натурального n числа n і $2n$ мають однакову кількість зображень у вигляді суми двох квадратів.

65. У кільці $\mathbb{Z}\big[(1+\sqrt{-23})/2\big]$ розкладіть число 27 у добуток а) трьох; b) двох нерозкладних множників.

66.* Припустимо, що елемент a кільця K розкладається в добуток нерозкладних елементів, і позначимо через m_a довжину найкоротшого такого розкладу, а через M_a — довжину найдовшого такого розкладу. Доведіть, що для кожного дійсного числа r існують такі область цілісності K та елемент $a \in K$, що $M_a/m_a > r$.

67.** Нехай m_a і M_a ті ж самі, що і в задачі 66. Доведіть, що існує область цілісності K, для якої множина чисел M_a/m_a не є обмеженою згори.

68. Доведіть, що полем часток $P((x))$ кільця $P[[x]]$ формальних степеневих рядів із коефіцієнтами з поля P є поле *рядів Лорана*, тобто формальних рядів вигляду $\sum_{n\in\mathbb{Z}} a_n x^n$, які містять лише скінченну кількість ненульових доданків із від'ємними показниками.

69. Нехай $p = 2k + 1$ — просте число. Доведіть, що $(k!)^2 + (-1)^k \equiv 0 \pmod{p}$.

Домашнє завдання

70. Доведіть, що елемент, асоційований з простим, сам є простим.

71. З'ясуйте, чи є нерозкладним елементом кільця $\mathbb{Z}[\sqrt{-5}]$ число а) $3 + 2i\sqrt{5}$; b) $4 + 3i\sqrt{5}$; c) 61.

72. Знайдіть у кільці $\mathbb{Z}[\sqrt{-3}]$ для числа $4 + 5\sqrt{3}i$ усі (з точністю до асоційованості) власні дільники і всі (з точністю до асоційованості і порядку множників) розклади в добуток нерозкладних елементів.

73. Доведіть, що кільце $\mathbb{Z}[\sqrt{-6}]$ не є факторіальним.

74. Доведіть, що коли P — поле, то кільця $P[x]$ і $P[x, y]$ не ізоморфні.

75. Розв'яжіть конґруенцію $13x \equiv 37 \pmod{41}$.

76. Користуючись алгоритмом Евкліда, обчисліть у кільці $\mathbb{Z}_n$ елемент, обернений до a, якщо а) $n = 521$, $a = 389$; b) $n = 2011$, $a = 2007$.

77. Користуючись алгоритмом Евкліда, обчисліть у факторкільці $\mathbb{Z}_2[x]/I$ елемент, обернений до $g + I$, якщо
a) $I = (x^4 + x + 1)$, $g = x^3 + x$;
b) $I = (x^5 + x^2 + 1)$, $g = x^4 + x^2 + 1$.

78. Знайдіть у кільці $\mathbb{Z}[i]$ НСД елементів a і b, якщо: a) $a = 18 + 4i$, $b = 23 + i$; b) $a = 85$, $b = 1 + 13i$; c) $a = 23 - 7i$, $b = 18 - 4i$.

79. Знайдіть у кільці $\mathbb{Z}[i]$ усі власні дільники (з точністю до асоційованості) числа a) 5; b) 7; c) 10; d) 21.

Заняття 4. Теоретико-числові застосування

Необхідні поняття. Ціле число a називається *квадратичним лишком* за модулем натурального числа n, якщо воно взаємно просте з n і існує таке число x, що $x^2 \equiv a \pmod{n}$ (тобто a є квадратом у мультиплікативній групі $\mathbb{Z}_n^*$). Якщо a взаємно просте з n, але конгруенція $x^2 \equiv a \pmod{n}$ розв'язків не має, то a називається *квадратичним нелишком* за модулем n.

Для довільних непарного простого числа p і цілого числа a *символ Лежандра* $\left(\frac{a}{p}\right)$ дорівнює 1, якщо a є квадратичним лишком за модулем p, -1, якщо a є квадратичним нелишком за модулем p, і 0, якщо a ділиться на p.

Необхідні твердження. **1. Китайська теорема про лишки** для кільця $\mathbb{Z}$. Якщо $m_1, m_2, \ldots, m_n$ — попарно взаємно прості числа, то для довільного набору $a_1, a_2, \ldots, a_n$ цілих чисел система

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \cdots\cdots\cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

має розв'язок.

2. Якщо $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ — канонічний розклад числа n, то $\mathbb{Z}_n^* = \mathbb{Z}^*_{p_1^{k_1}} \oplus \mathbb{Z}^*_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}^*_{p_m^{k_m}}$.

3. a) Для довільних непарного простого числа p і натурального числа k група $\mathbb{Z}^*_{p^k}$ є циклічною.

b) Для довільного $k > 2$ $\mathbb{Z}^*_{2^k} \simeq C_2 \times C_{2^{k-2}}$.

4. Якщо p — непарне просте число, то рівно половина елементів із $\mathbb{Z}^*_{p^k}$ є квадратичними лишками за модулем p^k.

5. Критерій Ойлера. Якщо p — непарне просте число, то

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

6. Властивості символу Лежандра.

a) Якщо $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

b) мультиплікативність: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

c) якщо $p \nmid b$, то $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

7. Число -1 є квадратичним лишком за модулем простого числа p тоді й лише тоді, коли $p \equiv 1 \pmod 4$.

8. Квадратичний закон взаємності.

a) Якщо p і q — різні непарні прості числа, то

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4};$$

b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Приклади розв'язання типових задач

Задача 1. *Розв'яжіть систему лінійних конгруенцій:*

$$a)\quad \begin{cases} x \equiv 13 \pmod{21}, \\ x \equiv 7 \pmod{22}, \\ x \equiv 9 \pmod{23}. \end{cases} \qquad b)\quad \begin{cases} 15x \equiv 24 \pmod{51}, \\ 28x \equiv 24 \pmod{72}, \\ 30x \equiv 24 \pmod{46}. \end{cases}$$

Розв'язання. Спочатку розв'яжемо три допоміжні системи:

$$\begin{cases} x \equiv 1 \pmod{21}, \\ x \equiv 0 \pmod{22}, \\ x \equiv 0 \pmod{23}, \end{cases} \quad \begin{cases} x \equiv 0 \pmod{21}, \\ x \equiv 1 \pmod{22}, \\ x \equiv 0 \pmod{23}, \end{cases} \quad \begin{cases} x \equiv 0 \pmod{21}, \\ x \equiv 0 \pmod{22}, \\ x \equiv 1 \pmod{23}. \end{cases} \tag{15}$$

Зауважимо, що коли m і n взаємно прості, то система з двох конґруенцій $x \equiv 0 \pmod m$, $x \equiv 0 \pmod n$ рівносильна конґруенції $x \equiv 0 \pmod{mn}$. Тому від конґруенцій (15) можна перейти до конґруенцій

$$\begin{cases} x \equiv 1 \pmod{21}, \\ x \equiv 0 \pmod{506}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{22}, \\ x \equiv 0 \pmod{483}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{23}, \\ x \equiv 0 \pmod{462}. \end{cases} \tag{16}$$

Якщо m і n взаємно прості, то існують такі a і b, що $am + bn = 1$. Із цієї рівності випливає, що число am є розв'язком системи конґруенцій $x \equiv 0 \pmod m$, $x \equiv 1 \pmod n$. Зображення $am + bn = 1$ можна знайти за допомогою алгоритму Евкліда.

Щоб розв'язати першу із систем (16), спочатку шукаємо за допомогою алгоритму Евкліда НСД чисел 506 і 21:

$$506 = 24 \cdot 21 + 2;$$
$$21 = 10 \cdot 2 + 1.$$

Звідси отримуємо:

$$1 = 21 - 10 \cdot 2 = 21 - 10 \cdot (506 - 24 \cdot 21) = 241 \cdot 21 - 10 \cdot 506.$$

Отже, число $a_1 = -10 \cdot 506 = -5060$ буде розв'язком першої із систем (16)

Аналогічно для другої із систем (16) знаходимо зображення $1 = 22 \cdot 22 - 1 \cdot 483$ і розв'язок $a_2 = -483$.

Так само для третьої із систем (16) знаходимо зображення $1 = 221 \cdot 23 - 11 \cdot 462$ і розв'язок $a_3 = -11 \cdot 462 = -5082$.

Отримані розв'язки систем (16) будуть і розв'язками рівносильних їм систем (15). Тому розв'язком початкової системи буде

$$x \equiv 13a_1 + 7a_2 + 9a_3 = 13 \cdot (-5060) + 7 \cdot (-483) + 9 \cdot (-5082) = \\ = -114899 \pmod{21 \cdot 22 \cdot 23}.$$

$21 \cdot 22 \cdot 23 = 10626$. Крім того, представником класу лишків зазвичай вибирають найменший додатний лишок із цього класі. Позаяк $-114899 \equiv \equiv 1987 \pmod{10626}$, то остаточно відповідь можна записати у вигляді $x \equiv 1987 \pmod{10626}$.

b) Зауважимо, що $\text{НСД}(15, 24, 51) = 3$, $\text{НСД}(28, 24, 72) = 4$, $\text{НСД}(30, 24, 36) = 2$. Тому першу конґруенцію системи можна розділити на 3, другу — на 4 і третю — на 2. У результаті отримаємо систему конґруенцій

$$\begin{cases} 5x \equiv 8 \pmod{17}, \\ 7x \equiv 6 \pmod{18}, \\ 15x \equiv 12 \pmod{23}, \end{cases} \tag{17}$$

яка рівносильна початковій. Крім того, за модулем 17 $5^{-1} = 7$, за модулем 18 $7^{-1} = 13$, і за модулем 23 $15^{-1} = 20$. Помноживши конґруенції системи (17) відповідно на 7, 13 і 20, отримаємо систему

$$\begin{cases} x \equiv 7 \cdot 8 \equiv 5 \pmod{17}, \\ x \equiv 13 \cdot 6 \equiv 6 \pmod{18}, \\ x \equiv 20 \cdot 12 \equiv 10 \pmod{23}. \end{cases} \tag{18}$$

Числа 17, 18 і 23 — попарно взаємно прості. Тому систему (18) можна розв'язувати аналогічно системі із попереднього пункту. Для цього будуємо набір допоміжних систем

$$\begin{cases} x \equiv 1 \pmod{17}, \\ x \equiv 0 \pmod{414}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{18}, \\ x \equiv 0 \pmod{391}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{23}, \\ x \equiv 0 \pmod{306}. \end{cases} \tag{19}$$

Далі з рівностей

$$1 = 3 \cdot 414 - 73 \cdot 17 = 7 \cdot 391 - 152 \cdot 18 = 10 \cdot 306 - 133 \cdot 23$$

знаходимо відповідні розв'язки цих систем: $a_1 = 3 \cdot 414 = 1242$, $a_2 = 7 \cdot 391 = 2737$, $a_3 = 10 \cdot 306 = 3060$. Враховуючи, що $17 \cdot 18 \cdot 23 = 7038$, розв'язком початкової системи буде

$$x \equiv 5a_1 + 6a_2 + 10a_3 = 5 \cdot 1242 + 6 \cdot 2737 + 10 \cdot 3060 = \\ = 53232 \equiv 3966 \pmod{7038}. \qquad \square$$

Задача 2. *Для яких значень параметра a система конгруенцій*

$$\begin{cases} x \equiv 7 \pmod{18}, \\ x \equiv 16 \pmod{27}, \\ x \equiv 3 \pmod{40}, \\ x \equiv a \pmod{60} \end{cases}$$

буде сумісною?

Розв'язання. Перейдемо до модулів, які є степенями простих чисел. Конґруенція $x \equiv 7 \pmod{18}$ рівносильна системі конгруенцій $x \equiv 1 \pmod 2$ і $x \equiv 7 \pmod 9$, а конгруенція $x \equiv 3 \pmod{40}$ — системі конгруенцій $x \equiv 3 \pmod 5$ і $x \equiv 3 \pmod 8$. Конґруенція $x \equiv 1 \pmod 2$ є наслідком конгруенції $x \equiv 3 \pmod 8$, а конгруенція $x \equiv 7 \pmod 9$ — наслідком конгруенції $x \equiv 16 \pmod{27}$. Тому конгруенції $x \equiv 1 \pmod 2$ і $x \equiv 7 \pmod 9$ можна опустити. Таким чином, система

$$\begin{cases} x \equiv 7 \pmod{18}, \\ x \equiv 16 \pmod{27}, \\ x \equiv 3 \pmod{40} \end{cases}$$

рівносильна системі

$$\begin{cases} x \equiv 3 \pmod 8, \\ x \equiv 16 \pmod{27}, \\ x \equiv 3 \pmod 5. \end{cases}$$

З іншого боку, конгруенція $x \equiv a \pmod{60}$ рівносильна системі трьох конгруенцій $x \equiv a \pmod 4$, $x \equiv a \pmod 3$ і $x \equiv a \pmod 5$. Але з того, що $x \equiv 3 \pmod 8$, випливає, що $x \equiv 3 \pmod 4$, а з $x \equiv 16 \pmod{27}$ випливає, що $x \equiv 3 \pmod 4$. Крім того маємо ще конгруенцію $x \equiv 3 \pmod 5$.

Тому для a отримуємо систему

$$\begin{cases} a \equiv 3 \pmod 4, \\ a \equiv 1 \pmod 3, \\ a \equiv 3 \pmod 5. \end{cases}$$

Її можна розв'язувати методом задачі 1. Але, враховуючи маленькі модулі, розв'язок легко знаходиться простим перебором: $a \equiv 43 \pmod{60}$. □

Задача 3. *Знайдіть усі трійки (p, q, r) простих чисел, для яких $p^2 + q^2 + r^2 = pqr$.*

Розв'язання. При розв'язанні рівнянь у цілих числах часто бувають корисними міркування за модулем певного числа. Дане рівняння зручно розглядати за модулем 3.

За модулем 3 квадрат може дорівнювати 0 або 1. Якщо всі квадрати p^2, q^2, r^2 ненульові, то

$$pqr \equiv p^2 + q^2 + r^2 \equiv 1 + 1 + 1 \equiv 0 \pmod 3.$$

Але тоді в добуткові pqr принаймні один із множників дорівнює 0, що суперечить припущенню.

Отже, за модулем 3 принаймні один із квадратів p^2, q^2, r^2 дорівнює 0. Припустимо, що $p^2 \equiv 0 \pmod 3$. Тоді $p \equiv 0 \pmod 3$ і $q^2 + r^2 \equiv 0 \pmod 3$. Кожен із двох доданків у лівій частині дорівнює 0 або 1, тому конгруенція виконується лише у випадку $q^2 \equiv r^2 \equiv 0 \pmod 3$, тобто коли $q \equiv r \equiv 0 \pmod 3$.

Таким чином, конгруенція $p^2 + q^2 + r^2 \equiv pqr \pmod 3$ виконується тоді й лише тоді, коли $\equiv q \equiv r \equiv 0 \pmod 3$. Єдиним простим число, яке конгруентне 0 за модулем 3, є 3. Отже, єдиною трійкою, що задовольняє умову задачі, може бути лише $(3, 3, 3)$. Очевидно, що ця трійка задовольняє умову. □

Задача 4. *Доведіть, що коли p — просте число вигляду $4k + 1$, то сума s усіх квадратичних лишків за модулем p дорівнює $\dfrac{p(p-1)}{4}$.*

Розв'язання. p є числом вигляду $4k + 1$, тому $\left(\dfrac{-1}{p}\right) = 1$. Але тоді

$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right).$$

Отже, або обидва числа a і $p-a$ є квадратичними лишками, або обидва є нелишками (зауважимо, що одне з цих чисел є парним, а друге — непарним). Всього маємо $\dfrac{p-1}{2}$ квадратичних лишків, які розбиваються на $\dfrac{p-1}{4}$ пар вигляду $(a, p-a)$. Сума чисел кожної пари дорівнює p, тому $s = p \cdot \dfrac{p-1}{4} = \dfrac{p(p-1)}{4}$. □

Задача 5. *Доведіть, що коли p — просте число вигляду $4k+3$, а число $q = 2p+1$ — також просте, то $2^p \equiv 1 \pmod q$.*

Розв'язання. $q = 8k+7$, тому за квадратичним законом взаємності

$$\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8} = (-1)^{(64k^2+112k+48)/8} = (-1)^{2(4k^2+7k+3)} = 1.$$

Але за критерієм Ойлера $\left(\dfrac{2}{q}\right) \equiv 2^{(q-1)/2} = 2^p \pmod q$. □

Задача 6. *Обчисліть* $\left(\dfrac{1039}{2039}\right)$.

Розв'язання. Використовуючи квадратичний закон взаємності, маємо:

$$\left(\frac{1039}{2039}\right) = (-1)^{(1039-1)(2039-1)/4}\left(\frac{2039}{1039}\right) = -\left(\frac{1000}{1039}\right) =$$
$$= -\left(\frac{2^3 \cdot 5^3}{1039}\right) = -\left(\frac{2}{1039}\right)^3\left(\frac{5}{1039}\right)^3.$$

Але

$$\left(\frac{2}{1039}\right) = (-1)^{(1039^2-1)/8} = (-1)^{(1040\cdot 1038)/8} = 1,$$
$$\left(\frac{5}{1039}\right) = (-1)^{(1039-1)(5-1)/4}\left(\frac{1039}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Тому $\left(\dfrac{1039}{2039}\right) = -1$. □

Задача 7. *Знайдіть усі непарні прості числа p, за модулем яких число 3 є квадратичним лишком.*

Розв'язання. За квадратичним законом взаємності

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2},$$

тому $\left(\frac{3}{p}\right) = 1$ тоді й лише тоді, коли або $\left(\frac{p}{3}\right) = 1$ і $(-1)^{(p-1)/2} = 1$, або $\left(\frac{p}{3}\right) = -1$ і $(-1)^{(p-1)/2} = -1$.

У першому випадку $p \equiv 1 \pmod 3$ і $p - 1 \equiv 0 \pmod 4$, звідки $p \equiv 1 \pmod{12}$.

У другому випадку $p \equiv 2 \pmod 3$ і $p - 1 \equiv 2 \pmod 4$, звідки $p \equiv 11 \equiv -1 \pmod{12}$.

Таким чином, число 3 є квадратичним лишком за модулем простого числа p тоді й лише тоді, коли $p \equiv \pm 1 \pmod{12}$. □

Задача 8. *Доведіть, що число* 128 *є квадратичним нелишком за модулем кожного простого числа* p *вигляду* $p = 8k \pm 5$.

Розв'язання. За квадратичним законом взаємності

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(64k^2 \pm 80k + 25 - 1)/8} = (-1)^{8k^2 \pm 10k + 3}.$$

Позаяк число $8k^2 \pm 10k + 3$ — непарне, то $\left(\frac{2}{p}\right) = -1$. Тому

$$\left(\frac{128}{p}\right) = \left(\frac{2}{p}\right)^7 = (-1)^7 = -1.$$ □

Задача 9. *З'ясуйте, для яких цілих чисел* n *число* *а)* $59n + 32$; *б)* $79n + 2$ *буде квадратом цілого числа.*

Розв'язання. Зауважимо, що коли $an + b = k^2$, то b є квадратичним лишком за модулем a.

а) З'ясуємо, чи є 32 квадратичним лишком за модулем 59:

$$\left(\frac{32}{59}\right) = \left(\frac{2}{59}\right)^5 = \left((-1)^{(59^2-1)/8}\right)^5 = (-1)^5 = -1.$$

Отже, 32 не є квадратичним лишком за модулем 59, а тому для жодного n число $59n + 32$ не буде квадратом цілого числа.

b) З'ясуємо, чи є 2 квадратичним лишком за модулем 79:

$$\left(\frac{2}{79}\right) = (-1)^{(79^2-1)/8} = (-1)^{780} = 1.$$

Отже, необхідна умова існування цілих чисел n, для яких число $79n+2$ буде квадратом, виконується. Розглянемо тепер діофантове рівняння

$$79n + 2 = m^2 \tag{20}$$

і покладемо $m = 79k + a$. Із рівності (20) отримуємо:

$$79n + 2 = 79^2k^2 + 2 \cdot 79ak + a^2, \tag{21}$$

звідки $a^2 - 2 \equiv 0 \pmod{79}$. Позаяк $2 \equiv 81 = 9^2 \pmod{79}$, то $a = \pm 9$ і рівняння (21) набуває вигляду

$$79n + 2 = 79^2k^2 \pm 18 \cdot 79k + 81,$$

звідки $n = 79k^2 \pm 18k + 1$. □

Основні задачі

10. Розв'яжіть систему лінійних конгруенцій:

$$a)\begin{cases} x \equiv 3 \pmod{13}, \\ x \equiv 5 \pmod{27}, \\ x \equiv 2 \pmod{20}; \end{cases} \qquad b)\begin{cases} x \equiv 3 \pmod{23}, \\ x \equiv 7 \pmod{11}, \\ x \equiv 1 \pmod{20}; \end{cases}$$

$$c)\begin{cases} x \equiv 2 \pmod{14}, \\ x \equiv 5 \pmod{15}, \\ x \equiv 1 \pmod{19}. \end{cases}$$

11. Розв'яжіть систему лінійних конгруенцій:

$$a)\begin{cases} 20x \equiv 12 \pmod{56}, \\ 20x \equiv 34 \pmod{54}, \\ 24x \equiv 21 \pmod{57}; \end{cases} \qquad b)\begin{cases} 21x \equiv 15 \pmod{45}, \\ 27x \equiv 33 \pmod{48}, \\ 22x \equiv 18 \pmod{46}; \end{cases}$$

12. Знайдіть найменше натуральне число, яке при діленні на m, n і k дає відповідно остачі a, b і c:
a) $m = 12$, $n = 13$, $k = 14$, $a = 5$, $b = 6$, $c = 7$;
b) $m = 10$, $n = 12$, $k = 15$, $a = 9$, $b = 5$, $c = 14$;
c) $m = 14$, $n = 16$, $k = 20$, $a = 10$, $b = 6$, $c = 2$;
d) $m = 15$, $n = 16$, $k = 18$, $a = 13$, $b = 5$, $c = 7$.

13. Для яких значень параметра a система конгруенцій

$$a)\begin{cases} x \equiv 11 \pmod{24}, \\ x \equiv 7 \pmod{10}, \\ x \equiv 5 \pmod{22}, \\ x \equiv a \pmod{30}; \end{cases} \qquad b)\begin{cases} x \equiv 10 \pmod{35}, \\ x \equiv 8 \pmod{18}, \\ x \equiv 6 \pmod{20}, \\ x \equiv a \pmod{42}; \end{cases}$$

$$c)\begin{cases} x \equiv 5 \pmod{28}, \\ x \equiv 17 \pmod{20}, \\ x \equiv 7 \pmod{30}, \\ x \equiv a \pmod{70}; \end{cases}$$

буде сумісною?

14. Обчисліть
a) $n \bmod 60$, якщо $n \bmod 20 = 7$ і $n \bmod 42 = 19$;
b) $n \bmod 70$, якщо $n \bmod 30 = 13$ і $n \bmod 84 = 25$;
c) $n \bmod 105$, якщо $n \bmod 45 = 17$ і $n \bmod 70 = 32$;
d) $n \bmod 84$, якщо $n \bmod 60 = 27$ і $n \bmod 70 = 37$.

15. Вкажіть найбільший можливий порядок елемента в мультиплікативній групі a) $\mathbb{Z}^*_{210}$; b) $\mathbb{Z}^*_{252}$; c) $\mathbb{Z}^*_{280}$; d) $\mathbb{Z}^*_{200}$.

16. Знайдіть усі ідемпотенти в кільці $\mathbb{Z}_{p^k}$, де p — просте число.

17. Доведіть, що коли натуральне число n має точно m різних простих дільників, то кільце $\mathbb{Z}_n$ має точно 2^m різних ідемпотентів.

18. Знайдіть усі цілі розв'язки рівняння $x^2 + y^2 = 3z^2$.

19. Доведіть, що жодне число $m \equiv 7 \pmod 8$ не можна подати у вигляді суми трьох квадратів.

20. Складіть список усіх квадратичних лишків і список усіх нелишків за модулем простого числа p:
a) $p = 5$; b) $p = 7$; c) $p = 11$; d) $p = 13$.

21. Чи може квадратичний лишок за модулем простого числа p бути твірним елементом групи $\mathbb{Z}^*_p$?

22. Доведіть, що для довільних цілого числа a і непарного простого числа p кількість розв'язків конґруенції $x^2 \equiv a \pmod p$ дорівнює $1 + \left(\dfrac{a}{p}\right)$.

23. Нехай p — непарне просте число. Доведіть, що
a) добуток P_1 усіх квадратичних лишків за модулем p задовольняє конґруенцію $P_1 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$;
b) добуток P_2 усіх квадратичних нелишків за модулем p задовольняє конґруенцію $P_1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.

24. Доведіть, що -1 буде квадратичним лишком за модулем простого числа $p > 2$ тоді й лише тоді, коли $p \equiv 1 \pmod{4}$.

25. Доведіть, що коли p — просте число вигляду $4k + 3$, то рівно одне з чисел a і $-a$ є квадратичним лишком за модулем p.

26. Обчисліть: a) $\left(\frac{137}{1039}\right)$; b) $\left(\frac{2023}{1231}\right)$; c) $\left(\frac{853}{1409}\right)$; d) $\left(\frac{5381}{6277}\right)$.

27. Знайдіть усі непарні прості числа p, за модулем яких число 5 є квадратичним лишком.

28. Доведіть, що число a є квадратичним лишком за модулем простого числа p: a) $a = 8$, $p = 8k + 7$; b) $a = 27$, $p = 12k \pm 1$.

29. Доведіть, що число a є квадратичним нелишком за модулем простого числа p: a) $a = 32$, $p = 8k \pm 3$; b) $a = 243$, $p = 12k \pm 5$.

30. З'ясуйте, чи має конґруенція розв'язки, і якщо має, то знайдіть їх: a) $x^2 \equiv 11 \pmod{23}$; b) $x^2 \equiv 12 \pmod{23}$; c) $x^2 \equiv 13 \pmod{23}$.

31. З'ясуйте, для яких цілих чисел n число a) $19n + 12$; b) $41n + 36$; c) $67n + 42$; d) $53n + 11$ буде квадратом цілого числа.

32. Розв'яжіть конгруенцію
a) $x^2 - 8x + 6 \equiv 0 \pmod{13}$; b) $3x^2 + 7x + 9 \equiv 0 \pmod{19}$;
c) $3x^2 + 7x + 9 \equiv 0 \pmod{35}$; d) $5x^2 - 4x - 1 \equiv 0 \pmod{143}$.

Додаткові задачі

33. Нехай $\varphi(n)$ — функція Ойлера. За допомогою китайської теореми про остачі доведіть, що для взаємно простих чисел m і n виконується рівність $\varphi(mn) = \varphi(m)\varphi(n)$.

34. Нехай $I_1, \ldots, I_n$ — ідеали кільця K з одиницею. Доведіть, що відображення

$$\varphi : K \to \prod_{k=1}^{n} K/I_k, \quad x \mapsto (x + I_1, \ldots, x + I_n),$$

буде сюр'єктивним тоді й лише тоді, коли $I_k + I_j = K$ для довільних $k \neq j$.

35. Доведіть, що для кожного набору $a_1, \ldots, a_n$ невід'ємних цілих чисел знайдеться таке натуральне число b, що система конгруенцій

$$\begin{aligned} x &\equiv a_1 \pmod{b+1} \\ x &\equiv a_2 \pmod{2b+1} \\ &\ldots\ldots\ldots\ldots\ldots \\ x &\equiv a_n \pmod{nb+1} \end{aligned}$$

має розв'язок.

36. Доведіть, що діофантове рівняння

$$a)\ x^2 - 15y^2 = z^2; \qquad b)\ x^2 - yz = 9z^2$$

має нескінченно багато розв'язків.

37.* Знайдіть усі цілі розв'язки рівняння $x^3 = y^2 + 2$.

38.** Знайдіть усі цілі розв'язки рівняння $x^5 - y^2 = 1$.

39. Доведіть, що коли жодне з чисел a, b, c не ділиться на просте число p, то конґруенція $ax^2 + by^2 \equiv c \pmod{p}$ має розв'язок.

40. Нехай p — непарне просте число, $f(x) = ax^2 + bx + c$, $a \not\equiv 0 \pmod{p}$, $d = b^2 - 4ac$.

a) Обчисліть $\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right)$, якщо $d \equiv 0 \pmod{p}$.

b) Доведіть, що коли $d \not\equiv 0 \pmod{p}$, то $\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right) = -\left(\frac{a}{p}\right)$.

41. Доведіть, що коли p — просте число вигляду $4k+1$, а число $q = 2p+1$ — також просте, то 2 є твірним елементом групи $\mathbb{Z}_q^*$.

42. Нехай числа p і q задовольняють умови зад. 41. Для яких простих чисел q число 5 буде твірним елементом групи $\mathbb{Z}_q^*$?

43. Нехай p — просте число вигляду $2^{2^k}+1$. Доведіть, що кожен квадратичний нелишок за модулем p є твірним елементом мультиплікативної групи $\mathbb{Z}_p^*$.

44. Доведіть, що число $2^{251}-1$ не є простим.

45. Нехай p — просте число вигляду 2^q-1, де $q>2$ — просте. Доведіть, що 3 є квадратичним нелишком за модулем p.

46. Доведіть, що коли p — просте число вигляду $4k+1$, то розв'язок конгруенції $x^2\equiv -1 \pmod p$ має вигляд $x=\pm(2k)!$.

47. Доведіть, що коли a є квадратичним лишком за модулем простого числа $p=4k+3$, то розв'язок конгруенції $x^2\equiv a \pmod p$ має вигляд $x\equiv \pm a^{k+1} \pmod p$.

48.* Доведіть, що коли a є квадратичним лишком за модулем простого числа $p=8k+5$, то розв'язок конгруенції $x^2\equiv a \pmod p$ має вигляд або $x\equiv \pm a^{k+1} \pmod p$, або $x\equiv \pm a^{k+1}\cdot 2^{2k+1} \pmod p$.

49. Нехай p — непарне просте число.

а) Доведіть, що коли $n=p^k$ або $n=2p^k$, то розв'язками конґруенції $x^2\equiv 1 \pmod n$ будуть лише $x\equiv \pm 1 \pmod n$.

b) Доведіть, що коли $n>5$ і не задовольняє умову п. а), то конґруенція $x^2\equiv 1 \pmod n$ має більше двох розв'язків.

50. Нехай $n=p_1^{k_1}\cdots p_m^{k_m}$ $(k_1,\ldots,k_m\geq 1)$ — непарне число. Доведіть, що конґруенція $x^2\equiv 1 \pmod n$ має 2^m розв'язків.

51. Доведіть, що кожний простий дільник числа Ферма $F_n=2^{2^n}+1$ має вигляд $p=2^{n+1}\cdot k+1$.

Домашнє завдання

52. Розв'яжіть систему лінійних конгруенцій:

а) $\begin{cases} x\equiv 7 \pmod{15},\\ x\equiv 4 \pmod{32},\\ x\equiv 19 \pmod{23}; \end{cases}$ b) $\begin{cases} x\equiv 13 \pmod{16},\\ x\equiv 2 \pmod{25},\\ x\equiv 11 \pmod{27}; \end{cases}$

53. Розв'яжіть систему лінійних конгруенцій:

а) $\begin{cases} 20x\equiv 32 \pmod{52},\\ 15x\equiv 27 \pmod{54},\\ 16x\equiv 14 \pmod{50}; \end{cases}$ b) $\begin{cases} 24x\equiv 8 \pmod{68},\\ 21x\equiv 33 \pmod{60},\\ 16x\equiv 42 \pmod{66}. \end{cases}$

54. Для яких значень параметра a система конгруенцій

$$\begin{cases} x\equiv 5 \pmod 6,\\ x\equiv 8 \pmod{15},\\ x\equiv a \pmod{10}; \end{cases}$$

буде сумісною?

55. Знайдіть усі прості числа x і y, для яких $7x^2 - 2y^2 = 13$.

56. Доведіть, що коли $n = k^2+1$, то числа a і $-a$ будуть квадратичними лишками/нелишками за модулем n одночасно.

57. Обчисліть: a) $\left(\frac{438}{593}\right)$; b) $\left(\frac{787}{1787}\right)$.

58. Знайдіть усі непарні прості числа p, за модулем яких число -3 є квадратичним лишком.

59. З'ясуйте, чи має конґруенція розв'язки, і якщо має, то знайдіть їх: a) $x^2 \equiv 2 \pmod{31}$; b) $x^2 \equiv 3 \pmod{31}$.

Заняття 5. Поля та їх розширення

Необхідні поняття. Поле P, яке не містить власних підполів, називається *простим*.

Якщо одиниця як елемент адитивної групи поля P має скінчений порядок, то цей порядок (тобто найменше натуральне n, для якого виконується рівність $\underbrace{1+1+\cdots+1}_{n} = 0$) називається *характеристикою* поля P і позначається $\mathrm{char}(P)$. Якщо ж такого n не існує, то кажуть, що характеристика поля P дорівнює 0.

Якщо $F \supseteq P$, то поле F можна розглядати як векторний простір над полем P. Розмірність цього векторного простору називається *степенем розширення* $F \supseteq P$ і позначається $[F : P]$. Розширення $F \supseteq P$ називається *скінченним*, якщо степінь розширення $[F : P]$ є скінченним, і *нескінченним* у противному разі.

Розширення $F \supseteq P$ називається *простим*, якщо існує такий елемент $a \in F$, що $F = P(a)$. Кажуть також, що поле F одержане *приєднанням елемента* a до поля P.

Аналогічно визначається *приєднання* $P(A)$ до поля P довільної множини елементів A.

Нехай $F \supseteq P$. Елемент $a \in F$ називається *алгебричним* елементом розширення $F \supseteq P$ (або *алгебричним* над полем P), якщо a є коренем деякого ненульового многочлена $f(x) \in P[x]$. Многочлен $f(x)$ називається *анулюючим* для елемента a.

У противному разі a називається *трансцендентним* елементом.

Просте розширення $P(a) \supseteq P$ називається алгебричним або трансцендентним у залежності від того, яким є елемент a — алгебричним чи трансцендентним.

Мінімальним многочленом $\min_a(x)$ алгебричного елемента a називається нормований анулюючий многочлен найменшого можливого степеня. Степінь мінімального многочлена $\min_a(x)$ називається також *степенем* алгебричного елемента a.

Необхідні твердження. **1.** Якщо $\varphi : P_1 \to P_2$ — ізоморфізм полів, то $\varphi(0) = 0$; $\varphi(1) = 1$; $\varphi(-a) = -\varphi(a)$; $\varphi(a^{-1}) = \big(\varphi(a)\big)^{-1}$.

2. Поле $\mathbb{Q}$ і кожне поле $\mathbb{Z}_p$, де p — просте число, є простими. Кожне просте поле ізоморфне або полю $\mathbb{Q}$, або полю $\mathbb{Z}_p$, де p — просте число.

3. Кожне поле містить єдине просте підполе.

4. Якщо просте підполе поля P ізоморфне полю $\mathbb{Z}_p$, то характери-

стика поля P дорівнює p. Якщо просте підполе поля P ізоморфне полю $\mathbb{Q}$, то характеристика поля P дорівнює 0.

5. У вежі $K \supseteq F \supseteq P$ розширень полів розширення $K \supseteq P$ буде скінченним тоді й лише тоді, коли скінченним буде кожне з розширень $K \supseteq F$ і $F \supseteq P$. Якщо всі ці розширення скінченні, то $[K : P] = [K : F] \cdot [F : P]$.

6. Властивості мінімального многочлена:
a) Нормований мінімальний многочлен $\min_a(x)$ елемента a визначений однозначно.
b) $\min_a(x)$ ділить кожний анулюючий многочлен $\min_a(x)$ елемента a.
c) Кожен мінімальний многочлен $\min_a(x)$ є незвідним над полем P.

7. Теорема про будову простого алгебричного розширення: Нехай елемент a поля $F \supseteq P$ є алгебричним степеня n над полем P. Тоді

$$P(a) = \{a_0 + a_1 a + a_2 a^2 + \cdots + a_{n-1} a^{n-1} : a_0, a_1, \ldots, a_{n-1} \in P\}.$$

Зокрема, розширення $P(a) \supseteq P$ є скінченним, степінь розширення дорівнює n, поле $P(a)$ ізоморфне факторкільцю $P[x]/\big(\min_a(x)\big)$, а елементи 1, a, a^2, …, a^{n-1} утворюють базу $P(a)$ як векторного простору над P.

8. Теорема про будову простого трансцендентного розширення. Нехай елемент a поля $F \supseteq P$ є трансцендентним над P. Тоді поле $P(a)$ збігається з полем усіх раціональних дробів від a. Зокрема, розширення $P(a) \supseteq P$ є нескінченним і всі прості трансцендентні розширення поля P ізоморфні між собою.

9. Теорема про символічне приєднання Кронекера. Для кожного многочлена додатного степеня $f(x) \in P[x]$ існує розширення $F \supseteq P$, в якому $f(x)$ має корінь.

Приклади розв'язання типових задач

Задача 1. *З'ясуйте, чи утворює поле множина $\mathbb{R} \times \mathbb{R}$ всіх впорядкованих пар дійсних чисел, якщо додавання і множення визначаються такими правилами*:
a) $(a, b) \oplus (c, d) = (a + c, b + d)$, $(a, b) \odot (c, d) = (ac, bd)$;
b) $(a, b) \oplus (c, d) = (a + c, b + d)$, $(a, b) \odot (c, d) = (ac - bd, ad + bc)$;
c) $(a, b) \oplus (c, d) = (a + c, b + d)$, $(a, b) \odot (c, d) = (ac + 2bd, ad + bc)$.

Розв'язання. В усіх випадках дія $\oplus$ визначається однаково. Із її означення випливає, що множина $\mathbb{R} \times \mathbb{R}$ із дією $\oplus$ є прямою сумою двох

абелевих груп $(\mathbb{R}, +)$, а тому також є абелевою групою. Тому перевірки вимагають лише ті властивості поля, які пов'язані із множенням.

a) Із означення дій $\oplus$ і $\odot$ випливає, що в цьому випадку ми маємо справу із прямим квадратом $\mathbb{R} \oplus \mathbb{R}$ поля $\mathbb{R}$. Але пряма сума двох кілець завжди містить дільники нуля. Справді, $(1,0) \odot (0,1) = (0,0)$. А в полі дільників нуля нема. Отже, в цьому випадку множина $\mathbb{R} \times \mathbb{R}$ поля не утворює.

b) Якщо пару (a, b) дійсних чисел ототожнити з комплексним числом $a + bi$, то множина $\mathbb{R} \times \mathbb{R}$ ототожнюється з множиною $\mathbb{C}$ комплексних чисел, а дії $\oplus$ і $\odot$ — із додаванням і множенням комплексних чисел. Отже, в цьому випадку множина $\mathbb{R} \times \mathbb{R}$ з діями $\oplus$ і $\odot$ ізоморфна полю $\mathbb{C}$, а тому і сама є полем.

c) З'ясуємо, чи є дільники нуля в цьому випадку. Якщо $a \neq 0$ і $c \neq 0$, то рівності $(a, b) \odot (c, d) = (0, 0)$ і $(1, b/a) \odot (1, d/c) = (0, 0)$ рівносильні. А рівність $(1, x) \odot (1, y) = (0, 0)$ рівносильна системі $1 + 2xy = 0$, $x + y = 0$, одним із розв'язків якої є, наприклад, $x = 1/\sqrt{2}$, $y = -1/\sqrt{2}$. Отже, $(1, 1/\sqrt{2}) \odot (1, -1/\sqrt{2}) = (0, 0)$, а тому в цьому випадку множина $\mathbb{R} \times \mathbb{R}$ поля не утворює. □

Задача 2. *Для яких цілих чисел $n \neq 0$ множина матриць*

$$K = \left\{ \begin{pmatrix} a & b \\ nb & a \end{pmatrix} \,\middle|\, a, b \in P \right\}$$

утворює поле, якщо a) $P = \mathbb{Q}$; b) $P = \mathbb{R}$; c) $P = \mathbb{C}$?

Розв'язання. K є підмножиною кільця з одиницею $M_2(P)$. Тому множина K буде полем тоді й лише тоді, коли вона є комутативним підкільцем з одиницею і разом із кожною ненульовою матрицею містить обернену до неї.

Очевидно, що K містить одиничну матрицю. Крім того

$$\begin{pmatrix} a & b \\ nb & a \end{pmatrix} \pm \begin{pmatrix} c & d \\ nd & c \end{pmatrix} = \begin{pmatrix} a \pm c & b \pm d \\ n(b \pm d) & a \pm c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ nb & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ nd & c \end{pmatrix} = \begin{pmatrix} ac + nbd & ad + bc \\ n(ad + bc) & ac + nbd \end{pmatrix} = \begin{pmatrix} c & d \\ nd & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ nb & a \end{pmatrix}.$$

Таким чином, множина K замкнена відносно додавання, віднімання і множення, причому множення є комутативним. Тому K є комутативним кільцем з одиницею. Лишилося з'ясувати, чи для кожної ненульової матриці з K існує обернена.

Обернена існує лише для невиродженої матриці. Якщо матриця

$$A = \begin{pmatrix} a & b \\ nb & a \end{pmatrix}$$

невироджена, тобто якщо $a^2 - nb^2 \neq 0$, то обернена матриця має вигляд

$$A^{-1} = \frac{1}{a^2 - nb^2} \begin{pmatrix} a & -b \\ -nb & a \end{pmatrix}$$

і належить множині K.

Лишилося з'ясувати, для яких n ненульова матриця A бути виродженою. Для ненульової матриці рівність $a^2 - nb^2 = 0$ виконується тоді й лише тоді, коли $n = a^2/b^2$, тобто коли n є квадратом. Якщо a і b беруться з поля $\mathbb{Q}$, то це означає, що n є квадратом натурального числа, якщо з $\mathbb{R}$, то n є додатним, а у випадку поля $\mathbb{C}$ кожне число є квадратом.

Таким чином, у випадку a) множина K утворює поле, якщо n не є квадратом натурального числа; у випадку b) — якщо $n < 0$; а у випадку c) таких n нема. □

Задача 3. *Якою може бути характеристика поля, якщо в ньому виконується рівність* $(1+1+1+1+1)^3 = (1+1+1)^5$?

Розв'язання. Якщо характеристика поля дорівнює p, то рівність $(1+1+1+1+1)^3 = (1+1+1)^5$ рівносильна конґруенції $5^3 \equiv 3^5 \pmod{p}$. $3^5 - 5^3 = 243 - 125 = 118$, тому одержуємо конґруенцію $118 \equiv 0 \pmod{p}$. Простими дільниками числа $118 = 2 \cdot 59$ є лише 2 і 59, тому характеристика поля може дорівнювати лише одному з цих чисел. □

Задача 4. *З'ясуйте, чи будуть ізоморфними поля*
a) $\mathbb{Q}(\sqrt{2})$ *і* $\mathbb{Q}(\sqrt{3})$; *b)* $\mathbb{Q}(\sqrt{3-\sqrt{2}})$ *і* $\mathbb{Q}(\sqrt{3+\sqrt{2}})$.

Розв'язання. a) Припустимо, що ізоморфізм $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$ існує. Оскільки $\varphi(1) = 1$, то $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 2$. Тому при ізоморфізмі φ рівність $(\sqrt{2})^2 = 2$ переходить у рівність $(\varphi(\sqrt{2}))^2 = 2$. Але $\varphi(\sqrt{2})$ має вигляд $\varphi(\sqrt{2}) = a + b\sqrt{3}$, де $a, b \in \mathbb{Q}$. Тому отримуємо рівність

$$(a + b\sqrt{3})^2 = 2,$$

звідки

$$2ab\sqrt{3} = 2 - a^2 - 3b^2.$$

Число $\sqrt{3}$ — ірраціональне, а число $2 - a^2 - 3b^2$ — раціональне. Тому остання рівність можлива лише тоді, коли $ab = 0$. Але якщо $a = 0$, то $b = \sqrt{2/3}$, а якщо $b = 0$, то $a = \sqrt{2}$. В обох випадках приходимо до суперечності з раціональністю чисел a і b. Отже, припущення про існування ізоморфізму $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$ приводить до суперечності, а тому поля $\mathbb{Q}(\sqrt{2})$ і $\mathbb{Q}(\sqrt{3})$ не є ізоморфними.

b) За теоремою про будову простого алгебричного розширення поле $\mathbb{Q}(\sqrt{3-\sqrt{2}})$ ізоморфне факторкільцю $\mathbb{Q}[x]/(f(x))$, де $f(x)$ — мінімальний многочлен числа $\sqrt{3-\sqrt{2}}$. Знайдемо $f(x)$. Із рівності $x = \sqrt{3-\sqrt{2}}$ випливає, що $x^2 = 3 - \sqrt{2}$, звідки $(x^2-3)^2 = 2$ і $x^4 - 6x^2 + 7 = 0$. Отже, многочлен $x^4 - 6x^2 + 7$ є анулюючим для числа $\sqrt{3-\sqrt{2}}$. Безпосередньо застосувати ознаку Айзенштайна для доведення незвідності цього многочлена не можна. Але після заміни $x = y+1$ одержуємо многочлен $y^4 + 4y^3 - 8y + 2$, який буде незвідним за ознакою Айзенштайна для $p = 2$. Тому многочлен $x^4 - 6x^2 + 7$ буде мінімальним для $\sqrt{3-\sqrt{2}}$.

Аналогічно з рівності $x = \sqrt{3+\sqrt{2}}$ також випливає, що $x^4 - 6x^2 + 7 = 0$. Отже, мінімальні многочлени для чисел $\sqrt{3-\sqrt{2}}$ і $\sqrt{3+\sqrt{2}}$ збігаються. А тому поля $\mathbb{Q}(\sqrt{3-\sqrt{2}})$ і $\mathbb{Q}(\sqrt{3+\sqrt{2}})$ будуть ізоморфними. □

Задача 5. *Нехай a — корінь многочлена $x^3 + x^2 - 2x + 1 \in Q[x]$. Знайдіть многочлен з раціональними коефіцієнтами, коренем якого є $a^2 + a - 1$.*

Розв'язання. І спосіб. Нехай $a_1 = a$, a_2, a_3 — корені многочлена $x^3 + x^2 - 2x + 1$. Розглянемо многочлен

$$x^3 + b_1x^2 + b_2x + b_3 = (x - a_1^2 - a_1 + 1)(x - a_2^2 - a_2 + 1)(x - a_3^2 - a_3 + 1),$$

Одним із коренів якого є $a^2 + a - 1$. Коефіцієнти b_1, b_2, b_3 є симетричними

многочленами від a_1, a_2, a_3. За теоремою Вієта вони дорівнюють:

$$b_1 = -(a_1^2 + a_1 - 1) - (a_2^2 + a_2 - 1) - (a_3^2 + a_3 - 1) =$$
$$= -(a_1^2 + a_2^2 + a_3^2) - (a_1 + a_2 + a_3) + 3;$$
$$b_2 = (a_1^2 + a_1 - 1)(a_2^2 + a_2 - 1) +$$
$$+(a_1^2 + a_1 - 1)(a_3^2 + a_3 - 1) + (a_2^2 + a_2 - 1)(a_3^2 + a_3 - 1) =$$
$$= (a_1^2 a_2^2 + a_1^2 a_3^2 + a_2^2 a_3^2) +$$
$$+(a_1^2 a_2 + a_1 a_2^2 + a_1^2 a_3 + a_1 a_3^2 + a_2^2 a_3 + a_2 a_3^2) +$$
$$+(a_1 a_2 + a_1 a_3 + a_2 a_3 - 2a_1^2 - 2a_2^2 - 2a_3^2) -$$
$$-2(a_1 + a_2 + a_3) + 3;$$
$$b_3 = -(a_1^2 + a_1 - 1)(a_2^2 + a_2 - 1)(a_3^2 + a_3 - 1) =$$
$$= -a_1^2 a_2^2 a_3^2 - (a_1^2 a_2^2 a_3 + a_1^2 a_2 a_3^2 + a_1 a_2^2 a_3^2) +$$
$$+(a_1^2 a_2^2 + a_1^2 a_3^2 + a_2^2 a_3^2 - a_1^2 a_2 a_3 - a_1 a_2^2 a_3 - a_1 a_2 a_3^2) -$$
$$+(a_1^2 a_2 + a_1 a_2^2 + a_1^2 a_3 + a_1 a_3^2 + a_2^2 a_3 + a_2 a_3^2 - a_1 a_2 a_3) -$$
$$-(a_1^2 + a_2^2 + a_3^2 - a_1 a_2 - a_1 a_3 - a_2 a_3) -$$
$$-(a_1 + a_2 + a_3) + 1.$$

За основною теоремою про симетричні многочлени кожен симетричний многочлен від a_1, a_2, a_3 є многочленом від елементарних симетричних многочленів $\sigma_1 = a_1 + a_2 + a_3$, $\sigma_2 = a_1 a_2 + a_1 a_3 + a_2 a_3$, $\sigma_3 = a_1 a_2 a_3$. Виражати через елементарні симетричні многочлени зручно кожну однорідну симетричну компоненту окремо. Нагадаємо, як це робиться, на прикладі многочлена

$$f(a_1, a_2, a_3) = a_1^2 a_2^2 + a_1^2 a_3^2 + a_2^2 a_3^2.$$

Враховуючи степені многочленів f та σ_1, σ_2, σ_3, можемо записати з невизначеними коефіцієнтами:

$$f(a_1, a_2, a_3) = A_1 \sigma_1^4 + A_2 \sigma_1^2 \sigma_2 + A_3 \sigma_2^2 + A_4 \sigma_1 \sigma_3. \tag{22}$$

Щоб знайти коефіцієнти A_1, ..., A_4, будемо надавати певних значень змінним a_1, a_2, a_3 і обчислювати значення правої і лівої частин рівності (22) (результати обчислень зручно оформити у вигляді таблиці):

a_1	a_2	a_3	f	σ_1	σ_2	σ_3	права частина
1	0	0	0	1	0	0	A_1
1	1	0	1	2	1	0	$16A_1 + 4A_2 + A_3$
1	-1	0	1	0	-1	0	A_3
1	1	1	3	3	3	1	$81A_1 + 27A_2 + 9A_3 + 3A_4$

Із першого рядка знаходимо $A_1 = 0$, а з третього — $A_3 = 1$. Після цього із позосталих двох рядків отримуємо систему

$$1 = 4A_2 + 1, \quad 3 = 27A_2 + 9 + 3A_4,$$

звідки знаходимо: $A_2 = 0$, $A_4 = -2$. Таким чином,

$$a_1^2a_2^2 + a_1^2a_3^2 + a_2^2a_3^2 = \sigma_2^2 - 2\sigma_1\sigma_3.$$

Аналогічно знаходимо:

$$\begin{gathered} a_1^2 + a_2^2 + a_3^2 = \sigma_1^2 - 2\sigma_2, \\ a_1^2a_2 + a_1a_2^2 + a_1^2a_3 + a_1a_3^2 + a_2^2a_3 + a_2a_3^2 = \sigma_1\sigma_2 - 3\sigma_3, \\ a_1^2a_2^2a_3 + a_1^2a_2a_3^2 + a_1a_2^2a_3^2 = \sigma_2\sigma_3, \\ a_1^2a_2a_3 + a_1a_2^2a_3 + a_1a_2a_3^2 = \sigma_1\sigma_3. \end{gathered}$$

Тому

$$\begin{gathered} b_1 = -\sigma_1^2 + 2\sigma_2 - \sigma_1 + 3, \\ b_2 = \sigma_2^2 - 2\sigma_1\sigma_3 + \sigma_1\sigma_2 - 3\sigma_3 + 5\sigma_2 - 2\sigma_1^2 - 2\sigma_1 + 3; \\ b_3 = -\sigma_3^2 - \sigma_2\sigma_3 + \sigma_2^2 - 3\sigma_1\sigma_3 + \sigma_1\sigma_2 - 4\sigma_3 - \sigma_1^2 + 3\sigma_2 - \sigma_1 + 1. \end{gathered}$$

Але a_1, a_2 і a_3 — це корені многочлена $x^3 + x^2 - 2x + 1$. Тому за теоремою Вієта $\sigma_1 = -1$, $\sigma_2 = -2$, $\sigma_3 = -1$. Підставляючи ці значення у вирази для b_1, b_2, b_3, отримуємо:

$$b_1 = -1, \quad b_2 = 0, \quad b_3 = -1.$$

Отже, число $a^2 + a - 1$ є коренем многочлена $x^3 - x^2 - 1$.

II спосіб. Многочлен $x^3 + x^2 - 2x + 1$ не має раціональних коренів, а тому є незвідним над полем $\mathbb{Q}$. Тому розширення $\mathbb{Q}(a) \supset \mathbb{Q}$ має степінь

3, а числа 1, a і a^2 утворюють базу розширення. Позаяк $a^2+a-1 \in \mathbb{Q}(a)$, то число $b = a^2 + a - 1$ є алгебричним над $\mathbb{Q}$ степеня ≤ 3. Тому для b існує анулюючий многочлен $g(x) \in \mathbb{Q}[x]$ степеня 3. Запишемо його у вигляді

$$g(x) = x^3 + \alpha x^2 + \beta x + \gamma.$$

Із рівності $g(b) = 0$ одержуємо:

$$(a^2 + a - 1)^3 + \alpha(a^2 + a - 1)^2 + \beta(a^2 + a - 1) + \gamma = 0. \qquad (23)$$

Враховуючи, що $a^3 = -a^2 + 2a - 1$, рівність (23) можна спростити:

$$(1 - a) - \alpha a + \beta(a^2 + a - 1) + \gamma = 0,$$

або

$$\beta a^2 + (\beta - \alpha - 1)a + (1 - \beta + \gamma) = 0.$$

Числа a^2, a, 1 утворюють базу розширення $\mathbb{Q}(a) \supset \mathbb{Q}$, тому остання рівність рівносильна такій системі рівнянь:

$$\beta = 0, \quad \beta - \alpha - 1 = 0, \quad 1 - \beta + \gamma = 0.$$

Розв'язуючи цю систему, отримуємо: $\alpha = -1$, $\beta = 0$, $\gamma = -1$. Отже, число $a^2 + a - 1$ є коренем многочлена $x^3 - x^2 - 1$. □

Задача 6. *Нехай* $a = \sqrt{2} + i$, $b = \sqrt{3} - i$.
a) Доведіть, що $\mathbb{Q}(a, b) \neq \mathbb{Q}(a + b)$.
b) Доведіть, що $\mathbb{Q}(a, b) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$.

Розв'язання. a) Число $a + b = \sqrt{2} + \sqrt{3}$ є дійсним, тому $\mathbb{Q}(a + b) \subseteq \mathbb{R}$. А числа a і b не є дійсними, тому $\mathbb{Q}(a, b) \nsubseteq \mathbb{R}$. Звідси випливає, що $\mathbb{Q}(a, b) \neq \mathbb{Q}(a + b)$.

b) Враховуючи попередній пункт і вигляд чисел a і b, маємо таку вежу розширень:

$$\mathbb{Q} \subset \mathbb{Q}(a + b) \subset \mathbb{Q}(a, b) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, i), \qquad (24)$$

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, i) \qquad (25)$$

(те, що включення $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ є строгим, випливає із розв'язання задачі 4.a).

Знайдемо степінь розширення $\mathbb{Q}(a+b) \supset \mathbb{Q}$. Для цього знайдемо мінімальний многочлен числа $a+b=\sqrt{2}+\sqrt{3}$. Маємо такий ланцюжок імплікацій:

$$x=\sqrt{2}+\sqrt{3} \Rightarrow (x-\sqrt{2})^2=3 \Rightarrow x^2-1=2\sqrt{2}x \Rightarrow$$
$$\Rightarrow (x^2-1)^2=8x^2 \Rightarrow x^4-10x^2+1=0.$$

Отже, многочлен x^4-10x^2+1 є анулюючим для числа $\sqrt{2}+\sqrt{3}$. Щоб довести, що він є незвідним над полем $\mathbb{Q}$, знайдемо його розклад на множники над полем $\mathbb{R}$ (корені біквадратного рівняння $x^4-10x^2+1=0$ обчислюються легко):

$$x^4-10x^2+1=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}).$$

Раціональних коренів многочлен x^4-10x^2+1 не має. Якщо він є звідним, то розкладається в добуток двох квадратних многочленів із раціональними коефіцієнтами. Але жоден із добутків

$$(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})=(x-\sqrt{2})^2-3,$$
$$(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}-\sqrt{3})=(x-\sqrt{3})^2-2,$$
$$(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})=x^2-(\sqrt{2}+\sqrt{3})^2$$

не є многочленом із раціональними коефіцієнтами. Тому многочлен x^4-10x^2+1 є незвідним над полем $\mathbb{Q}$ і є мінімальним для числа $\sqrt{2}+\sqrt{3}$. Отже, степінь розширення $\mathbb{Q}(a+b) \supset \mathbb{Q}$ дорівнює 4.

Із вежі розширень (24) маємо:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}] \geq [\mathbb{Q}(a,b):\mathbb{Q}(a+b)]\cdot[\mathbb{Q}(a+b):Q] \geq 2\cdot 4=8,$$

причому рівність $[\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}]=8$ буде мати місце лише тоді, коли $][\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}(a,b)]=1$ і $[\mathbb{Q}(a,b):\mathbb{Q}(a+b)]=2$. А з вежі розширень (24) випливає, що

$$[\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}]=$$
$$=[\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}(\sqrt{2},\sqrt{3})]\cdot[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q})]=$$
$$=2\cdot 2\cdot 2=8.$$

Тому $[\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}(a,b)]=1$ і $\mathbb{Q}(a,b)=\mathbb{Q}(\sqrt{2},\sqrt{3},i)$. □

Задача 7. *Нехай $P(t) \supset P$ — просте трансцендентне розширення. Доведіть, що для кожного елемента $a \in P(t) \setminus P$ підполе $P(a)$ буде ізоморфне полю $P(t)$.*

Розв'язання. Досить показати, що кожен елемент $a \in P(t) \setminus P$ є трансцендентним над P. Кожен елемент $a \in P(t) \setminus P$ можна записати у вигляді відношення $a = \frac{f(t)}{g(t)}$ взаємно простих многочленів $f(t)$ і $g(t)$. Припустимо, що елемент a є алгебричним над P, а $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in P[x]$ — його анулюючий многочлен. Із рівності

$$\alpha_0 + \alpha_1 \frac{f(t)}{g(t)} + \cdots + \alpha_n \left(\frac{f(t)}{g(t)}\right)^n = 0$$

після зведення до спільного знаменника випливає, що

$$\alpha_0 g^n(t) + \alpha_1 g^{n-1}(t) f(t) + \cdots + \alpha_n f^n(t) = 0.$$

У лівій частині всі доданки, крім останнього, діляться на $g(t)$. Тому $f^n(t)$ також ділиться на $g(t)$. Аналогічно доводиться, що $g^n(t)$ ділиться на $f(t)$. Але це суперечить тому, що многочлени $f(t)$ і $g(t)$ — взаємно прості.

Таким чином, припущення, що a є алгебричним над P, приводить до суперечності, а тому a є трансцендентним. □

Задача 8. *Знайдіть степінь і яку–небудь базу наступних розширень поля $\mathbb{Q}$: а) $\mathbb{Q}(\sqrt{2}+i)$; б) $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$.*

Розв'язання. а) Позаяк $(\sqrt{2}+i)^2 = 1 + 2\sqrt{2}i$, то поле $\mathbb{Q}(\sqrt{2}+i)$ містить число $\sqrt{2}i$. А з рівності $\sqrt{2}i \cdot (\sqrt{2}+i) = 2i - \sqrt{2}$ випливає, що поле $\mathbb{Q}(\sqrt{2}+i)$ містить число $2i - \sqrt{2}$. Але тоді $\mathbb{Q}(\sqrt{2}+i)$ містить і числа $i = \frac{1}{3}\big((\sqrt{2}+i) + (2i - \sqrt{2})\big)$ та $\sqrt{2}i$. Тому $\mathbb{Q}(\sqrt{2}+i) \supseteq \mathbb{Q}(\sqrt{2}, i)$. Із другого боку очевидно, що $\mathbb{Q}(\sqrt{2}+i) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Тому $\mathbb{Q}(\sqrt{2}+i) = \mathbb{Q}(\sqrt{2}, i)$. Це дає вежу розширень

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}+i).$$

Мінімальними многочленами для чисел $\sqrt{2}$ та i є, очевидно, многочлени другого степеня $x^2 - 2$ та $x^2 + 1$. Отже, степінь кожного із розширень $\mathbb{Q}(\sqrt{2}, i) \supset \mathbb{Q}(\sqrt{2})$ та $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ дорівнює 2. Тому

$$[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Базою розширення $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ є $1, \sqrt{2}$, а базою розширення $\mathbb{Q}(\sqrt{2}, i) \supset \mathbb{Q}(\sqrt{2})$ є $1, i$. Тому базою розширення $\mathbb{Q}(\sqrt{2}+i) \supset \mathbb{Q}$ буде $1 = 1 \cdot 1$, $\sqrt{2} = \sqrt{2} \cdot 1$, $i = 1 \cdot i$, $\sqrt{2}i = \sqrt{2} \cdot i$.

b) $\sqrt{6} \cdot \sqrt{10} = 2\sqrt{15}$, тому $\sqrt{15} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$ і $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$. Але $\sqrt{10} \notin \mathbb{Q}(\sqrt{6})$. Справді, із рівності $\sqrt{10} = a + b\sqrt{6}$, де $a, b \in \mathbb{Q}$, випливає, що $2ab\sqrt{6} = 10 - a^2 - 6b^2$. У правій частині стоїть раціональне число, а число в лівій частині буде раціональним тоді й лише тоді, коли $ab = 0$, тобто коли $a = 0$ або $b = 0$. Але в першому випадку маємо $10 - 6b^2 = 0$, що суперечить раціональності числа b, а в другому — $10 - a^2 = 0$, що суперечить раціональності a. Це дає вежу розширень

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{6}, \sqrt{10}) = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}).$$

Степінь кожного із розширень $\mathbb{Q}(\sqrt{6}, \sqrt{10}) \supset \mathbb{Q}(\sqrt{6})$ та $\mathbb{Q}(\sqrt{6}) \supset \mathbb{Q}$ дорівнює 2, тому степінь розширення $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) \supset \mathbb{Q}$ дорівнює

$$[\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}] =$$
$$= [\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}(\sqrt{6})] \cdot [\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Базою розширення $\mathbb{Q}(\sqrt{6}) \supset \mathbb{Q}$ є $1, \sqrt{6}$, а базою розширення $\mathbb{Q}(\sqrt{6}, \sqrt{10}) \supset \mathbb{Q}(\sqrt{6})$ є $1, \sqrt{10}$. Тому базою розширення $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) \supset \mathbb{Q}$ буде $1 = 1 \cdot 1$, $\sqrt{6} = \sqrt{6} \cdot 1$, $\sqrt{10} = 1 \cdot \sqrt{10}$, $2\sqrt{15} = \sqrt{6} \cdot \sqrt{10}$. □

Задача 9. *Знайдіть степінь і яку–небудь базу поля розкладу над полем $\mathbb{Q}$ для многочлена а) $x^4 - 2$, б) $x^8 + 1$.*

Розв'язання. а) Нехай F — поле розкладу многочлена $x^4 - 2$. Над полем комплексних чисел маємо розклад

$$x^4 - 2 = (x - \sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2}). \tag{26}$$

Тому маємо таку вежу розширень: $F \supset \mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$. За ознакою Айзенштайна (для $p = 2$) многочлен $x^4 - 2$ є незвідним над полем $\mathbb{Q}$, тому $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Крім того, $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, а $F \nsubseteq \mathbb{R}$. Тому $[F : \mathbb{Q}(\sqrt[4]{2})] \geq 2$. Отже,

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \geq 2 \cdot 4 = 8.$$

Із другого боку, поле $\mathbb{Q}(\sqrt[4]{2}, i)$ містить усі корені многочлена $x^4 - 2$, тому $\mathbb{Q}(\sqrt[4]{2}, i) \supseteq F$ і $[F : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}]$. Із вежі розширень $\mathbb{Q}(\sqrt[4]{2}, i) \supset \mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ випливає, що

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Отже, $[F:\mathbb{Q}]=8$ і $F=\mathbb{Q}(\sqrt[4]{2},i)$.

Базою розширення $\mathbb{Q}(\sqrt[4]{2},i)\supset\mathbb{Q}(\sqrt[4]{2})$ є $1,\ i$, а базою розширення $\mathbb{Q}(\sqrt[4]{2})\supset\mathbb{Q}$ є $1,\ \sqrt[4]{2},\ \sqrt[4]{4},\ \sqrt[4]{8}$. Тому базою поля розкладу $F=\mathbb{Q}(\sqrt[4]{2},i)$ многочлена x^4-2 буде $1=1\cdot 1,\ \sqrt[4]{2}=1\cdot\sqrt[4]{2},\ \sqrt[4]{4}=1\cdot\sqrt[4]{4},\ \sqrt[4]{8}=1\cdot\sqrt[4]{8},$ $i=i\cdot 1,\ i\cdot\sqrt[4]{2},\ i\cdot\sqrt[4]{4},\ i\cdot\sqrt[4]{8}$.

b) Коренями многочлена x^8+1 будуть числа

$$\varepsilon_k=\cos\Big(\frac{\pi}{8}+\frac{k\pi}{4}\Big)+i\sin\Big(\frac{\pi}{8}+\frac{k\pi}{4}\Big),\quad k=0,1,\dots,7.$$

Зауважимо, що $\varepsilon_k=\varepsilon_0^{2k+1}$. Тому поле $F=\mathbb{Q}(\varepsilon_0)$ буде містити всі корені многочлена x^8+1 і збігатиметься з полем розкладу цього многочлена.

Якщо — звідний, то звідним буде і многочлен $f(y)=(y+1)^8+1$, і навпаки. Але

$$(y+1)^8+1=y^8+\binom{8}{1}y^7+\binom{8}{2}y^6+\dots+\binom{8}{7}y+2.$$

Позаяк

$$\binom{8}{1}=\binom{8}{7}=8,\ \binom{8}{2}=\binom{8}{6}=28,\ \binom{8}{3}=\binom{8}{5}=56,\ \binom{8}{4}=70,$$

то всі коефіцієнти многочлена $f(y)$, окрім старшого, діляться на 2. Але вільний член не ділиться на 4, тому за ознакою Айзенштайна $f(y)$ буде незвідним. Отже, незвідним буде і многочлен x^8+1, коренем якого є ε_0. Тому $[\mathbb{Q}(\varepsilon_0):\mathbb{Q}]=8$, а базою поля розкладу буде $1,\ \varepsilon_0,\ \varepsilon_0^2,\ \varepsilon_0^3,\ \varepsilon_0^4,\ \varepsilon_0^5,$ $\varepsilon_0^6,\ \varepsilon_0^7$. □

Основні задачі

10. З'ясуйте, чи утворює поле множина $\mathbb{Q}\times\mathbb{Q}$ всіх упорядкованих пар раціональних чисел, якщо додавання і множення визначаються такими правилами:
a) $(a,b)\oplus(c,d)=(a+c,b+d),\ (a,b)\odot(c,d)=(ac,bd)$;
b) $(a,b)\oplus(c,d)=(a+c,b+d),\ (a,b)\odot(c,d)=(ac-bd,ad+bc)$;
c) $(a,b)\oplus(c,d)=(a+c,b+d),\ (a,b)\odot(c,d)=(ac+2bd,ad+bc)$.

11. Нехай P — поле. Доведіть, що кільце функцій $\mathrm{Map}(X,P)$ буде полем тоді й лише тоді, коли множина X — одноелементна.

12. Скількома способами можна визначити додавання і множення у множині $\{0, 1, a, b\}$, щоб вийшло поле?

13. Скільки підполів має поле із зад. 12?

14. Доведіть, що всі поля порядку 4 ізоморфні.

15. Чи утворює поле множина
a) $\{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$; b) $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$;
c) $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$;
d) $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$;
e) $\{a + b\sqrt{2} + ci + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\}$?

16. Для яких натуральних чисел $n < p$ множина матриць $\left\{ \begin{pmatrix} a & b \\ nb & a \end{pmatrix} \mid a, b \in \mathbb{Z}_p \right\}$ утворює поле, якщо a) $p = 3$; b) $p = 5$; c) $p = 7$?

17. Чи будуть ізоморфними поле $\mathbb{Q}$ і поле $\mathbb{Q}[\sqrt{2}]$?

18. Чи може поле бути ізоморфним своєму власному підполю?

19. Доведіть, що для кожного вільного від квадратів цілого числа n множини
a) $P_1 = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$ зі звичайними додаванням і множенням;
b) $P_2 = \{\left(\begin{smallmatrix} a & b \\ nb & a \end{smallmatrix}\right) : a, b \in \mathbb{Q}\}$ із матричними додаванням і множенням;
c) $P_3 = \mathbb{Q} \times \mathbb{Q}$ із додаванням і множенням за правилами

$$(a, b) \oplus (c, d) = (a + c, b + d), \quad (a, b) \odot (c, d) = (ac + nbd, ad + bc)$$

є полями, причому для кожного n ці три поля ізоморфні.

20. Доведіть, що в адитивній групі поля всі ненульові елементи мають однаковий порядок.

21. Чи може об'єднання $P_1 \cup P_2$ двох підполів P_1 і P_2 поля P теж бути підполем поля P?

22. Доведіть, що в полі порядку n виконується тотожність $x^n = x$.

23. Розв'яжіть у полі $\mathbb{Q}(\sqrt{2})$ рівняння
a) $x^2 + (4 - 2\sqrt{2})x + (3 - 2\sqrt{2}) = 0$; b) $x^2 - x - 3 = 0$;
c) $x^2 + x - (7 - 6\sqrt{2}) = 0$; d) $x^2 - 2x + (1 - \sqrt{2}) = 0$.

24. Знайдіть характеристику поля, якщо в ньому виконується рівність
a) $(1+1+1+1+1)^2 = (1+1)^5$;
b) $(1+1+1+1+1+1+1)^2 = (1+1)^7$.

25. Наведіть приклад нескінченного поля додатної характеристики.

26. Доведіть, що коли q є степенем простого числа p і P є полем характеристики p, то для довільних елементів $a, b \in P$ виконується рівність $(a+b)^q = a^q + b^q$.

27. Використовуючи те, що характеристика поля $\mathbb{Z}_p$ дорівнює p, доведіть теорему Ферма про подільність $a^p - a$ на p,

28. Доведіть, що в полі P характеристики $p > 0$ із рівності $a^{pk} = 1$ випливає рівність $a^k = 1$.

29. Чи існує поле, яке строго містить поле $\mathbb{C}$?

30. Нехай $F \supset P$ — розширення полів, $c \in F$. Доведіть, що
a) відображення

$$\varphi : P[x] \to F, \quad a_0 + a_1 x + \cdots + a_n x^n \mapsto a_0 + a_1 c + \cdots + a_n c^n,$$

є гомоморфізмом кілець;
b) елемент c буде трансцендентним тоді й лише тоді, коли $\mathrm{Ker}\varphi = 0$;
c) елемент c буде алгебричним тоді й лише тоді, коли $\mathrm{Ker}\varphi \neq 0$.

31. Доведіть, що поля $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ і $\mathbb{Q}(\sqrt{2-\sqrt{3}})$ ізоморфні.

32. a) Доведіть, що коли $\mathrm{char}(P) \neq 2$ і $[F : P] = 2$, то існує такий елемент $a \in F$, що $F = P(a)$ і $a^2 \in P$.
b) Чи залишиться твердження правильним для полів характеристики 2?

33. Нехай F — розширення поля P і $a \in F$. Доведіть, що наступні умови рівносильні:
a) елемент a є алгебричним над P;
b) $P[a] = P(a)$;
c) $[P(a) : P] < \infty$;
d) $[P[a] : P] < \infty$.

34. Доведіть, що $[P(x) : P(x^2)] = 2$ для кожного поля P.

35. Для елемента a знайдіть мінімальний многочлен над полем P:
a) $a = \sqrt{3}$, $P = \mathbb{Q}$; b) $a = \sqrt[50]{8}$, $P = \mathbb{Q}$;
c) $a = 1 + \sqrt{3}$, $P = \mathbb{Q}(\sqrt{2} + \sqrt{3})$; d) $a = \sqrt{2} + \sqrt{3}$, $P = \mathbb{Q}(1 + \sqrt{3})$.

36. Нехай a — корінь многочлена $x^3 + 3x^2 - 9x + 6 \in Q[x]$. Подайте у вигляді многочлена від a найменшого можливого степеня наступні елементи поля $\mathbb{Q}(a)$: a) $a^4 + a$; b) a^5; c) $\frac{1}{a}$; d) $\frac{a^4+3a+1}{a^2+2a-11}$.

37. Нехай a — корінь многочлена $x^3 - x - 1 \in Q[x]$. Знайдіть многочлен з раціональними коефіцієнтами, коренем якого є число $a^2 - a - 1$.

38. Нехай $\mathbb{Q}(a)$ — просте трансцендентне розширення поля $\mathbb{Q}$. Доведіть, що поле розкладу многочлена $x^2 - a$ з коефіцієнтами із $\mathbb{Q}(a)$ ізоморфне полю $\mathbb{Q}(a)$.

39. Нехай $F \supset P$ і елементи $a, b \in F$ є алгебричними n над P степенів m і k відповідно. Доведіть, що елементи $a + b$ і ab є алгебричними над P і степінь кожного з них не перевищує mk.

40. Нехай $F = P(a)$ і елемент a є алгебричним степеня n над полем P. Доведіть, що кожен елемент $b \in F$ є алгебричним над P і степінь b є дільником числа n.

41. Чи може поле з 8 елементів містити підполе з 4 елементів?

42. Доведіть, що коли степінь $[F : P]$ розширення $F \supset P$ є простим числом, то $F = P(a)$ для довільного $a \in F \setminus P$.

43. Знайдіть степінь і яку–небудь базу наступних розширень поля $\mathbb{Q}$: a) $\mathbb{Q}(1 + \sqrt{5})$; b) $\mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{4})$; c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$; d) $\mathbb{Q}(1 + i)$.

44. Знайдіть степінь поля розкладу над $\mathbb{Q}$ для многочлена:
a) $x^2 - 2$, b) $x^3 - 2$, c) $x^4 + 2$, d) $x^4 + x^2 + 1$ e) $x^8 - 1$.

45. Знайдіть степінь поля розкладу над $\mathbb{Q}$ для многочлена:
a) $x^p - 1$ (p — просте число), b) $x^n - 1$, c) $x^p - a$ (p — просте число і a не є p–м степенем елемента з $\mathbb{Q}$).

46. Доведіть, що кожне алгебрично замкнене поле є нескінченним.

Додаткові задачі

47. Доведіть, що множина $\mathbb{Q}$ із діями

$$x \oplus y = x + y + 1, \quad x \odot y = xy + x + y$$

є полем.

48. Доведіть, що множина $P((x)) = \left\{ \sum_{n\geq N}^{\infty} a_n x^n \mid a_n \in P \text{ і } N \in \mathbb{Z} \right\}$ *рядів Лорана* з коефіцієнтами з поля P буде полем відносно природно визначених додавання і множення рядів.

49. Доведіть, що в полі $\mathbb{Z}_p$ виконуються рівності
a) $\sum_{k=1}^{p-1} \frac{1}{k} = 0$ $(p > 2)$; b) $\sum_{k=1}^{(p-1)/2} \frac{1}{k^2} = 0$ $(p > 3)$.

50. Доведіть, що кожна скінченна область цілісності K порядку ≥ 2 є полем.

51. Доведіть, що поле часток кільця $\mathbb{Z}[i]$ ізоморфне полю $\mathbb{Q}[i]$.

52. Нехай P — поле характеристики $p > 0$ і A, B — дві переставні матриці однакового порядку з коефіцієнтами з поля P. Доведіть, що $(A + B)^p = A^p + B^p$.

53. Нехай P — поле характеристики p.
a) Доведіть, що перетворення $P \to P$, $a \mapsto a^p$, є ін'єктивним ендоморфізмом.
b) Доведіть, що коли поле P — скінченне, то перетворення $a \mapsto a^p$ є автоморфізмом.
c) Наведіть приклад поля P характеристики p, для якого перетворення $a \mapsto a^p$ не є автоморфізмом.

54.* Доведіть, що в полі характеристики $p > 0$ виконується рівність $(a - b)^{p-1} = \sum_{k=0}^{p-1} a^k b^{p-1-k}$.

55. Доведіть, що кожне поле порядку p^2, де p — просте число, містить єдине власне підполе.

56. Доведіть, що для довільних ненульових раціональних чисел a і b наступні умови рівносильні:
a) $\mathbb{Q}(\sqrt{a}) \simeq \mathbb{Q}(\sqrt{b})$;
b) $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$;
c) число a/b є квадратом раціонального числа.

57. Нехай F — розширення поля P і A — підполе всіх тих елементів з F, які є алгебричними над P. Доведіть, що коли елемент $a \in F$ є алгебричним над A, то $a \in A$.

58. a) Доведіть, що коли a є алгебричним над P елементом непарного степеня, то $P(a) = P(a^2)$.
b) Чи правильне зворотне твердження, тобто що коли $P(a) = P(a^2)$, то a є алгебричним над полем P елементом непарного степеня?

59. Нехай $L \supseteq P$ — алгебричне розширення. Доведіть, що розширення $L(x) \supseteq P(x)$ також є алгебричним і що $[L(x) : P(x)] = [L : P]$.

60. Доведіть, що для довільного елемента $a \in P(x) \setminus P$ поле $P(x)$ є алгебричним розширенням поля $P(a)$.

61. Нехай $P(t_1, \ldots, t_n)$ — поле раціональних функцій від змінних t_1, $\ldots$, t_n. Доведіть, що елемент $a \in P(t_1, \ldots, t_n)$ буде алгебричним над P тоді й лише тоді, коли $a \in P$.

62.* Доведіть, що поля $\mathbb{Q}(x)$ і $\mathbb{Q}(x, y)$ не ізоморфні.

63. Нехай ε_n — первісний корінь степеня n з 1. Знайдіть степінь і яку–небудь базу даного розширення поля $\mathbb{Q}$: a) $\mathbb{Q}(\varepsilon_p)$, де p — просте число; b) $\mathbb{Q}(\varepsilon_6)$; c) $\mathbb{Q}(\varepsilon_3, \sqrt[3]{3})$.

64. Нехай $f(x) \in P[x]$ — многочлен степеня n, а F — його поле розкладу. Доведіть, що степінь розширення $F \supseteq P$ є дільником числа $n!$.

65. a) Нехай a і b —алгебричні над полем P елементи степенів m і n відповідно, причому m і n — взаємно прості. Доведіть, що $[P(a, b) : P] = mn$.
b) Наведіть приклад таких алгебричних над полем P елементів a і b степенів m і n $(m \neq n)$ відповідно, що $[P(a, b) : P] < mn$.

66. Доведіть, що коли степінь n незвідного над полем P многочлена $f(x)$ є взаємно простим зі степенем $[F : P]$ розширення $F \supseteq P$, то $f(x)$ залишається незвідним і над полем F.

67. Нехай a_1, a_2, a_3 — комплексні корені многочлена $x^3 - x + 1$. Що можна сказати про розширення $\mathbb{Q}(a_1^{19} + a_2^{19} + a_3^{19})$?

68.* Нехай P — поле і p — просте число. Доведіть, що многочлен $x^p - a \in P[x]$ або незвідний, або має в полі P корінь.

69.* Наведіть приклад такого незвідного многочлена $f(x) \in \mathbb{Q}[x]$ і його коренів a_1, a_2, a_3, що поля $\mathbb{Q}(a_1, a_2)$ і $\mathbb{Q}(a_1, a_3)$ — не ізоморфні.

70. Доведіть, що коли характеристика поля не дорівнює 2, то кожен елемент поля є різницею двох квадратів.

71. Доведіть, що коли характеристика поля P не дорівнює 2 і в полі P елемент -1 є сумою k квадратів, то кожен елемент поля P можна розкласти в суму щонайбільше $k+1$ квадратів.

72. Наведіть приклад таких полів $P \subset L \subset M$, що $[M : P] < \infty$, але $M \simeq L$.

73. Нехай $\mathrm{char}P \neq 2$, n — непарне число і розширення $F \supseteq P$ поля P містить усі корені степеня n з одиниці. Доведіть, що F містить усі корені степеня $2n$ з одиниці.

74.** Нехай F — таке підполе поля $\mathbb{C}$, що $[\mathbb{C} : F] < \infty$. Доведіть, що $[\mathbb{C} : F] \leq 2$.

Домашнє завдання

75. З'ясуйте, чи утворює поле множина $\mathbb{C} \times \mathbb{C}$ всіх впорядкованих пар комплексних чисел, якщо додавання і множення визначаються такими правилами:
a) $(a,b) \oplus (c,d) = (a+c, b+d)$, $(a,b) \odot (c,d) = (ac, bd)$;
b) $(a,b) \oplus (c,d) = (a+c, b+d)$, $(a,b) \odot (c,d) = (ac-bd, ad+bc)$;
c) $(a,b) \oplus (c,d) = (a+c, b+d)$, $(a,b) \odot (c,d) = (ac+2bd, ad+bc)$.

76. a) Чи утворює поле відносно звичайних додавання і множення множина
a) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, b) $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$?

77. Якою може бути характеристика поля, якщо в ньому виконується рівність $(1+1+1+1+1+1+1)^3 = (1+1+1)^7$?

78. З'ясуйте, чи будуть ізоморфними поля $\mathbb{Q}(\sqrt{3})$ і $\mathbb{Q}(\sqrt{5})$.

79. Нехай a — корінь многочлена $x^3 - x - 1 \in Q[x]$.
a) Подайте у вигляді многочлена від a найменшого можливого степеня наступні елементи поля $\mathbb{Q}(a)$: a^5; $\frac{1}{a}$; $\frac{a-2}{a^2+1}$.
b) Знайдіть многочлен з раціональними коефіцієнтами, коренем якого є $a^2 + a$.

80. Знайдіть степінь і яку–небудь базу даного розширення поля $\mathbb{Q}$:
a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$; b) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$; c) $\mathbb{Q}(\sqrt{3}, i)$.

81. Знайдіть степінь і яку–небудь базу поля розкладу над $\mathbb{Q}$ для многочлена a) $(x^2-2)(x^2-3)$, b) x^3-3, c) x^4-5.

Заняття 6. Автоморфізми полів. Скінченні поля.

Необхідні поняття. перетворення $\varphi : P \to P$ поля P називається *автоморфізмом* поля P, якщо воно взаємно однозначне і зберігає дії, тобто $\varphi(a+b) = \varphi(a) + \varphi(b)$ і $\varphi(ab) = \varphi(a)\varphi(b)$. Множина всіх автоморфізмів поля P позначається $\mathrm{Aut}\, P$.

Для кожного підполя $P \subseteq F$ через $\mathrm{Aut}(F : P)$ позначається множина $\{\varphi \in \mathrm{Aut}\, F \mid \varphi(x) = x \text{ для всіх } x \in P\}$.

Розширення $K \supseteq P$ називається *нормальним*, якщо довільний незвідний над P многочлен $f(x) \in P[x]$, який має в полі K хоча б один корінь, розкладається над K на лінійні множники.

Необхідні твердження. **1.** Кожне просте поле має тільки тривіальний автоморфізм.

2. Кожен автоморфізм поля діє тотожно на простому підполі.

3. Множина $\mathrm{Aut}P$ всіх автоморфізмів поля P утворює групу відносно композиції автоморфізмів.

4. Множина $\mathrm{Aut}(F : P)$ є підгрупою групи $\mathrm{Aut}\, F$.

5. Якщо $K = P(a)$ — просте алгебричне розширення поля P, то $|\mathrm{Aut}(K : P)| \leq [K : P]$.

6. Для скінченного розширення F поля P характеристики 0 наступні умови рівносильні:

(1) розширення $F \supseteq P$ — нормальне;

(2) для кожного елемента $c \in F \setminus P$ існує такий автоморфізм $\varphi \in \mathrm{Aut}(F : P)$, що $\varphi(c) \neq c$;

(3) $[F : P] = |\mathrm{Aut}(F : P)|$;

(4) F є полем розкладу деякого многочлена $f(x) \in P[x]$.

7. Якщо a і b — корені незвідного многочлена $f(x) \in P[x]$ степеня n, то відображення

$$\alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1} a^{n-1} \mapsto \alpha_0 + \alpha_1 b + \cdots + \alpha_{n-1} b^{n-1}$$

є ізоморфізмом поля $P(a)$ на поле $P(b)$.

8. Теорема про примітивний елемент. Кожне скінченне розширення поля характеристики 0 є простим алгебричним розширенням.

9. Якщо P — скінченне поле, то існує таке просте число p, що просте підполе поля P ізоморфне $\mathbb{Z}_p$, а порядок поля P є степенем числа p.

10. Теорема про класифікацію скінченних полів. Для довільних простого числа p і натурального числа n існує поле порядку p^n. Будь–які два скінченні поля однакового порядку є ізоморфними.

11. Скінченне поле порядку p^n є полем розкладу многочлена $x^{p^n} - x \in \mathbb{Z}_p$ і збігається з множиною всіх його коренів.

12. Теорема про решітку підполів скінченного поля Нехай F — поле порядку p^n і K — його підполе. Тоді K має порядок p^m, причому $m \mid n$.

Навпаки, для кожного дільника m числа n поле F містить підполе K порядку p^m, причому тільки одне.

13. Мультиплікативна група GF_q^* скінченного поля GF_q порядку q є циклічною групою порядку $q-1$.

14. Якщо F — скінченне розширення поля $\mathbb{Z}_p$, в якому незвідний многочлен $f(x) \in \mathbb{Z}[x]$ має корінь, то $f(x)$ розкладається над полем F на лінійні множники.

Приклади розв'язання типових задач

Задача 1. *Нехай P — просте підполе поля F. Доведіть, що кожен автоморфізм поля F діє на P тотожно.*

Розв'язання. Нехай $\varphi \in \operatorname{Aut} F$. Нагадаємо, що $\varphi(1) = 1$. Позаяк кожне просте поле ізоморфне або $\mathbb{Z}_p$, де p — просте число, або $\mathbb{Q}$, то розглянемо два випадки:

1) $P = \mathbb{Z}_p$. Кожен елемент $k \in \mathbb{Z}_p$ можна записати у вигляді $k = \underbrace{1 + \cdots + 1}_{k}$. Тому

$$\varphi(k) = \varphi\big(\underbrace{1 + \cdots + 1}_{k}\big) = \underbrace{\varphi(1) + \cdots + (1)}_{k} = \underbrace{1 + \cdots + 1}_{k} = k. \qquad (27)$$

2) $P = \mathbb{Q}$. Аналогічно (27) доводимо, що для кожного натурального числа n $\varphi(n) = n$. Далі для кожного від'ємного цілого числа m отримуємо:

$$\varphi(m) = \varphi(-|m|) = -\varphi(|m|) = -|m| = m.$$

Нарешті, для довільного раціонального числа $\dfrac{m}{n}$ маємо:

$$\varphi\Big(\frac{m}{n}\Big) = \frac{\varphi(m)}{\varphi(n)} = \frac{m}{n}. \qquad \square$$

Зауваження. Із зад. 1 випливає, зокрема, що просте поле не має нетотожних автоморфізмів.

Задача 2. *Знайдіть усі автоморфізми поля* $\mathbb{R}$.

Розв'язання. Нехай $\varphi \in \operatorname{Aut}\mathbb{R}$. Поле $\mathbb{Q}$ є простим підполем поля $\mathbb{R}$, тому, згідно зад. 1, $\varphi(a) = a$ для всіх раціональних чисел a. Далі зауважимо, що число з $\mathbb{R}$ буде додатним тоді й лише тоді, коли воно є квадратом ненульового числа, і що φ квадрати переводить у квадрати: $\varphi(x{\cdot}x) = \varphi(x){\cdot}\varphi(x)$. Отже, φ зберігає властивість бути додатним числом. Тому $\varphi(x) - \varphi(y) = \varphi(x - y) > 0$ тоді й лише тоді, коли $x - y > 0$. Але нерівності $a - b > 0$ і $a > b$ рівносильні. Тому $\varphi(x) > \varphi(y)$ тоді й лише тоді, коли $x > y$. Отже, φ зберігає відношення порядку на множині $\mathbb{R}$.

Із аналізу відомо, що кожне дійсне число x однозначно визначається так званим перетином Дедекінда, тобто парою множин $A = \{a \in \mathbb{Q} \mid a < x\}$ і $B = \{b \in \mathbb{Q} \mid b > x\}$. Позаяк φ зберігає відношення порядку і лишає на місці всі раціональні числа, то для $\varphi(x)$ множини A і B будуть тими самими. Тому $\varphi(x) = x$.

Отже, поле $\mathbb{R}$ має лише один автоморфізм — тотожний. □

Задача 3. *Знайдіть усі автоморфізми поля* *a)* $\mathbb{Q}(\sqrt{2})$; *b)* $\mathbb{Q}(\sqrt[3]{3})$; *c)* $Q(\sqrt{2} + \sqrt{3})$.

Розв'язання. a) Нехай $\varphi \in \operatorname{Aut}\mathbb{Q}(\sqrt{2})$. $(\sqrt{2})^2 = 2$, тому

$$(\varphi(\sqrt{2}))^2 = \varphi((\sqrt{2})^2) = \varphi(2) = 2.$$

Отже, $\varphi(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$.

Якщо $\varphi(\sqrt{2}) = \sqrt{2}$, то для довільного елемента $a + b\sqrt{2}$ із $\mathbb{Q}(\sqrt{2})$ $(a, b \in \mathbb{Q})$ маємо:

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b\sqrt{2}.$$

Отже, в цьому випадку маємо тотожний автоморфізм.

Якщо ж $\varphi(\sqrt{2}) = -\sqrt{2}$, то для довільного $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ маємо:

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a - b\sqrt{2}.$$

Безпосередньо перевіряється, що в цьому випадку

$$\begin{gathered}\varphi\big(a+b\sqrt{2})+(c+d\sqrt{2})\big)=\varphi\big(a+c)+(b+d)\sqrt{2})\big)=\\ =(a+c)-(b+d)\sqrt{2})=(a-b\sqrt{2})+(c-d\sqrt{2})=\\ =\varphi\big(a+b\sqrt{2})+\varphi\big(c+d\sqrt{2}),\\ \varphi\big(a+b\sqrt{2})\cdot(c+d\sqrt{2})\big)=\varphi\big(ac+2bd)+(b+d)\sqrt{2})\big)=\\ =(ac+2bd)-(b+d)\sqrt{2})=(a-b\sqrt{2})\cdot(c-d\sqrt{2})=\\ =\varphi\big(a+b\sqrt{2})\cdot\varphi\big(c+d\sqrt{2}),\end{gathered}$$

тобто в цьому випадку φ також є автоморфізмом.

Таким чином, поле $\mathbb{Q}(\sqrt{2})$ має 2 автоморфізми:

$$\varphi_1 : a+b\sqrt{2}\mapsto a+b\sqrt{2} \quad \text{і} \quad \varphi_2 : a+b\sqrt{2}\mapsto a-b\sqrt{2}.$$

b) Позаяк $\mathbb{Q}$ є простим підполем поля $\mathbb{Q}(\sqrt[3]{3})$, то для довільного $\varphi\in \operatorname{Aut}\mathbb{Q}(\sqrt[3]{3})$ із рівності $(\sqrt[3]{3})^3=2$ випливає, що $(\varphi(\sqrt[3]{3}))^3=\varphi(2)=2$. Отже, автоморфізм φ має переводити $\sqrt[3]{3}$ у корінь многочлена x^3-2. Але поле $\mathbb{Q}(\sqrt[3]{3})=\{a+b\sqrt[3]{3}+c(\sqrt[3]{3})^2 \mid a,b,c\in\mathbb{Q}\}$ містить лише дійсні числа, а многочлен x^3-2 має лише один дійсний корінь — $\sqrt[3]{3}$. Тому $\varphi(\sqrt[3]{3})=\sqrt[3]{3}$ і для довільного елемента $a+b\sqrt[3]{3}+c(\sqrt[3]{3})^2\in\mathbb{Q}(\sqrt[3]{3})$

$$\varphi(a+b\sqrt[3]{3}+c(\sqrt[3]{3})^2)=a+b\varphi(\sqrt[3]{3})+c\varphi((\sqrt[3]{3})^2)=a+b\sqrt[3]{3}+c(\sqrt[3]{3})^2.$$

Таким чином, поле $\mathbb{Q}(\sqrt[3]{3})$ має лише тотожний автоморфізм.

c) Очевидно, що $Q(\sqrt{2}+\sqrt{3})\subseteq Q(\sqrt{2},\sqrt{3})$. Навпаки, із

$$\begin{gathered}\sqrt{2}+\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})\Rightarrow\\ \Rightarrow(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}\in Q(\sqrt{2}+\sqrt{3})\Rightarrow\sqrt{6}\in Q(\sqrt{2}+\sqrt{3})\Rightarrow\\ \Rightarrow\sqrt{6}\cdot(\sqrt{2}+\sqrt{3})=3\sqrt{2}+2\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})\Rightarrow\\ \Rightarrow(3\sqrt{2}+2\sqrt{3})-2(\sqrt{2}+\sqrt{3})=\sqrt{2}\in Q(\sqrt{2}+\sqrt{3})\Rightarrow\\ \Rightarrow(\sqrt{2}+\sqrt{3})-\sqrt{2}=\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})\end{gathered}$$

випливає, що $Q(\sqrt{2}+\sqrt{3})\supseteq Q(\sqrt{2},\sqrt{3})$. Отже,

$$Q(\sqrt{2}+\sqrt{3})=Q(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Q}\}.$$

Аналогічно попередньому доводимо, що $\varphi(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$ і $\varphi(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$. Тому автоморфізмами поля $Q(\sqrt{2}+\sqrt{3})$ можуть бути лише такі 4 відображення:

$$\varphi_1(\sqrt{2}) = \sqrt{2}, \quad \varphi_1(\sqrt{3}) = \sqrt{3},$$
$$\varphi_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};$$
$$\varphi_2(\sqrt{2}) = -\sqrt{2}, \quad \varphi_2(\sqrt{3}) = \sqrt{3},$$
$$\varphi_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6};$$
$$\varphi_3(\sqrt{2}) = \sqrt{2}, \quad \varphi_3(\sqrt{3}) = -\sqrt{3},$$
$$\varphi_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6};$$
$$\varphi_4(\sqrt{2}) = -\sqrt{2}, \quad \varphi_4(\sqrt{3}) = -\sqrt{3},$$
$$\varphi_4(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$

Відображення φ_1 є тотожним перетворенням, а тому є автоморфізмом.

Для відображення φ_2 маємо:

$$\varphi_2\big((a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) + (a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6})\big) =$$
$$= \varphi_2\big((a_1 + a_2) + (b_1 + b_2)\sqrt{2} + (c_1 + c_2)\sqrt{3} + (d_1 + d_2)\sqrt{6}\big) =$$
$$= (a_1 + a_2) - (b_1 + b_2)\sqrt{2} + (c_1 + c_2)\sqrt{3} - (d_1 + d_2)\sqrt{6} =$$
$$= (a_1 - b_1\sqrt{2} + c_1\sqrt{3} - d_1\sqrt{6}) + (a_2 - b_2\sqrt{2} + c_2\sqrt{3} - d_2\sqrt{6})$$
$$= \varphi_2(a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) + \varphi_2(a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6});$$

$$\varphi_2\big((a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) \cdot (a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6})\big) =$$
$$= \varphi_2\big((a_1a_2 + 2b_1b_2 + 3c_1c_2 + 6d_1d_2) + (a_1b_1 + b_1a_2 + 3c_1d_2 + 3d_1c_2)\sqrt{2} +$$
$$+(a_1c_2 + c_1a_2 + 2b_1d_2 + 2d_1b_2)\sqrt{3} + (a_1d_2 + b_1c_2 + c_1b_1 + d_1a_2)\sqrt{6}\big) =$$
$$= (a_1a_2 + 2b_1b_2 + 3c_1c_2 + 6d_1d_2) - (a_1b_1 + b_1a_2 + 3c_1d_2 + 3d_1c_2)\sqrt{2} +$$
$$+(a_1c_2 + c_1a_2 + 2b_1d_2 + 2d_1b_2)\sqrt{3} - (a_1d_2 + b_1c_2 + c_1b_1 + d_1a_2)\sqrt{6} =$$
$$= (a_1 - b_1\sqrt{2} + c_1\sqrt{3} - d_1\sqrt{6}) \cdot (a_2 - b_2\sqrt{2} + c_2\sqrt{3} - d_2\sqrt{6})$$
$$= \varphi_2(a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) \cdot \varphi_2(a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6}).$$

Отже, відображення φ_2 є автоморфізмом. Аналогічно перевіряється, що φ_3 також є автоморфізмом. Нарешті, відображення φ_4 є композицією автоморфізмів φ_2 і φ_3, а тому також є автоморфізмом.

Таким чином, поле $Q(\sqrt{2}+\sqrt{3})$ має 4 автоморфізми: φ_1, φ_2, φ_3 і φ_4. □

Задача 4. *Знайдіть групу автоморфізмів поля розкладу многочлена* $x^5+1 \in \mathbb{Q}[x]$.

Розв'язання. Позначимо поле розкладу через P. Позаяк $x^5+1 = (x+1)(x^4-x^3+x^2-x+1)$, то поле розкладу многочлена x^5+1 збігається з полем розкладу многочлена $f(x)=x^4-x^3+x^2-x+1$. Коренями многочлена x^5+1 є ті корені многочлена $x^{10}-1$, які не є коренями x^5-1, тобто ε_{10}, ε_{10}^3, ε_{10}^7, ε_{10}^9 і -1, де $\varepsilon_{10}=\cos\frac{\pi}{5}+i\sin\frac{\pi}{5}$ — первісний корінь степеня 10 із 1. Очевидно, що $P \supseteq \mathbb{Q}(\varepsilon_{10})$. Але поле $\mathbb{Q}(\varepsilon_{10})$ містить і кожне з чисел ε_{10}^3, ε_{10}^7, ε_{10}^9, тому $P=\mathbb{Q}(\varepsilon_{10})$.

Многочлен $f(x)=\dfrac{x^5+1}{x+1}$ — незвідний, бо незвідним за ознакою Айзенштайна є многочлен

$$f(y-1)=y^4-\binom{5}{1}y^3+\binom{5}{2}y^2-\binom{5}{3}y+\binom{5}{4}$$

(усі коефіцієнти, крім старшого, діляться на 5, але вільний член не ділиться на 25). Тому за теоремою про просте алгебричне розширення кожне з полів $P=\mathbb{Q}(\varepsilon_{10})$, $\mathbb{Q}(\varepsilon_{10}^3)$, $\mathbb{Q}(\varepsilon_{10}^7)$, $\mathbb{Q}(\varepsilon_{10}^9)$ є розширенням степеня 4 поля $\mathbb{Q}$. Оскільки $\varepsilon_{10}^3, \varepsilon_{10}^7, \varepsilon_{10}^9 \in P$, то $P=\mathbb{Q}(\varepsilon_{10}^3)=\mathbb{Q}(\varepsilon_{10}^7)=\mathbb{Q}(\varepsilon_{10}^9)$. Тому за твердженням **7** відображення

$$\varphi : a+b\varepsilon_{10}+c\varepsilon_{10}^2+d\varepsilon_{10}^3 \mapsto a+b\varepsilon_{10}^3+c(\varepsilon_{10}^3)^2+d(\varepsilon_{10}^3)^3$$

буде автоморфізмом поля P.

Автоморфізмами будуть і степені автоморфізму φ. Зауважимо, що

$$\varphi^2(\varepsilon_{10})=\varphi(\varphi(\varepsilon_{10}))=\varphi(\varepsilon_{10}^3)=(\varphi(\varepsilon_{10}))^3=(\varepsilon_{10}^3)^3=\varepsilon_{10}^9.$$

Аналогічно отримуємо, що $\varphi^3(\varepsilon_{10})=\varepsilon_{10}^7$, $\varphi^4(\varepsilon_{10})=\varepsilon_{10}$. Зокрема, φ^4 збігається з тотожним автоморфізмом. Таким чином, φ породжує циклічну групу $\langle\varphi\rangle$ порядку 4 автоморфізмів поля P. Із другого боку, за твердженням **5** $|\mathrm{Aut}\,P| \le 4$. Тому $\mathrm{Aut}\,P=\langle\varphi\rangle$. □

Задача 5. *Доведіть, що для кожного автоморфізму* φ *поля* F *множина*

$$\mathrm{Fix}(\varphi)=\{x \in F \mid \varphi(x)=x\}$$

нерухомих точок цього автоморфізму є підполем поля F.

Розв'язання. Нехай $x, y \in \mathrm{Fix}(\varphi)$. Тоді

$$\varphi(x+y) = \varphi(x) + \varphi(y) = x + y, \quad \varphi(-x) = -\varphi(x) = -x,$$
$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = x \cdot y, \quad \varphi(x^{-1}) = (\varphi(x))^{-1} = x^{-1}.$$

Таким чином, множина $\mathrm{Fix}(\varphi)$ замкнена відносно додавання, множення і взяття протилежного та оберненого елементів. Тому $\mathrm{Fix}(\varphi)$ є підполем. □

Задача 6. *Доведіть, що поле $\mathbb{Q}(\varepsilon_n)$, де ε_n — первісний корінь степеня n з 1, є нормальним розширенням поля $\mathbb{Q}$.*

Розв'язання. Кожен корінь степеня n з 1 є степенем первісного кореня степеня n. Тому поле $\mathbb{Q}(\varepsilon_n)$ містить усі корені степеня n з 1 і над цим полем многочлен $x^n - 1$ розкладається на лінійні множники:

$$x^n - 1 = (x-1)(x-\varepsilon_n)(x-\varepsilon_n^2)\cdots(x-\varepsilon_n^{n-1}).$$

Отже, $\mathbb{Q}(\varepsilon_n)$ є полем розкладу многочлена $x^n - 1$, а тому є нормальним розширенням поля $\mathbb{Q}$. □

Задача 7. *З'ясуйте, чи буде поле $\mathbb{Q}(\sqrt[6]{3}, i)$ нормальним розширенням поля $\mathbb{Q}$.*

Розв'язання. $\sqrt[6]{3}$ є коренем многочлена $x^6 - 3$. Іншими його коренями є $-\sqrt[6]{3}$ та $\sqrt[6]{3}\Big(\pm\dfrac{\sqrt{3}}{2} \pm \dfrac{1}{2}i\Big)$. Тому поле розкладу P многочлена $x^6 - 3$ містить як $\sqrt[6]{3}$, так і

$$i = \big(\sqrt[6]{3}\big)^{-1} \cdot \left(\sqrt[6]{3}\Big(\frac{\sqrt{3}}{2} + \frac{1}{2}i\Big) + \sqrt[6]{3}\Big(-\frac{\sqrt{3}}{2} + \frac{1}{2}i\Big)\right).$$

Отже, $P \supseteq \mathbb{Q}(\sqrt[6]{3}, i)$.

Навпаки, якщо розширення поля $\mathbb{Q}$ містить $\sqrt[6]{3}$ та i, то воно містить $(\sqrt[6]{3})^3 = \sqrt{3}$, а тому містить і числа $\sqrt[6]{3}\Big(\pm\dfrac{\sqrt{3}}{2} \pm \dfrac{1}{2}i\Big)$. Отже, $P \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$.

Таким чином, $P = \mathbb{Q}(\sqrt[6]{3}, i)$, тобто $\mathbb{Q}(\sqrt[6]{3}, i)$ є полем розкладу многочлена $x^6 - 3$. Тому $\mathbb{Q}(\sqrt[6]{3}, i)$ є нормальним розширенням поля $\mathbb{Q}$. □

Задача 8. *Знайдіть групу автоморфізмів поля розкладу многочлена $x^3 + 2x + 1$ із раціональними коефіцієнтами.*

Розв'язання. Похідна $3x^2+2$ даного многочлена строго додатна, тому він має лише один дійсний корінь a. Позначимо один із комплексних коренів через b (другим буде спряжене число $\overline{b}$). Тоді для поля розкладу P одержуємо таку вежу розширень:

$$P = \mathbb{Q}(a,b) \supset \mathbb{Q}(a) \supset \mathbb{Q}. \tag{28}$$

Зауважимо, що b є коренем многочлена другого степеня $\dfrac{x^3+2x+1}{x-a}$. Тому $[\mathbb{Q}(a,b):\mathbb{Q}(a)] = 2$, $[\mathbb{Q}(a):\mathbb{Q}] = 3$ і $[P:\mathbb{Q}] = 2\cdot 3 = 6$. Позаяк P є полем розкладу, то за твердженням **6** $\operatorname{Aut} P$ має порядок 6.

Кожен автоморфізм φ поля P лишає на місці всі раціональні числа. Тому з рівності $c^3+2c+1=0$ випливає, що

$$\varphi(c)^3 + 2\varphi(c) + 1 = \varphi(c)^3 + \varphi(2)\varphi(c) + \varphi(1) = \varphi(c^3+2c+1) = \varphi(0) = 0.$$

Отже, φ корінь многочлена x^3+2x+1 переводить у корінь цього ж многочлена, тобто група $\operatorname{Aut} P$ діє на множині $\{a, b, \overline{b}\}$ коренів цього многочлена як група підстановок. Із (24) випливає, що кожен елемент поля P можна записати у вигляді

$$(\alpha_1 + \alpha_2 a + \alpha_3 a^2) + b(\alpha_4 + \alpha_5 a + \alpha_6 a^2),$$

де $\alpha_1, \ldots, \alpha_6 \in \mathbb{Q}$. Тому якщо автоморфізм φ лишає на місці корені a і b, то він лишає на місці кожен елемент поля P, тобто є тотожним. Отже, різним автоморфізмам із $\operatorname{Aut} P$ мають відповідати різні підстановки на множині $\{a, b, \overline{b}\}$ коренів многочлена x^3+2x+1. Оскільки $|\operatorname{Aut} P| = 6$, то ми одержуємо всі підстановки на цій множині.

Таким чином, група $\operatorname{Aut} P$ ізоморфна групі S_3 всіх підстановок трьохелементної множини. □

Задача 9. *Нехай GF_q — скінченне поле порядку q. Доведіть, що кожне відображення $\varphi : GF_q \to GF_q$ можна задати многочленом $f(x) \in GF_q[x]$ степеня $< q$.*

Розв'язання. Нехай $GF_q = \{a_1, a_2, \ldots, a_q\}$, а відображення φ в точках $a_1, a_2, \ldots, a_q$ набуває відповідно значень $b_1, b_2, \ldots, b_q$. За інтерполяційною формулою Лагранжа існує многочлен $f(x) \in GF_q[x]$ степеня $< q$

$$f(x) = \sum_{k=1}^{q} b_k \frac{(x-a_1)\cdots(x-a_{k-1})(x-a_{k+1})\cdots(x-a_q)}{(a_k-a_1)\cdots(a_k-a_{k-1})(a_k-a_{k+1})\cdots(a_k-a_q)},$$

який в даних точках набуває даних значень. Позаяк точками a_1, a_2, $\ldots$, a_q вичерпується вся область визначення відображення φ, то $f(x)$ задає те саме відображення, що й φ. $\square$

Задача 10. *a) Доведіть, що многочлен $f(x) = x^3 + x^2 + 1$ незвідний над полем $\mathbb{Z}_2$.*
b) Побудуйте таблицю множення поля $\mathbb{Z}_2(a)$, де a — корінь многочлена $f(x)$.
c) Розкладіть над цим полем многочлен $f(x)$ на лінійні множники.
d) Знайдіть який–небудь твірний елемент b мультиплікативної групи $(\mathbb{Z}_2(a))^*$ і подайте інші елементи групи $(\mathbb{Z}_2(a))^*$ у вигляді степенів елемента b.
e) Обчисліть у полі $\mathbb{Z}_2(a)$ значення виразу $\dfrac{(a+1)(a^2+a+1)}{a^2+1}$.

Розв'язання. a) Якщо многочлен $f(x) \in P[x]$ степеня 3 розкладається над полем P у добуток, то хоча б один із множників має степінь 1. Але тоді (x) має корінь у полі P. Легко перевіряється, що (x) многочлен $x^3 + x^2 + 1$ у полі $\mathbb{Z}_2 = \{0, 1\}$ коренів не має. Тому він незвідний.

b) За теоремою про будову простого алгебричного розширення поле $\mathbb{Z}_2(a)$ містить такі елементи: 0, 1, a, $a+1$, a^2, a^2+1, a^2+a, a^2+a+1. Враховуючи, що $a^3+a^2+1=0$, тобто $a^3 = a^2+1$, одержуємо таку таблицю множення (обмежуємося лише множенням ненульових елементів):

	1	a	a+1	a^2	a^2+1	a^2+a	a^2+a+1
1	1	a	a+1	a^2	a^2+1	a^2+a	a^2+a+1
a	a	a^2	a^2+a	a^2+1	a^2+a+1	1	a+1
a+1	1+a	a^2+a	a^2+1	1	a	a^2+a+1	a^2
a^2	a^2	a^2+1	1	a^2+a+1	a+1	a	a^2+a
a^2+1	a^2+1	a^2+a+1	a	a+1	a^2+a	a^2	1
a^2+a	a^2+a	1	a^2+a+1	a	a^2	a+1	a^2+1
a^2+a+1	a^2+a+1	a+1	a^2	a^2+a	1	a^2+1	a

.

c) a є коренем $f(x)$, тому одним із множників буде $x+a$. Розділимо $f(x)$ на $x+a$ за схемою Горнера:

	1	1	0	1
a	1	$a+1$	a^2+a	0

.

Отже, $x^3 + x^2 + 1 = (x+a)\big(x^2 + (a+1)x + (a^2+a)\big)$. Безпосередньо перевіряється, що одним із коренів многочлена $x^2+(a+1)x+(a^2+a)$ є a^2.

За теоремою Вієта знаходимо другий корінь: $-(a+1)-a^2 = a^2+a+1$. Таким чином,

$$x^3+x^2+1 = (x+a)(x+a^2)(x+a^2+a+1).$$

d) Група $(\mathbb{Z}_2(a))^*$ є циклічною групою порядку 7. Число 7 — просте, тому будь-який неодиничний елемент буде твірним. Зокрема, можна взяти $b = a$. Використовуючи побудовану в b) таблицю множення для групи $(\mathbb{Z}_2(a))^*$, отримуємо:

$$a^1 = a, \quad a^2 = a^2, \quad a^3 = a^2+1, \quad a^4 = a^2+a+1,$$
$$a^5 = a+1, \quad a^6 = a^2+a, \quad a^7 = 1.$$

e) Із таблиці множення отримуємо, що

$$\frac{(a+1)(a^2+a+1)}{a^2+1} = \frac{a^2}{a^2+1}.$$

Позначимо значення останнього дробу через xa^2+ya+z. Тоді

$$(xa^2+ya+z)(a^2+1) = a^2. \tag{29}$$

Перемноживши множники лівої частини (29), після зведення подібних членів отримуємо:

$$(y+z)a^2+(x+y)a+(x+y+z) = a^2.$$

Порівнюючи коефіцієнти при степенях a у лівій та правій частині, отримуємо систему

$$y+z = 1, \quad x+y = 0, \quad x+y+z = 0,$$

з якої знаходимо $x = 1$, $y = 1$, $z = 0$. Отже,

$$\frac{(a+1)(a^2+a+1)}{a^2+1} = a^2+a. \qquad \square$$

Задача 11. *Розкладіть на незвідні множники многочлен $f(x)$ над полем $\mathbb{Z}_p$;*
a) $f(x) = x^4+x^3+x+2$, $p = 3$; *b)* $f(x) = x^6+1$, $p = 2$.

Розв'язання. a) Безпосередньо перевіряється, що жоден елемент поля $\mathbb{Z}_3$ не є коренем многочлена $x^4 + x^3 + x + 2$. Тому лінійних множників він не має. Щоб перевірити, чи має цей многочлен множники степеня 2, знайдемо всі незвідні многочлени вигляду $x^2 + ax + b$ над полем $\mathbb{Z}_3$. Многочлен степеня ≤ 3 буде незвідним тоді й лише тоді, коли він не має коренів. Тому незвідні многочлени степеня 2 легко знаходяться за допомогою перебору: $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$. Остаточно отримуємо:

$$x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2).$$

b) Нагадаємо, що в полі характеристики 2 має місце тотожність $(a + b)^2 = a^2 + b^2$. Тому $x^6 + 1 = (x^3 + 1)^2$. Сума кубів розкладається як $x^3 + 1 = (x + 1)(x^2 + x + 1)$. Нарешті, $x^2 + x + 1$ не має коренів у полі $\mathbb{Z}_2$, тому є незвідним. Остаточно отримуємо:

$$x^6 + 1 = (x^3 + 1)^2 = (x + 1)^2(x^2 + x + 1)^2. \qquad \square$$

Задача 12. *Нехай α — корінь многочлена $x^4 + x^3 + 1$ з коефіцієнтами з поля $\mathbb{Z}_2$ і $P = \mathbb{Z}_2(\alpha)$. Знайдіть у полі P всі корені многочлена $f(x) = x^4 + x + 1$.*

Розв'язання. I спосіб. Поле $\mathbb{Z}_2(\alpha)$ складається з елементів вигляду $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$. Безпосередньо перевіряємо, які з них є кореняими $f(x)$. Щоб зменшити об'єм обчислень, зауважимо, що в полі $\mathbb{Z}_2(\alpha)$ має місце тотожність $(a+b)^2 = a^2 + b^2$. Тому для довільного елемента β

$$f(\beta + 1) = (\beta + 1)^4 + (\beta + 1) + 1 = \beta^4 + 1 + \beta + 1 + 1 = \beta^4 + \beta + 1 = f(\beta).$$

Маємо (при обчисленнях використовуємо той факт, що α є коренем многочлена $x^4 + x^3 + 1$, тому $\alpha^4 = \alpha^3 + 1$):

$$f(0) = f(1) = 1 \neq 0, \quad f(\alpha) = f(\alpha + 1) = \alpha^3 + \alpha \neq 0,$$
$$f(\alpha^2) = f(\alpha^2 + 1) = \alpha^3 + \alpha^2 + \alpha + 1 \neq 0,$$
$$f(\alpha^2 + \alpha) = f(\alpha^2 + \alpha + 1) = 0.$$

Таким чином, два корені — $\beta_1 = \alpha^2 + \alpha$ і $\beta_2 = \alpha^2 + \alpha + 1$ — вже маємо. Після ділення $f(x)$ на $(x - \beta_1)(x - \beta_2)$ отримуємо:

$$f(x) = (x - \beta_1)(x - \beta_2)(x^2 + x + \alpha^3 + \alpha).$$

Далі шукаємо корені многочлена $g(x) = x^2 + x + \alpha^3 + \alpha$:

$$g(\alpha^3) = g(\alpha^3 + 1) = \alpha^3 + \alpha^2 + 1 \neq 0,$$
$$g(\alpha^3 + \alpha) = g(\alpha^3 + \alpha + 1) = \alpha^3 + \alpha + 1 \neq 0,$$
$$g(\alpha^3 + \alpha^2) = g(\alpha^3 + \alpha^2 + 1) = 0.$$

Це дає нам ще два корені многочлена $f(x)$: $\beta_3 = \alpha^3 + \alpha^2$ і $\beta_4 = \alpha^3 + \alpha^2 + 1$. Отже, коренями многочлена $f(x)$ будуть елементи $\alpha^2 + \alpha$, $\alpha^2 + \alpha + 1$, $\alpha^3 + \alpha^2$ і $\alpha^3 + \alpha^2 + 1$.

II спосіб. Візьмемо записаний у загальному вигляді з невизначеними коефіцієнтами елемент $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ поля $\mathbb{Z}_2(\alpha)$ і підставимо його у многочлен $f(x)$:

$$(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)^4 + (a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) + 1. \qquad (30)$$

Враховуючи, що в полі $\mathbb{Z}_2$ виконується тотожність $a^2 = a$, а в полі $\mathbb{Z}_2(\alpha)$ — тотожність $(a + b)^2 = a^2 + b^2$, можемо переписати (30) у вигляді

$$a_3\alpha^{12} + a_2\alpha^8 + a_1\alpha^4 + a_0 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 + 1. \qquad (31)$$

Враховуючи, що $\alpha^4 = \alpha^3 + 1$, після послідовного пониження степеня і зведення подібних членів вираз (31) набуває вигляду

$$(a_1 + a_2 + a_3)\alpha^3 + (a_1 + a_2 + a_3)\alpha + (a_1 + a_3 + 1). \qquad (32)$$

Вираз (32) дорівнює 0 тоді й лише тоді, коли всі коефіцієнти при степенях α дорівнюють 0. Це дає систему лінійних рівнянь

$$a_1 + a_2 + a_3 = 0, \quad a_1 + a_3 + 1 = 0$$

із коефіцієнтами з поля $\mathbb{Z}_2$, загальний розв'язок якої має вигляд $a_3 = a_1 + 1$, $a_2 = 1$, a_1 і a_0 — довільні. Це дає 4 корені многочлена $f(x)$: $\alpha^3 + \alpha^2$, $\alpha^3 + \alpha^2 + 1$, $\alpha^2 + \alpha$ і $\alpha^2 + \alpha + 1$. □

Основні задачі

13. Нехай $F \supseteq \mathbb{Q}$ і елемент $c \in F$ є коренем многочлена $f(x) \in \mathbb{Q}[x]$. Доведіть, що для кожного автоморфізму φ поля F елемент $\varphi(a)$ також є коренем многочлена $f(x)$.

14. Знайдіть усі ті автоморфізми поля $\mathbb{C}$, які лишають нерухомими всі дійсні числа.

15. Знайдіть усі автоморфізми поля а) $Q(\sqrt{3})$, b) $Q(\sqrt[3]{2})$, c) $Q(\sqrt[4]{2})$.

16. Знайдіть усі автоморфізми поля розкладу над $\mathbb{Q}$ многочлена а) x^3-2; b) x^4-2.

17. а) Доведіть, що для кожного непарного числа n існує таке розширення $P \supset \mathbb{Q}$ степеня n, що $\mathrm{Aut}(P) = E$.
b) Чи виконується подібне твердження для парних чисел n?

18. Нехай $K \subseteq F$. Чи випливає з рівності $\mathrm{Aut}(F) = E$ рівність $\mathrm{Aut}(K) = E$?

19. Нехай ε_n — первісний корінь степеня n з 1. Доведіть, що група автоморфізмів поля $\mathbb{Q}(\varepsilon_n)$ ізоморфна групі $\mathbb{Z}_n^*$.

20. Наведіть приклад такого поля $F \subseteq \mathbb{C}$, група автоморфізмів якого ізоморфна а) C_2; b) C_4; c) K_4; d) C_6.

21. Доведіть, що кожне розширення степеня 2 є нормальним.

22. Нехай $P \subseteq K \subseteq F$ — вежа скінченних розширень. Які з наступних імплікацій є правильними:
а) розширення $P \subseteq F$ — нормальне $\Rightarrow$ розширення $K \subseteq F$ — нормальне;
b) розширення $P \subseteq K$ і $K \subseteq F$ — нормальні $\Rightarrow$ розширення $P \subseteq F$ — нормальне;
c) розширення $P \subseteq F$ — нормальне $\Rightarrow$ розширення $P \subseteq K$ — нормальне?

23. З'ясуйте, чи буде нормальним розширенням поля $\mathbb{Q}$ поле а) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\sqrt[3]{2})$; c) $\mathbb{Q}(\sqrt[4]{2})$; d) $\mathbb{Q}(\sqrt{2}, i)$; e) $\mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$, де ε_3 — первісний корінь степеня 3 з 1.

24. Знайдіть групу автоморфізмів поля розкладу многочлена $f(x)$ з раціональними коефіцієнтами:
а) $f(x) = x^4 + x^2 + 1$; b) $f(x) = x^4 + 1$.

25. Знайдіть найменше нормальне розширення поля $\mathbb{Q}$, яке б містило поле: а) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\sqrt[3]{2})$; c) $\mathbb{Q}(\sqrt[4]{2})$.

26. Нехай K є полем розкладу деякого многочлена $f(x) \in \mathbb{Q}[x]$. Доведіть, що многочлен f можна взяти незвідним.

27. Нехай p — просте число. Знайдіть усі підполя поля $GF_{p^{11}}$ із p^{11} елементів.

28. Доведіть, що будь–який ненульовий ендоморфізм скінченного поля є автоморфізмом.

29. Чи може скінченне поле бути алгебрично замкненим?

30. Доведіть, що кожне скінченне розширення F скінченного поля P є простим.

31. Доведіть, що скінченне поле F є нормальним розширенням кожного свого підполя $P \subseteq F$.

32. a) Доведіть, що многочлен $f(x) = x^3+x+1$ незвідний над полем $\mathbb{Z}_2$.
b) Побудуйте таблицю множення поля $\mathbb{Z}_2(a)$, де a — корінь многочлена $f(x)$.
c) Розкладіть над цим полем многочлен $f(x)$ на лінійні множники.
d) Знайдіть який–небудь твірний елемент a групи $(\mathbb{Z}_3(a))^*$ і подайте інші елементи групи P^* у вигляді степенів a.
e) Обчисліть у полі $\mathbb{Z}_2(a)$ значення виразу $\dfrac{(a+1)(a^2+a)}{a^2+a+1}$.

33. a) Доведіть, що многочлен $f(x) = x^2+1$ є незвідним над полем $\mathbb{Z}_3$.
b) Побудуйте таблицю множення поля $\mathbb{Z}_3(a)$, де a — корінь многочлена $f(x)$.
c) Знайдіть усі твірні елементи мультиплікативної групи цього поля.
d) Розкладіть над цим полем на незвідні множники многочлени x^2+1, x^2+x+1 і x^2+2x+2.

34. Доведіть, що многочлен $f(x)$ є незвідним над полем P. Побудуйте таблицю множення для поля $P(\alpha)$, де α — корінь многочлена $f(x)$. Знайдіть усі твірні елементи циклічної групи P^*. Розкладіть над полем $P(\alpha)$ на незвідні множники многочлени $g(x)$ і $h(x)$.

a) $P = \mathbb{Z}_2$, $f(x) = x^3+x^2+1$, $g(x) = x^4+x^2+1$, $h(x) = x^3+x+1$;

b) $P = \mathbb{Z}_2$, $f(x) = x^3+x+1$, $g(x) = x^4+x^3+x+1$, $h(x) = x^3+x^2+1$;

c) $P = \mathbb{Z}_3$, $f(x) = x^2+x+2$, $g(x) = x^4+2x^3+2x^2+1$, $h(x) = x^2+2x+2$;

d) $P = \mathbb{Z}_3$, $f(x) = x^2+2x+2$, $g(x) = x^4+2x^2+2x+1$, $h(x) = x^2+1$.

35. Вкажіть явно який-небудь ізоморфізм між полями $\mathbb{Z}_3(a)$ і $\mathbb{Z}_3(b)$, де a і b — корені многочленів $f(x)$ і $g(x)$ із $\mathbb{Z}_3[x]$ відповідно:
a) $f(x) = x^2 + x + 2$, $g(x) = x^2 + 1$;
b) $f(x) = x^3 + 2x + 2$, $g(x) = x^3 + 2x^2 + 1$.
Скількома способами можна встановити такий ізоморфізм?

36. Нехай a — корінь многочлена $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Розв'яжіть у полі $\mathbb{Z}_2(a)$ систему рівнянь

$$\begin{array}{rcrcl} ax_1 & + & (a+1)x_2 & = & 1\,, \\ (a+1)x_1 & + & ax_2 & = & 0\,. \end{array}$$

37. Знайдіть над полем $\mathbb{Z}_2$ усі незвідні многочлени степенів a) 3, b) 4.

38. Знайдіть над полем $\mathbb{Z}_2$ кількість незвідних многочленів степеня a) 5; b) 6; c) 7.

39. Чи буде незвідним над полем $\mathbb{Z}_5$ многочлен a) $x^3 + x - 1$; b) $x^4 + 3x^3 + 3x^2 + 3x + 3$?

40. Знайдіть над полем GF_9 кількість незвідних унітарних многочленів степеня a) 2; b) 3; c) 4.

41. Розкладіть на незвідні множники многочлен $f(x)$ над полем $\mathbb{Z}_p$:
a) $f(x) = x^4 + 2x^2 + 2x + 2$, $p = 3$;
b) $f(x) = x^3 + 2x^2 + 4x + 1$, $p = 5$;
c) $f(x) = x^3 + 4x^2 + 2x + 1$, $p = 5$.

42. Нехай α — корінь многолена $x^4 + x^3 + 1$ з коефіцієнтами з поля $\mathbb{Z}_2$ і $P = \mathbb{Z}_2(\alpha)$. Знайдіть у полі P всі корені многочлена a) $x^4 + x^3 + 1$; b) $x^4 + x^3 + x^2 + x + 1$.

Додаткові задачі

43.* Знайдіть усі неперервні автоморфізми поля $\mathbb{C}$.

44. Наведіть приклад такого поля $F \subseteq \mathbb{C}$, група автоморфізмів якого ізоморфна a) S_3; b) C_3; c) C_5.

45. Опишіть із точністю до ізоморфізму всі можливі групи автоморфізмів полів розкладу незвідних многочленів третього степеня з раціональними коефіцієнтами.

46. Нехай p — просте число. Знайдіть групу автоморфізмів поля розкладу многочлена $f(x) = \dfrac{x^p - 1}{x - 1} \in \mathbb{Q}[x]$.

47. Знайдіть групу автоморфізмів простого трансцендентного розширення $P(t) \supset P$.

48. Нехай $\mathbb{Q} \subseteq K \subset \mathbb{C}$ і розширення $\mathbb{Q} \subseteq K$ є нормальним. Доведіть, що коли степінь розширення $\mathbb{Q} \subseteq K$ є непарним числом, то $K \subseteq \mathbb{R}$.

49. Знайдіть групу автоморфізмів поля розкладу многочлена $x^5 + 1$.

50.* Нехай $f(x) \in P[x]$ незвідний многочлен і $K \supseteq P$ — нормальне розширення. Доведіть, що над K многочлен $f(x)$ розкладається на незвідні множники однакового степеня.

51. Нехай P — поле розкладу многочлена $x^n - 1 \in \mathbb{Q}[x]$. Знайдіть степінь розширення $P \supseteq \mathbb{Q}$.

52. Доведіть, що над полем P характеристики $p > 0$ для многочлена $x^p - a$ є лише дві можливості: або бути незвідним, або бути p–м степенем лінійного многочлена.

53. Нехай $P = \mathbb{Z}_p(t)$ — трансцендентне розширення поля $\mathbb{Z}_p$.
a) Доведіть, що многочлен $f(x) = x^p - t$ є незвідним над полем P.
b) Нехай a — корінь многочлена $f(x)$. Розкладіть $f(x)$ на незвідні множники над полем $P(a)$.

54. a) Доведіть, що для многочленів $f(x) \in \mathbb{Z}_p[x]$ виконується *тотожність Шенемана* $f^p(x) = f(x^p)$.
b) Чи можна поле $\mathbb{Z}_p$ замінити довільним полем характеристики p?

55. Доведіть, що мультиплікативна група поля F буде циклічною тоді й лише тоді, коли F — скінченне поле.

56. Нехай p — просте число. Доведіть, що коли степінь многочлена $f(x) \in \mathbb{Z}_p[x]$ не перевищує $p - 2$, то $\sum_{a \in \mathbb{Z}_p} f(a) = 0$.

57. a) Доведіть, що всі елементи поля GF_{2^n} є квадратами.
b) Нехай GF_q — поле непарного порядку q. Доведіть, що квадрати утворюють у групі GF_q^* підгрупу H індекса 2.

58. Нехай GF_{p^n} і GF_{p^m} містяться в деякому скінченному полі P. Знайдіть порядок a) поля $GF_{p^n} \cap GF_{p^m}$; b) найменшого підполя, яке містить GF_{p^n} і GF_{p^m}.

59. Нехай GF_{p^n} — скінченне поле порядку p^n. Доведіть, що
a) відображення $\varphi_F : GF_{p^n} \to GF_{p^n}$, $x \mapsto x^p$, є автоморфізмом поля GF_{p^n} (т.зв. *автоморфізм Фробеніуса*);
b) група $\mathrm{Aut}(GF_{p^n})$ автоморфізмів поля GF_{p^n} є циклічною порядку n і породжується автоморфізмом Фробеніуса φ_F.

60. Знайдіть над полем GF_q кількість незвідних унітарних многочленів степеня a) 2; b) 3; c) 4.

61. Знайдіть над полем $\mathbb{Z}_2$ кількість незвідних многочленів степеня a) 10; b) 11; c) 12.

62. Доведіть, що для довільних простого числа p і натуральних n і k знайдеться многочлен $f(x) \in GF_{p^n}$ степеня k, який буде незвідним над полем GF_{p^n}.

63. Доведіть, що многочлен $f(x) \in \mathbb{Z}_p[x]$ має корені в $\mathbb{Z}_p$ тоді й лише тоді, коли $\mathrm{НСД}(f(x), x^p - x) \neq 1$.

64. Доведіть, що множина всіх тих $a \in GF_{p^n}$, для яких многочлен $x^p + x + a$ має корінь у полі GF_{p^n}, є векторним простором над полем GF_p. Знайдіть його розмірність.

65.* Доведіть, що многочлен x^4+1 буде звідним над кожним скінченним полем.

66.* Нехай $c_n(q)$ — ймовірність того, що випадково вибрана матриця порядку n над скінченним полем порядку q є невиродженою. Обчисліть $c_n(q)$ і доведіть, що границя $c(q) = \lim\limits_{n\to\infty} c_n(q)$ існує і є додатною.

67. (*Теорема Вільсона*) Нехай $f(x)$ — незвідний многочлен степеня n із $\mathbb{Z}_p[x]$, а $h(x) = g_1(x)g_2(x)\cdots g_{p^n-1}(x)$ — добуток усіх ненульових многочленів із $\mathbb{Z}_p[x]$ степеня $< n$. Доведіть, що остача від ділення $h(x)$ на $f(x)$ дорівнює -1.

68. a) Доведіть, що у тривимірному векторному просторі GF_q^3 не можна вибрати $q+3$ вектори так, щоб кожні три з них були лінійно незалежними.

b)* Доведіть, що коли q — парне, то в тривимірному векторному просторі GF_q^3 можна вибрати $q+2$ векторів так, щоб кожні три з них були лінійно незалежними.

c)** Нехай q — непарне. Яку найбільшу кількість векторів можна вибрати у тривимірному векторному просторі GF_q^3 так, щоб кожні три з них були лінійно незалежними?

69. Нехай $f(x) \in \mathbb{Z}_p[x]$ — нормований незвідний многочлен степеня n і a — його корінь у деякому розширенні $P \supset \mathbb{Z}_p$.

a) Доведіть, що $f(x)$ розкладається над полем P на лінійні множники і знайдіть цей розклад.

b) Доведіть, що всі корені многочлена $f(x)$ в полі P мають однаковий порядок як елементи мультиплікативної групи P^*.

70. Нехай $\mathbb{F}$ — алгебрично замкнене поле характеристики p. Доведіть, що для кожного $n \geq 1$ воно містить єдине підполе порядку p^n.

71.*** Нехай F — скінченне поле і $n \geq 2$. Доведіть, що кількість нормованих многочленів степеня n із $F[x]$, які розкладаються в добуток парної кількості попарно різних незвідних многочленів, дорівнює кількості тих нормованих многочленів степеня n із $F[x]$, які розкладаються в добуток непарної кількості попарно різних незвідних многочленів.

Домашнє завдання

72. Знайдіть усі автоморфізми поля розкладу над $\mathbb{Q}$ многочлена $(x^2-2)(x^2-3)$.

73. Нехай ε_n — первісний корінь степеня n з 1. Знайдіть групу автоморфізмів поля a) $\mathbb{Q}(\varepsilon_7)$; b) $\mathbb{Q}(\varepsilon_9)$.

74. З'ясуйте, чи буде нормальним розширенням поля $\mathbb{Q}$ поле: a) $\mathbb{Q}(\sqrt[3]{3})$; b) $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

75. Обчисліть добуток усіх ненульових елементів поля GF_q.

76. a) Побудуйте таблицю множення поля $\mathbb{Z}_2(a)$, де a — корінь многочлена $x^3+x+1 \in \mathbb{Z}_2[x]$.
b) Розкладіть над цим полем на незвідні множники многочлени x^3+x+1 і x^3+x^2+1.
c) Знайдіть у мультиплікативній групі поля $\mathbb{Z}_2(a)$ порядок елемента $c = a^2+a+1$.
d) Вкажіть явно який-небудь ізоморфізм між полями $\mathbb{Z}_2(a)$ і $\mathbb{Z}_2(b)$, де a і b — корені многочленів x^3+x+1 і x^3+x^2+1 відповідно.

77. Нехай a — корінь многочлена $x^2+1 \in \mathbb{Z}_3[x]$. Обчисліть у полі $\mathbb{Z}_3(a)$ визначник $\begin{vmatrix} a+1 & a & a \\ a & a+1 & a \\ a & a & a+1 \end{vmatrix}$.

78. Знайдіть полем $\mathbb{Z}_3$ усі незвідні многочлени степеня 3 зі старшим коефіцієнтом 1.

79. Розкладіть многочлен $x^5 + x^3 + x^2 + 1$ з коефіцієнтами з поля $\mathbb{Z}_2$ на незвідні множники.

80. Нехай α — корінь многолена $x^4 + x^3 + 1$ з коефіцієнтами з поля $\mathbb{Z}_2$ і $P = \mathbb{Z}_2(\alpha)$. Знайдіть у полі P всі корені многочлена $x^2 + x + 1$.

Заняття 7. Алгебричні, трансцендентні та конструктивні числа

Необхідні поняття. Комплексне число z називається *алгебричним*, якщо воно є коренем деякого многочлена $f(x)$ з раціональними коефіцієнтами. Без обмеження загальності можна вважати, що $f(x)$ має цілі коефіцієнти (у противному разі можна помножити $f(x)$ на найменше спільне кратне знаменників його коефіцієнтів).

Комплексні числа, які не є алгебричними, називаються *трансцендентними*.

Якщо z — алгебричне число, то многочлен найменшого степеня із $\mathbb{Q}[x]$, для якого z є коренем, називається *мінімальним многочленом* числа z. Степінь цього мінімального многочлена називається *степенем* алгебричного числа z.

z називається *цілим алгебричним числом*, якщо z є коренем нормованого многочлена з цілими коефіцієнтами.

Якщо точку, яка відповідає комплексному числу z, можна побудувати за допомогою циркуля й лінійки з точок, що відповідають числам $z_1, z_2, \ldots, z_n$, то кажуть, що z є *побудовним* (або *конструйовним*) з чисел $z_1, z_2, \ldots, z_n$.

Число $z \in \mathbb{C}$ називається *конструктивним*, якщо його можна побудувати з числа 1.

Розширення $F \supseteq P$ поля $P = \mathbb{Q}(z_1, \ldots, z_n)$ називається *піфагоровим*, якщо існують такі проміжні підполя

$$P = P_0 \subset P_1 \subset P_2 \subset \cdots \subset P_k = F,$$

що степінь кожного розширення $P_{i-1} \subset P_i$, $i = 1, 2, \ldots, k$, не перевищує 2.

Необхідні твердження. **1.** Множина $\mathbb{A}$ алгебричних чисел утворює поле.

2. Числа e і π є трансцендентними.

3. Многочлен $f(x)$ ненульового степеня із цілими коефіцієнтами буде незвідним у кільці $\mathbb{Z}[x]$ тоді й лише тоді, коли він буде незвідним над полем раціональних чисел $\mathbb{Q}$.

4. Теорема Ліувілля Для кожного дійсного алгебричного числа a степеня $k > 1$ існує така додатна константа $c = c(a)$, що для кожного раціонального числа m/n виконується нерівність $\left|\dfrac{m}{n} - a\right| > \dfrac{c}{n^k}$.

5. Комплексне число $z = a + bi$ є побудовним тоді й лише тоді, коли є побудовними дійсні числа a і b.

6. Основна теорема про геометричні побудови. Нехай точкам $A_1, \ldots, A_n, B$ площини відповідають комплексні числа $z_1, \ldots, z_n, z$. Точка B є побудовною з точок $A_1, \ldots, A_n$ тоді й лише тоді, коли z належить деякому піфагоровому розширенню поля $P = \mathbb{Q}(z_1, \ldots, z_n)$.

7. Степінь кожного піфагорового розширення $\mathbb{Q}(z_1, \ldots, z_n) \supseteq \mathbb{Q}$ є степенем числа 2.

8. Якщо числа a і b — побудовні, то числа $a \pm b$, $a \cdot b$, a/b, $\sqrt{a}$ — також побудовні.

9. За допомогою циркуля та лінійки не можна виконати трисекцію кута 60°. Зокрема, кут 20° не є побудовним.

10. Теорема Ґауса. Правильний n–кутник можна побудувати за допомогою циркуля та лінійки тоді й лише тоді, коли n має вигляд $n = 2^k p_1 \cdots p_m$, де $p_1, \ldots, p_m$ — попарно різні прості числа Ферма.

Приклади розв'язання типових задач

Задача 1. *Чи буде дане число алгебричним? Якщо буде, то вкажіть многочлен з цілими коефіцієнтами, для якого це число буде коренем*: *a)* $\sqrt{3} + \sqrt[6]{3}$; *b)* $1 + \sqrt{\pi}$; *c)* $1 + \sqrt{2} + \sqrt{4} + \sqrt{8} + \cdots + \sqrt{2^n}$.

Розв'язання. a) Із ланцюжка імплікацій

$$x = \sqrt{3} + \sqrt[6]{3} \Rightarrow (x - \sqrt{3})^3 = \sqrt{3} \Rightarrow x^3 + 9x = \sqrt{3}(3x^2 + 4) \Rightarrow$$
$$\Rightarrow (x^3 + 9x)^2 = 3(3x^2 + 4)^2 \Rightarrow x^6 - 9x^4 + 9x^2 - 48 = 0.$$

випливає, що число $\sqrt{3} + \sqrt[6]{3}$ є коренем многочлена $x^6 - 9x^4 + +9x^2 - 48$ з цілими коефіцієнтами. Отже, воно є алгебричним. Навіть більше, воно є цілим алгебричним, бо старший коефіцієнт многочлена дорівнює 1.

b) Якби число $a = 1 + \sqrt{\pi}$ було алгебричним, то алгебричним було б і число $(a - 1)^2 = \pi$. Але це не так.

c) Розглянемо два випадки:

1) n — парне: $n = 2k$. Тоді

$$1 + \sqrt{2} + \sqrt{4} + \sqrt{8} + \cdots + \sqrt{2^n} =$$
$$= (1 + 2 + \cdots + 2^k) + \sqrt{2}(1 + 2 + \cdots + 2^{k-1}) =$$
$$= (2^{k+1} - 1) + \sqrt{2}(2^k - 1).$$

Із ланцюжка імплікацій

$$x = (2^{k+1}-1) + \sqrt{2}(2^k-1) \Rightarrow x - (2^{k+1}-1) = \sqrt{2}(2^k-1) \Rightarrow$$
$$\Rightarrow \left(x - (2^{k+1}-1)\right)^2 = \left(\sqrt{2}(2^k-1)\right)^2 \Rightarrow$$
$$\Rightarrow x^2 - (2^{k+2}-2)x + 2^{k+2} - 2^{k+1} - 1 = 0$$

випливає, що число $1+\sqrt{2}+\sqrt{4}+\sqrt{8}+\cdots+\sqrt{2^{2k}}$ є коренем многочлена $x^2 - (2^{k+2}-2)x + 2^{k+2} - 2^{k+1} - 1$ з цілими коефіцієнтами.

2) n — непарне: $n = 2k-1$. Тоді

$$1 + \sqrt{2} + \sqrt{4} + \sqrt{8} + \cdots + \sqrt{2^n} =$$
$$= (1 + 2 + \cdots + 2^{k-1}) + \sqrt{2}(1 + 2 + \cdots + 2^{k-1}) =$$
$$= (2^k - 1) + \sqrt{2}(2^k - 1).$$

Із ланцюжка імплікацій

$$x = (2^k-1) + \sqrt{2}(2^k-1) \Rightarrow x - (2^k-1) = \sqrt{2}(2^k-1) \Rightarrow$$
$$\Rightarrow \left(x - (2^k-1)\right)^2 = \left(\sqrt{2}(2^k-1)\right)^2 \Rightarrow$$
$$\Rightarrow x^2 - (2^{k+1}-2)x - 2^{2k+1} + 2^{2k} + 2^{k+2} - 2^{k+1} - 1 = 0$$

випливає, що число $1+\sqrt{2}+\sqrt{4}+\sqrt{8}+\cdots+\sqrt{2^{2k-1}}$ є коренем многочлена $x^2 - (2^{k+1}-2)x - 2^{2k+1} + 2^{2k} + 2^{k+2} - 2^{k+1} - 1$ з цілими коефіцієнтами. □

Задача 2. *Знайдіть мінімальний многочлен числа*
а) $\varepsilon = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$; *б)* $\sqrt[3]{2-\sqrt{3}} + 1$.

Розв'язання. а) Позаяк $\varepsilon^5 = 1$ і $\varepsilon \neq 1$, то ε є коренем многочлена

$$f(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

Анулюючий многочлен є мінімальним тоді, коли він незвідний. Щоб довести незвідність $f(x)$, зробимо заміну $x = y + 1$. Тоді

$$g(y) = f(y+1) = \frac{(y+1)^5 - 1}{y} =$$
$$= y^4 + \binom{5}{1}y^3 + \binom{5}{2}y^2 + \binom{5}{3}y + \binom{5}{4} = y^4 + 5y^3 + 10y^2 + 10y + 5.$$

Многочлен $g(y) = y^4 + 5y^3 + 10y^2 + 10y + 5$ є незвідним за ознакою Айзенштайна (для простого числа $p = 5$). Але многочлени $f(x)$ і $g(y) = f(y+1)$ є звідними/незвідними одночасно. Тому $f(x)$ також незвідний і є мінімальним для ε.

b) Маємо такий ланцюжок імплікацій:

$$\begin{aligned} x = \sqrt[3]{2-\sqrt{3}} + 1 \Rightarrow x - 1 = \sqrt[3]{2-\sqrt{3}} \Rightarrow (x-1)^3 = 2 - \sqrt{3} \Rightarrow \\ \Rightarrow (x-1)^3 - 2 = -\sqrt{3} \Rightarrow \big((x-1)^3 - 2\big)^2 = 3 \Rightarrow \\ \Rightarrow x^6 - 6x^5 + 15x^4 - 24x^3 + 27x^2 - 18x + 6 = 0. \end{aligned}$$

Многочлен $x^6 - 6x^5 + 15x^4 - 24x^3 + 27x^2 - 18x + 6$ є незвідним за ознакою Айзенштайна (для числа 3). Тому він є мінімальним для числа $\sqrt[3]{2-\sqrt{3}} + 1$. □

Задача 3.

Доведіть, що коли число a — раціональне, то числа $\cos a\pi$ і $\sin a\pi$ — алгебричні.

Розв'язання. Нехай $a = \dfrac{m}{n}$. Візьмемо число $z = \cos\dfrac{m}{n}\pi + i\sin\dfrac{m}{n}\pi$ і піднесемо його до степеня $2n$. Якщо це робити за формулою Муавра, то отримаємо:

$$z^{2n} = \cos 2m\pi + i\sin 2m\pi = 1. \tag{33}$$

Із другого боку, за формулою бінома Ньютона маємо:

$$z^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \Big(\cos\frac{m}{n}\pi\Big)^k \Big(i\sin\frac{m}{n}\pi\Big)^{2n-k}. \tag{34}$$

Прирівнюючи дійсні частини правих частин рівностей (33) і (34), отримуємо:

$$\sum_{k=0}^{n} \binom{2n}{2k} \Big(\cos\frac{m}{n}\pi\Big)^{2k} \Big(i\sin\frac{m}{n}\pi\Big)^{2n-2k} = 1. \tag{35}$$

Враховуючи, що $i^2 = -1$ та $\sin^2\dfrac{m}{n}\pi = 1 - \cos^2\dfrac{m}{n}\pi$, із (35) отримуємо:

$$\sum_{k=0}^{n} \binom{2n}{2k} \Big(\cos\frac{m}{n}\pi\Big)^{2k} (-1)^{n-k} \Big(1 - \cos^2\frac{m}{n}\pi\Big)^{n-k} = 1.$$

Отже, число $\cos\dfrac{m}{n}\pi$ є коренем многочлена

$$\sum_{k=0}^{n}\binom{2n}{2k}x^{2k}(-1)^{n-k}(1-x^2)^{n-k}-1$$

із цілими коефіцієнтами, а тому є алгебричним. Із алгебричності $\cos\dfrac{m}{n}\pi$ у свою чергу випливає алгебричність числа $\sqrt{1-\cos^2\dfrac{m}{n}\pi}$, а тим самим і числа $\sin\dfrac{m}{n}\pi$. □

Задача 4. *Позбавтеся від ірраціональностей у знаменнику*:
a) $\dfrac{1}{1+\sqrt{2}+3\sqrt{3}}$; *b*) $\dfrac{1}{1+2\sqrt[3]{2}-\sqrt[3]{4}}$.

Розв'язання. a) Позаяк знаменник містить лише ірраціональності степеня 2, то можна користуватися "шкільним" методом — домножанням чисельника і знаменника на число, спряжене до знаменника:

$$\frac{1}{1+\sqrt{2}+3\sqrt{3}}=\frac{1+\sqrt{2}-3\sqrt{3}}{(1+\sqrt{2}+3\sqrt{3})(1+\sqrt{2}-3\sqrt{3})}=$$
$$=\frac{1+\sqrt{2}-3\sqrt{3}}{(1+\sqrt{2})^2-27}=$$
$$=\frac{1+\sqrt{2}-3\sqrt{3}}{2\sqrt{2}-24}=\frac{(1+\sqrt{2}-3\sqrt{3})(2\sqrt{2}+24)}{(2\sqrt{2}-24)(2\sqrt{2}+24)}=$$
$$=\frac{-28-26\sqrt{2}+72\sqrt{3}+6\sqrt{6}}{568}=\frac{1}{284}(-14-13\sqrt{2}+36\sqrt{3}+3\sqrt{6}).$$

b) Скористаємося методом невизначених коефіцієнтів: число $\dfrac{1}{1+2\sqrt[3]{2}-\sqrt[3]{4}}$ належить полю $\mathbb{Q}(\sqrt[3]{2})$, тому воно має вигляд $x+y\sqrt[3]{2}+z\sqrt[3]{4}$, де x, y, z — раціональні числа. Звідси отримуємо:

$$1=(1+2\sqrt[3]{2}-\sqrt[3]{4})(x+y\sqrt[3]{2}+z\sqrt[3]{4})=$$
$$=(x-2y+4z)+(2x+y-2z)\sqrt[3]{2}+(-x+2y+z)\sqrt[3]{4}.$$

Числа 1, $\sqrt[3]{2}$ і $\sqrt[3]{4}$ лінійно незалежні над полем $\mathbb{Q}$, тому коефіцієнти при цих числах у лівій і правій частинах отриманої рівності мають бути

однаковими. Порівнюючи ці коефіцієнти, отримуємо систему лінійних рівнянь

$$\begin{aligned} x - 2y + 4z &= 1, \\ 2x + y - 2z &= 0, \\ -x + 2y + z &= 0. \end{aligned}$$

Розв'язуючи її, знаходимо: $x = 1/5$, $y = 0$, $z = 1/5$. Отже

$$\frac{1}{1 + 2\sqrt[3]{2} - \sqrt[3]{4}} = \frac{1}{5} + \frac{1}{5}\sqrt[3]{4} = \frac{1 + \sqrt[3]{4}}{5}. \qquad \square$$

Задача 5. *Доведіть, що для кожного алгебричного числа a існує таке натуральне число k, що число ka є цілим алгебричним.*

Розв'язання. Нехай a — корінь многочлена $x^n + c_1x^{n-1} + \cdots + c_n$ із раціональними коефіцієнтами і k — найменший спільний знаменник коефіцієнтів $c_1, \ldots, c_n$. Тоді

$$\begin{gathered} k^n(x^n + c_1x^{n-1} + \cdots + c_n) = \\ = (kx)^n + kc_1(kx)^{n-1} + k^2c_2(kx)^{n-2} + \cdots + k^{n-1}c_{n-1}(kx) + k^nc_n = \\ = (kx)^n + A_1(kx)^{n-1} + \cdots + A_{n-1}(kx) + A_n, \end{gathered}$$

де коефіцієнти $A_m = k^mc_m$ є цілими. Але тоді з рівності

$$k^n(x^n + c_1x^{n-1} + \cdots + c_n) = 0$$

випливає, що

$$(ka)^n + A_1(ka)^{n-1} + \cdots + A_{n-1}(ka) + A_n = 0.$$

Отже, число ka є коренем нормованого многочлена

$$y^n + A_1y^{n-1} + \cdots + A_{n-1}y + A_n$$

із цілими коефіцієнтами, а тому є цілим алгебричним. $\square$

Задача 6. *Доведіть трансцендентність числа* $a = \sum\limits_{n=1}^{\infty} \dfrac{1}{2^{n!}}$.

Розв'язання. Якщо число a записати у двійковій системі числення, то на місцях із номерами $1!, 2!, \ldots, n!, \ldots$ стоятимуть одиниці, а на інших місцях — нулі. Довжини проміжків із нулів дорівнюють $n! - (n-1)! - 1$

і стають як завгодно великими, якщо n зростає. Тому двійковий дріб для числа a не є періодичним і число a не є раціональним.

Припустимо тепер, що a є алгебричним числом степеня $k > 1$. Тоді за теоремою Ліувілля існує така додатна константа c, що для кожного раціонального числа m/n виконується нерівність $\left|\frac{m}{n} - a\right| > \frac{c}{n^k}$. Зокрема, для раціонального числа $\frac{d_n}{2^{n!}} = \sum\limits_{i=1}^{n} \frac{1}{2^{i!}}$ має виконуватися нерівність

$$\left|\frac{d_n}{2^{n!}} - a\right| > \frac{c}{(2^{n!})^k} = \frac{c}{2^{kn!}}. \tag{36}$$

Із другого боку,

$$\left|\frac{d_n}{2^{n!}} - a\right| = \sum_{i=n+1}^{\infty} \frac{1}{2^{i!}} < \sum_{j=2^{n+1}}^{\infty} \frac{1}{2^j} = \frac{1}{2^{(n+1)!-1}}. \tag{37}$$

Із (36) і (37) випливає, що для всіх n має виконуватися нерівність

$$\frac{1}{2^{(n+1)!-1}} > \frac{c}{2^{kn!}},$$

яка рівносильна нерівності

$$\frac{1}{c} > 2^{(n+1-k)n!-1}.$$

Отже, послідовність $b_n = 2^{(n+1-k)n!-1}$ має бути обмежена згори числом $1/c$. Але при фіксованому k послідовність b_n є необмежено зростаючою. Отримана суперечність доводить, що число a є трансцендентним. □

Задача 7. *Доведіть, що кут* a) $1°$; b) $19°$ *не є побудовним.*

Розв'язання. a) Якби кут $1°$ був побудовним, то для кожного натурального числа n був би побудовним кут $n°$. Але за твердженням **9** кут $20°$ не є побудовним. Тому не є побудовним і кут $1°$.

b) Якби кут $19°$ був побудовним, то був би побудовним і кут $19 \cdot 19° = 361°$, тобто кут $1°$. Але в попередньому пункті доведено, що він не є побудовним. Отже, не є побудовним і кут $19°$. □

Задача 8. *Чи можна за допомогою циркуля та лінійки побудувати ребро куба, рівновеликого даному правильному тетраедру?*

Розв'язання. Легко підрахувати, що об'єм правильного тетраедра з ребром 1 дорівнює $\dfrac{1}{6\sqrt{2}}$. Ребро куба, рівновеликого цьому тетраедру, дорівнює $\sqrt[3]{\dfrac{1}{6\sqrt{2}}} = \dfrac{1}{\sqrt[3]{6\sqrt{2}}}$. Тому задача зводиться до побудови за допомогою циркуля та лінійки числа $\dfrac{1}{\sqrt[3]{6\sqrt{2}}}$. Остання задача рівносильна побудові за допомогою циркуля та лінійки числа $\sqrt[3]{6\sqrt{2}}$.

Розглянемо розширення $\mathbb{Q}(\sqrt[3]{6\sqrt{2}}) \supset \mathbb{Q}$. Позаяк $(\sqrt[3]{6\sqrt{2}})^3 = 6\sqrt{2}$, то $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{6\sqrt{2}})$. Звідси у свою чергу випливає, що $\dfrac{\sqrt[3]{6\sqrt{2}}}{\sqrt{2}} = \sqrt[3]{3}$ також належить полю $\mathbb{Q}(\sqrt[3]{6\sqrt{2}})$. Отже, $\mathbb{Q}(\sqrt[3]{6\sqrt{2}}) \supset \mathbb{Q}(\sqrt[3]{3}, \sqrt{2})$. Зворотне включення очевидне, тому $\mathbb{Q}(\sqrt[3]{6\sqrt{2}}) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{2})$. Це дає вежу розширень

$$\mathbb{Q}(\sqrt[3]{3}, \sqrt{2}) \supseteq \mathbb{Q}(\sqrt[3]{3}) \supset \mathbb{Q}.$$

Число $\sqrt[3]{3}$ є коренем незвідного над $\mathbb{Q}$ многочлена $x^3 - 3$, тому $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$. Але тоді степінь розширення $\mathbb{Q}(\sqrt[3]{3}, \sqrt{2}) \supset \mathbb{Q}$ ділиться на 3 і це розширення не є піфагоровим. Тому побудувати за допомогою циркуля та лінійки ребро куба, рівновеликого даному правильному тетраедру, не можна. □

Основні задачі

9. Доведіть, що для довільних алгебричного числа a і натурального числа n число $b = \sqrt[n]{a}$ також буде алгебричним.

10. Доведіть, що для довільних раціональних чисел a, b, c число $a + b\sqrt{c}$ буде алгебричним. Яким буде його степінь?

11. З'ясуйте, які з наступних чисел є алгебричними, а які — трансцендентними:

a) $1 + \sqrt{2} + \sqrt{3}$; b) $1 + \sqrt[3]{5} - i\sqrt{3}$; c) $\dfrac{1-i}{2+\sqrt{\pi}}$;

d) $\sqrt{1 + \sqrt{2 + \sqrt{3 + \cdots + \sqrt{n}}}}$; e) $\sqrt{1 + \sqrt{1 + \sqrt{1 + \cdots + \sqrt{e}}}}$.

12. Побудуйте многочлен з цілими коефіцієнтами, для якого дане число буде коренем: a) $\sqrt{7} - \sqrt{5}$; b) $\sqrt{3} + 2\sqrt{2}$; c) $2i - \sqrt{2}$.

13. Знайдіть мінімальний многочлен числа: a) $\sqrt{2}+\sqrt{3}$; b) $i+2\sqrt{2}$; c) $\sqrt{3}+\sqrt[6]{3}$; d) $\sqrt{2}-i\sqrt{3}$; e) $\sqrt[3]{2-\sqrt{3}}+1$; f) $\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$; g) ε — первісний корінь степеня p з 1, де p — просте число.

14. Доведіть, що комплексні числа z і $\overline{z}$ або обидва алгебричні, або обидва трансцендентні.

15. Доведіть, що комплексне число $a+bi$ буде алгебричним тоді й лише тоді, коли алгебричними будуть дійсні числа a і b.

16. Позбавтеся від ірраціональностей у знаменнику:
a) $\dfrac{1}{2+\sqrt{2}-\sqrt{3}}$; b) $\dfrac{1+\sqrt{2}}{1+\sqrt{2}+3\sqrt{3}}$; c) $\dfrac{1}{1-\sqrt[3]{2}+\sqrt[3]{4}}$;
d) $\dfrac{1}{1+2\sqrt[3]{2}+\sqrt[3]{4}}$; e) $\dfrac{1}{1-\sqrt[3]{2}+2\sqrt[3]{4}}$; f) $\dfrac{1}{1+\sqrt[3]{3}+\sqrt[3]{9}}$.

17. Які з раціональних чисел є цілими алгебричними числами?

18. З'ясуйте, які з наступних чисел є цілими алгебричними числами: a) $\sqrt{2}$; b) $\sqrt{2}+\sqrt{3}$; c) $\frac{1+\sqrt{5}}{2}$; d) $\frac{2+\sqrt{5}}{2}$; e) $\frac{\sqrt{5}+\sqrt{13}}{2}$; f) $\frac{\sqrt[3]{2}}{2}$; g) $\sqrt{\frac{3-\sqrt{-3}}{2}}$.

19. Доведіть ірраціональність числа e.

20. Спираючись на трансцендентність числа e, доведіть трансцендентність числа $a=\sum\limits_{k=0}^{\infty}\dfrac{1}{(2k)!}$.

21. Доведіть, що кут a) 18°, b) 12°, c) 6°, d) 3° є побудовним.

22. Які з кутів $k°$, де k — ціле число з проміжку $[1,20]$, є побудовними?

23. Доведіть, що за допомогою циркуля та лінійки можна побудувати правильний 5-кутник.

24. Чи можна допомогою циркуля та лінійки побудувати правильний 9–кутник?

25. Доведіть, що за допомогою циркуля та лінійки для кожного трикутника можна побудувати рівновеликий йому квадрат.[1]

[1]Досить громіздку конструкцію побудови потрібного квадрата можна одержати безпосередньо з формули Герона.

26. Доведіть, що за допомогою циркуля та лінійки можна побудувати рівнобедрений трикутник, в якого центри вписаного й описаного кіл симетричні відносно основи трикутника.

27. Доведіть, що кожна пряма координатної площини або взагалі не містить конструктивних точок, або містить рівно одну таку точку, або містить нескінченно багато таких точок. Наведіть відповідні приклади.

Додаткові задачі

28. Наведіть приклад таких алгебричних чисел степенів 2 і 3 відповідно, добуток яких є алгебричним числом степеня а) 6; b) 3.

29. Знайдіть многочлен найменшого степеня з цілими коефіцієнтами, коренем якого є довжина сторони правильного 14–кутника, вписаного в круг радіуса 1.

30. Нехай n — фіксоване натуральне число. Чи утворюють поле алгебричні числа степеня $\leq n$?

31. Нехай $z_1, \ldots, z_k$ — ненульові комплексні числа. Доведіть, що коли для комплексного числа a кожен із добутків az_i можна подати у вигляді лінійної комбінації $az_i = \alpha_{i1}z_1 + \cdots + \alpha_{ik}z_k$ з раціональними коефіцієнтами α_{ij}, то a є алгебричним числом степеня не більшого ніж k.

32.* Доведіть, що поле $\mathbb{C}$ містить нескінченно багато різних алгебрично замкнених підполів.

33. Доведіть, що поле алгебричних чисел є полем часток кільця цілих алгебричних чисел.

34. Доведіть, що нормований мінімальний многочлен цілого алгебричного числа має цілі коефіцієнти.

35. Доведіть, що ненульовий елемент кільця цілих алгебричних чисел буде оборотним тоді й лише тоді, коли вільний член його нормованого мінімального многочлена дорівнює ± 1.

36. Доведіть, що коли числа $a_1, \ldots, a_n$ є цілими алгебричними, то кожен корінь многочлена $x^n + a_1x^{n-1} + \cdots + a_n$ також є цілим алгебричним числом.

37.*** Доведіть, що для ірраціонального числа a кожне з чисел $\cos a\pi$ і $\sin a\pi$ не є алгебричним.

38. a) Доведіть, що $\cos 36^\circ = \phi/2$, де ϕ — число золотого перетину.

b) Запропонуйте спосіб побудови правильного 5–кутника, який використовує попереднє твердження.

39. Не використовуючи теореми Ґауса, доведіть, що за допомогою циркуля та лінійки не можна побудувати правильний n-кутник, якщо a) $n = 7$; b) $n = 11$; c) $n = 13$.

40. Чи можна за допомогою циркуля та лінійки побудувати рівнобедрений трикутник із бічною стороною $b = 5$ і радіусом вписаного кола $r = 1$?

41. Доведіть, що кожне коло координатної площини або взагалі не містить конструктивних точок, або містить рівно одну таку точку, або рівно дві такі точки, або нескінченно багато таких точок. Наведіть відповідні приклади.

42. Доведіть, що задачі квадратури круга і спрямлення кола є еквівалентними.

43. a) Доведіть, що множина CS всіх конструктивних чисел утворює підполе поля $\mathbb{C}$.

b) Доведіть, що поле CS не має розширень степеня 2.

44.* Знайдіть усі такі натуральні числа n, для яких довільний кут можна поділити за допомогою циркуля та лінійки на n рівних частин.

45.* Наведіть приклад кута, який не є побудовним, але трисекція якого за допомогою циркуля та лінійки є можливою.

Домашнє завдання

46. Побудуйте многочлен з цілими коефіцієнтами, для дане число буде коренем: a) $\sqrt{3} - \sqrt{7}$; b) $i - 2\sqrt{2}$.

47. Знайдіть мінімальний многочлен числа:
a) $\sqrt[5]{3}$; b) $2 - 3i$; c) $1 + \sqrt{2} + \sqrt{3}$.

48. Доведіть, що число $\cos\alpha$ буде алгебричним тоді й лише тоді, коли алгебричним буде число $\sin\alpha$.

49. Позбавтеся від ірраціональностей у знаменнику:
a) $\dfrac{1}{1 + 2\sqrt{2} + \sqrt{3}}$; b) $\dfrac{1}{1 - 2\sqrt[3]{2} + \sqrt[3]{4}}$; c) $\dfrac{1}{-1 + \sqrt[3]{3} + \sqrt[3]{9}}$.

50. Як, вміючи будувати правильний 5–кутник, можна побудувати правильний a) 20–кутник; b) 15–кутник?

Відповіді та вказівки

Заняття 1. **10.** Жодна з множин кільця не утворює. **11.** b) — так; a), c) — ні. *Вказ.* a), c) — множина незамкнена відносно додавання. **12.** Так. *Вказ.* b) $\varepsilon_3^2 = -1 - \varepsilon$. **13.** a), b), c) — так, d) — ні. *Вказ.* b) Сума коефіцієнтів — це $f(1)$. **15.** b) Якщо одне з них міститься в іншому. **16.** a) Дільником 0 є лише 0, дільниками 1 є 1 і -1. b) Якщо a і n взаємно прості, то a є дільником 1; у противному разі a — дільник 0. **17.** b) $\overline{13}^{-1} = \overline{7}$; e) $\overline{17}^{-1} = \overline{23}$. **18.** a) Дільником 0 є лише 0, дільниками 1 є всі ненульові константи. b) Якщо 0 належить області значень функції f, то f є дільником 0; у противному разі f є дільником 1. c) f є дільником 1 тоді й лише тоді, коли не набуває значення 0, і дільником 0 тоді й лише тоді, коли вона набуває значення 0 в усіх точках деякого інтервалу $[a, b]$, $a < b$. *Вказ.* c) Якщо $f(c) \neq 0$, то $f(x) \neq 0$ в усіх точках деякого околу точки c. **19.** Лише a). *Вказ.* b) Розгляньте в кільці $\mathbb{Z}_6$ підкільце $P = \{\overline{0}, \overline{3}\}$. **20.** Так. *Вказ.* Розгляньте $M_2(\mathbb{R})$. **21.** *Вказ.* Якщо $ac = 0$ і $aba = a$, то $a(b + c)a = a$ **22.** *Вказ.* Використайте зад. 7. **23.** 8^n. **26.** *Вказ.* Ізоморфізмом буде відображення $x + y\sqrt{n} \mapsto \left(\begin{smallmatrix} x & y \\ ny & x \end{smallmatrix}\right)$. **27.** *Вказ.* Порівняйте кількість оборотних елементів у цих кільцях. **28.** k — просте число. *Вказ.* Якщо $k = uv$, де $u, v > 1$, то $\frac{1}{u}, \frac{1}{v} \in \mathbb{Z}_{(k)}$, але $\frac{1}{u} \cdot \frac{1}{v} = \frac{1}{k} \notin \mathbb{Z}_{(k)}$. **29.** Ні. *Вказ.* Жодна з функцій $\sin x \sin\sqrt{2}x$ і $\sin x + \sin\sqrt{2}x$ не є періодичною. **30.** Ні. Немає лівого нуля і не виконується дистрибутивний закон $(f + g) \circ h = f \circ h + g \circ h$. **32.** Так. Наприклад, $x \circ y = e^{\ln x \cdot \ln y}$. *Вказ.* Подивіться, у що переходить звичайне множення при бієкції $\mathbb{R} \to \mathbb{R}^+$, $x \mapsto \ln x$. **33.** *Вказ.* a) $a + b = (-1)(-1)(a + b) = (-1)((-a) + (-b)) = = (-1)(-b) + (-1)(-a) = b + a$ (перша й четверта рівності випливають із $-a = (-1) \cdot a$, друга — з дистрибутивності, третя — з $-a = (-1) \cdot a$ і властивості протилежних елементів). b) Якщо взяти некомутативну адитивну групу і нульове множення, то виконуються всі аксіоми кільця, крім існування одиниці та комутативності додавання. **34.** Кожне підкільце визначається деякою підмножиною P множини простих чисел і має вигляд $\left\{ \frac{m}{p_1^{n_1} \cdots p_k^{n_k}} \;\middle|\; m, n_1, \ldots, n_k \in \mathbb{Z},\ p_1, \ldots, p_k \in P \right\}$. *Вказ.* Використовуючи наявність одиниці, доведіть, що коли підкільце містить нескоротний дріб $\frac{m}{p_1^{n_1} \cdots p_k^{n_k}}$, то воно містить дріб $\frac{1}{p_1^{n_1} \cdots p_k^{n_k}}$, а тому і дроби $\frac{1}{p_1}, \ldots, \frac{1}{p_k}$. **35.** *Вказ.* $na \cdot ma = nm \cdot a^2 = ma \cdot na$. **36.** Матриця A — дільник 0, якщо $\det A = 0$, і дільник 1, якщо $\det A = \pm 1$. **37.** *Вказ.* a) Якщо a — оборотний зліва, то a не є правим дільником 0 і відображення $x \mapsto xa$ є бієкцією. b) Нехай a — лівий дільник 0. Якби a не був правим

дільником 0, то відображення $x \mapsto xa$ було б бієкцією і a був би правим дільником 1. **38.** b) Напр., $M_2(\mathbb{Z})$ або кільце неперервних функцій на $\mathbb{R}$. *Вказ.* a) Випливає із зад. 5 і 37. **39.** *Вказ.* Із $c(1-ab) = (1-ab)c = 1$ випливає, що $c-1 = abc = cab$. Тому $(1-ba)^{-1} = 1+bca$. **40.** a) $\sum_{n=0}^{\infty} x^n$; b) $\sum_{n=0}^{\infty}(-2)^n x^n$; c) $\sum_{n=0}^{\infty} F_n x^n$, де F_n — n-те число Фібоначчі. *Вказ.* c) Нехай $(1+x+x^2)^{-1} = \sum_{n=0}^{\infty} x^n(1+x)^n = \sum_{n=0}^{\infty} a_n x^n$. Покажіть, що $a_n = \sum_{k\geq 0}\binom{n-k}{k}$, $a_0 = a_1 = 1$ і що $a_{n+1} = a_n + a_{n-1}$ для всіх $n > 0$. **41.** Вироджені матриці зі слідом 0. *Вказ.* A нільпотентна тоді й лише тоді, коли $\chi_A(\lambda) = \lambda^2$. **42.** *Вказ.* Якщо $a^m = a^{m+k}$ і $m + i \equiv 0 \pmod{k}$, то a^{m+i} є ідемпотентом. **43.** *Вказ.* K_1 при $|\mathbb{R} \setminus D| > 1$ містить дільники 0, а при $|\mathbb{R} \setminus D| = 1$ $K_1 \simeq \mathbb{R}$. У той же час K_2 і $\mathbb{R}[x]$ містять необоротні елементи і не містять дільників 0. Припустимо тепер, що існує ізоморфізм $\varphi : K_2 \to \mathbb{R}[x]$. Легко пересвідчитись, що $\varphi(m/n) = m/n$ для $m/n \in \mathbb{Q}$. Позаяк оборотні елементи переходять в оборотні, то константи з K_2 переходять в константи з $\mathbb{R}[x]$. Крім того, квадрати (тобто додатні константи) мають переходити у квадрати, тому φ зберігає на $\mathbb{R}$ відношення порядку. Тому $\varphi(\mathbb{R}) = \mathbb{R}$. Але з рівності $\sin^2 x + \cos^2 x = 1$ випливає, що $\varphi(\sin x) \in \mathbb{R}$ і $\varphi(\cos x) \in \mathbb{R}$. Отже, φ не ін'єктивний, а тому не є ізоморфізмом. **44.** Наприклад, кільце многочленів від нескінченної кількості змінних. **45.** *Вказ.* Нехай a — твірний елемент адитивної групи кільця. Порівняйте довжину розкладу $a^2 = a + \cdots + a$ в $n\mathbb{Z}$ і $m\mathbb{Z}$. **46.** *Вказ.* a) Використайте зад. 35. b) Якщо адитивна група циклічна, то це випливає із зад. 35. У противному разі візьміть фіксований елемент a, який не є цілим кратним одиниці, і запишіть кожен елемент кільця у вигляді $m \cdot 1 + n \cdot a$, де $0 \leq m, n < p$. c) Напр., $\left\{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b, c \in \mathbb{Z}_p\right\}$. **47.** a) Ні; b) так; c) так. **48.** a), c) — так, b) — ні. *Вказ.* a) Одиницею буде функція, яка в усіх точках $x \neq 5$ дорівнює 1. **49.** Дільник 0 тільки b), дільник 1 тільки c). **50.** Дільник 1 — лише M, нільпотент — лише $\varnothing$, дільники 0 — всі власні підмножини $A \subset M$. **51.** a) 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22; b) 1, 5, 7, 11, 13, 17, 19, 23; c) 0, 6, 12, 18.

Заняття 2. **18.** a) — так; b),c) — ні. **19.** a) Так; b) ні. **20.** a) Так, $(\mathbb{Z}\oplus\mathbb{Z})/I \simeq \mathbb{Z}$ і є областю цілісності; b) ні; c) ні; d) так; $(\mathbb{Z}\oplus\mathbb{Z})/I \simeq$ $\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_5$ і не є областю цілісності. **21.** *Вказ.* K містить одиницю кільця $\mathbb{Z}\oplus\mathbb{Z}$. **24.** *Вказ.* a) Якщо $\bigcup_{n=1}^{\infty} I_n = K$, то існує таке n, що $1 \in I_n$. b) Розгляньте в кільці $K = \bigoplus_{k\in\mathbb{N}} \mathbb{Z}$ ідеали $I_n = \bigoplus_{i=1}^{n} \mathbb{Z}$ (пряма сума перших n доданків). **25.** a) $n\mathbb{Z}$; нескінченно багато. b) $d\mathbb{Z}_n$, де $d \mid n$; $(k_1+1)\cdots(k_m+1)$, якщо $n = p_1^{k_1}\cdots p_m^{k_m}$. c) Лише $\{0\}$ і $M_2(\mathbb{R})$. **26.** Жодне з відображень не є гомоморфізмом. *Вказ.* a) і b) не зберігають добуток, c) не зберігає суму. **27.** Тільки нульовий і тотожний. *Вказ.* У

полі $\mathbb{R}$ число є невід'ємним тоді й лише тоді, коли воно є квадратом. Ненульовий гомоморфізм $\varphi : \mathbb{R} \to \mathbb{R}$ лишає на місці раціональні числа і квадрати переводить у квадрати. Тому він зберігає відношення порядку. **29**. *Вказ.* Ядром гомоморфізму є ідеал поля. **30.** Тільки b). *Вказ.* a) Розгляньте занурення $\mathbb{Z} \to \mathbb{Q}$. **31.** 3 гомоморфізми: $(a, b) \mapsto 0$, $(a, b) \mapsto a$, $(a, b) \mapsto b$. *Вказ.* Елементи $(1, 0)$, $(0, 1)$ та $(1, 1)$ є ідемпотентами, а тому можуть переходити лише в 0 або 1. **32.** Усі многочлени із парним вільним членом. Факторкільце $\mathbb{Z}[x]/I$ містить 2 елементи і ізоморфне $\mathbb{Z}_2$. **33.** *Вказ.* Відображення $\overline{c(x-a)+d} \mapsto \overline{c(x-b)+d}$ є ізоморфізмом P_a на P_b. **34.** *Вказ.* Використайте зад. 15. **35.** *Вказ.* Кожен многочлен $h(x)$ степеня, меншого за степінь $f(x)g(x)$, однозначно записується у вигляді $h(x) = u(x)f(x) + v(x)g(x)$, де $u(x)$ має менший степінь, ніж $g(x)$, а $v(x)$ — менший степінь, ніж $f(x)$. **36.** *Вказ.* a) Див. зад. 33 і 15. b) Нільелементи є тільки в першому факторкільці. **37.** *Вказ.* a) Див. зад. 33 і 15. b) Тільки перше кільце є полем і тільки в другому є нільелементи. **38.** *Вказ.* Нехай c — комплексний корінь тричлена $x^2 + ax + b$. Тоді відображення $\mathbb{R}[x] \to \mathbb{C}$, $f(x) \mapsto f(c)$, є епіморфізмом, ядром якого є ідеал $(x^2 + ax + b)$. **39.** q^n. **40.** Ізоморфні дві пари: a) і c) та b) і d). *Вказ.* Використайте зад. 37. **41.** *Вказ.* Ізоморфізмом $\mathbb{R}[x, y]/(y)$ на $\mathbb{R}[x, y]/(x)$ буде відображення $f(x, y) + (y) \mapsto f(y, x) + (x)$. **42.** *Вказ.* Дільники 0 є тільки в другому кільці. **43.** b) Ні. *Вказ.* b) Таким не буде, наприклад, ідеал усіх функцій f, для яких множина $\{x \in \mathbb{R} \,|\, f(x) \neq 0\}$ є обмеженою. **44.** *Вказ.* a) Для $A \in M_n(\mathbb{R})$ через $A^{(i)}$ позначимо матрицю, i-й рядок якої збігається з i-м рядком матриці A, а решта рядків — нульові. Нехай $I \subseteq M_n(\mathbb{R})$ — лівий ідеал. Тоді I — підпростір векторного простору $M_n(\mathbb{R})$ і разом із кожною матрицею A містить усі матриці $A^{(i)}$. Для кожної матриці $A \in I$ візьмемо $V_A = \{\boldsymbol{x} \in \mathbb{R}^n \mid A\boldsymbol{x} = 0\}$ і нехай $V_I = \bigcap_{A \in I} V_A$. Очевидно, що $I \subseteq I^l_{V_I}$. Для доведення зворотного включення зауважимо, що V_A є ортогональним доповненням у просторі $\mathbb{R}^n$ зі стандартним скалярним добутком до підпростору, породженого рядками матриці A, і що $B \in I^l_V$ тоді й лише тоді, коли кожен рядок матриці B належить $V^\perp$. Позаяк $\dim M_n(\mathbb{R}) < \infty$, то існують такі $A_1, \ldots, A_k \in I$, що $V = V_{A_1} \cap \cdots \cap V_{A_k}$. Рядки матриць $A_1, \ldots, A_k$ утворюють систему твірних простору $V_I^\perp$. Якщо $B \in I^l_{V_I}$, то кожен рядок матриці B є лінійною комбінацією рядків матриць $A_1, \ldots, A_k$, тому кожна матриця $B^{(i)} = \sum \lambda_{rs} A_s^{(r)}$ належить I. Крім того, $B = B^{(1)} + \cdots + B^{(n)}$. **45.** Підмножина $I \subseteq \mathbb{Z} \oplus \mathbb{Z}$ буде ідеалом тоді й лише тоді, коли вона має вигляд $I = \{(a, b) \mid a \in I_1, b \in I_2\}$, де I_1 і I_2 — ідеали кільця $\mathbb{Z}$. **46.** *Вказ.* Нехай $a \neq 0$. Ланцюг $Ka \supseteq Ka^2 \supseteq Ka^3 \supseteq \cdots$ обриває-

ться, тому для деякого k $Ka^k = Ka^{k+1}$, $a^k = ba^{k+1}$ і $1 = ba$. Далі із $b = bab$ випливає $1 = ab$. **47.** *Вказ.* Кожний мінімальний ідеал є головним. Якщо $I = (a)$, то $(a^2) \subseteq (a)$, звідки $(a^2) = (a)$ і $a = ba^2$. Тоді $I = (ba)$ і ba — ідемпотент. **48.** Ідеалів 2^n і вони мають вигляд $P_{i_1} \oplus \cdots \oplus P_{i_k}$. **49.** *Вказ.* a) $a + bi \mapsto (a + b) \bmod 2$. b) При епіморфізмі $\mathbb{Z}[i] \to \mathbb{Z}$ одиниця має переходити в одиницю. У що має переходити i? **50.** Ні. *Вказ.* У що має переходити $1/2$? **51.** *Вказ.* Оскільки $\frac{1}{n} \cdot n = 1$, то $\varphi\left(\frac{1}{n}\right) = \varphi(n)^{-1}$. **52.** *Вказ.* $c = \varphi(x)$. **54.** *Вказ.* Кожне з них ізоморфне кільцю $\mathbb{R}[x]$. Для першого факторкільця це очевидно. Крім того, з рівності $f(x, y) = \sum_{k\geq 0} y^k h_k(x) = \sum_{k\geq 0} x^{2k} h_k(x) + \sum_{k\geq 0}(y^k - x^{2k})h_k(x)$ і подільності $y^k - x^{2k}$ на $y - x^2$ випливає, що кожен многочлен із $\mathbb{R}[x, y]$ можна записати у вигляді $f(x, y) = f(x, x^2) + (y - x^2)g(x, y)$. Тому відображення $\mathbb{R}[x, y] \to \mathbb{R}[x]$, $f(x, y) \mapsto f(x, x^2)$, буде епіморфізмом із ядром $(x^2 - y)$. **55.** *Вказ.* Якщо $\mathbb{Z} \simeq \mathbb{Z}[x]/(2x - 1)$, то існує епіморфізм $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ із ядром $(2x - 1)$. Але якщо $\varphi(x) = k$, то $\operatorname{Ker}\varphi = (x - k) \neq (2x - 1)$. **56.** *Вказ.* Розгляньте образ гомоморфізму $\mathbb{Z} \to K$, $n \mapsto n \cdot 1'$, де $1'$ — одиниця кільця K. **57.** a) $\mathbb{Z}_p$, де p — просте число; b) $\mathbb{Z}$ і $\mathbb{Z}_n$, де n — натуральне число. *Вказ.* Використайте зад. 56. **58**. Розгляньте гомоморфізм $\varphi_c : P[x] \to P$, $f(x) \mapsto f(c)$, де $c = -a^{-1}b$, і застосуйте основну теорема про гомоморфізм кілець. **59.** *Вказ.* Застосуйте основну теорему про гомоморфізм кілець до гомоморфізму $P[x] \to \operatorname{Hom}(V, V)$, $f(x) \mapsto f(\varphi)$. **60.** 4. *Вказ.* Якщо адитивна група $(K, +)$ циклічна, то $K \simeq \mathbb{Z}_9$. У противному разі $(K, +)$ є прямою сумою двох циклічних груп порядку 3. Нехай $(K, +) = \langle 1, a\rangle$. Для кожної з можливостей $a^2 = \alpha + \beta a$, $\alpha, \beta \in \{0, 1, 2\}$ таблиця Келі для $(K, \cdot)$ заповнюється однозначно і збігається з відповідною таблицею для факторкільця $\mathbb{Z}_3[x]/(x^2 - \beta x - \alpha)$. Далі використайте зад. 33 і 15. **61.** *Вказ.* $J(A) - \lambda E = T^{-1}(A - \lambda E)T$, де T — матриця переходу до жорданової бази. Позаяк кожен мінор порядку k матриці AB розкладається в суму добутків мінорів порядку k матриц A і B, то мінори порядку k матриці $J(A) - \lambda E$ є лінійними комбінаціями мінорів порядку k матриці $A - \lambda E$. Отже, $I_k(A) \supseteq I_k(J(A))$. Зворотне включення доводиться аналогічно. **62.** b) $\frac{1}{n+2}\binom{2n+2}{n+1}$; c) $\frac{1}{n+1}\binom{2n}{n}$. *Вказ.* b) Потужність множини M_n є n-м числом Каталана c_n. c) Ідеал із $T_n(\mathbb{R})$ буде нільпотентним тоді й лише тоді, коли він містить лише матриці, у яких всі діагональні елементи дорівнюють 0. Встановіть взаємно однозначну відповідність між такими ідеалами і шляхами з множини M_n. **63.** *Вказ.* Покажіть, що множина тих коефіцієнтів матриць із I, які стоять на перетині фіксованих i–го рядка і j–го стовпця, утворює ідеал кільця K. **64.** c) Ні. *Вказ.*

b) Для кожної ненульової функції $h \in I_{\{c\}}$ $\sqrt{|h|} \in I_{\{c\}}$, але $\sqrt{|h|} \notin (h)$. c) Оскільки ідеал $I_{\{c\}}$ не є головним, то для будь–якої функції $f \in C[a,b]$ з єдиним нулем $c \in [a,b]$ ідеал (f) не має вигляд I_A. d) Нехай для ідеалу I такої точки не існує. Для кожної точки $a \in [a,b]$ візьміть таку функцію f_a, що $f_a(a) > 0$, і окіл $U_a = (a - \varepsilon_a, a + \varepsilon_a)$, на якому f_a не дорівнює 0. Виберіть скінченне покриття $(U_a)_{a \in A}$ множини $[a,b]$. Тоді функція $f = \sum_{a \in A} f_a g_a$, де $g_a = \begin{cases} \varepsilon_a - |x-a|, & \text{якщо } |x-a| < \varepsilon; \\ 0, & \text{в противному разі,} \end{cases}$ належить I і є дільником 1. e) Використайте вказ. до п. b). **65.** a — так; b,c — ні. **66.** a),b) Ні; c) буде правим ідеалом. **67.** Правильна тільки a). *Вказ.* a) При сюр'єктивному гомоморфізмі одиниця переходить в одиницю. b) Розгляньте гомоморфізм $\mathbb{Z} \to \mathbb{Z}_2$, $n \mapsto \overline{n}$. **68.** $\operatorname{Ker} \varphi = (x^2 - 2)\mathbb{Q}[x]$, $\operatorname{Im} \varphi = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. **69.** Тільки d). *Вказ.* Використайте зад. 11. **70.** a) і d) ізоморфні $\mathbb{C}$, b) і c) ізоморфні $\mathbb{R} \oplus \mathbb{R}$. *Вказ.* Використайте зад. 37. **71.** *Вказ.* Покажіть, що відображення $P[x,y] \to P$, $a + bx + cy + dx^2 + \cdots \mapsto a$, є епіморфізмом, і знайдіть його ядро.

Заняття 3. **19.** a) Так; b) ні. *Вказ.* a) Якщо $a' = \varepsilon a$ і $b' = \sigma b$, де ε і σ — дільники одиниці, то $a'b' = \varepsilon\sigma ab$. b) У кільці $\mathbb{Z}$ $3 \sim 3$ і $2 \sim -2$, але $3+2 \nsim 3-2$. **20.** Так. *Вказ.* Підставте замість c a і b. **21.** *Вказ.* Потужність ненульового класу асоційованих елементів дорівнює потужності множини дільників одиниці. **22.** Жодна. *Вказ.* a) Многочлен $x^2 - 2$ є незвідним в $\mathbb{Q}[x]$, але не в $\mathbb{R}[x]$. b) Число 6 є простим в $\mathbb{Z}[1/2]$, але не в $\mathbb{Z}$. **23.** a) Ні; b), c) так. **24.** a) $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$; b) $5 - i\sqrt{3} = (1 - i\sqrt{3}) \cdot (2 + i\sqrt{3})$; c) $3 + 2i\sqrt{3} = i\sqrt{3} \cdot (2 - i\sqrt{3})$. **25.** *Вказ.* $N(2 + \sqrt{-5}) = N(2 - \sqrt{-5}) = 9$, а в $\mathbb{Z}[\sqrt{-5}]$ немає елементів із нормою 3. Із другого боку, $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 3 \cdot 3$, але в $\mathbb{Z}[\sqrt{-5}]$ число 3 на жодне з чисел $2 + \sqrt{-5}$ і $2 - \sqrt{-5}$ не ділиться. **26.** a) Ні; решта — так. *Вказ.* c) $x^4 + y^4 = (x^2 + y^2)^2 - 2x^2y^2$; e) із розкладу $x^5 - y^5$ на множники над полем $\mathbb{C}$ випливає, що $x^4 + x^3y + x^2y^2 + xy^3 + y^4 = (x^2 - 2\cos\frac{\pi}{5}xy + y^2)(x^2 + 2\cos\frac{\pi}{5}xy + y^2)$. **27.** *Вказ.* Кожен спільний дільник a і b є спільним дільником a і $ac + b$ і навпаки. **29.** Наприклад, $a = 1$, $b = x^5$, $c = x^6$. *Вказ.* b) Якщо НСД(b,c) не існує, то НСД(НСД$(1,b),c) = 1$, а НСД$(1,$НСД$(b,c))$ не існує. **32.** *Вказ.* $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. **33.** a) Так; b), c) не завжди. *Вказ.* b) Повний прообраз $\varphi^{-1}(J)$ ідеалу $J = 2\mathbb{Z}$ при епіморфізмі $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(0)$, не є головним. c) Розгляньте для складеного n $\mathbb{Z}_n$ як епіморфний образ $\mathbb{Z}$. **34.** *Вказ.* a) Ідеал $(2,x)$ — не головний; b) ідеал (x,y) — не головний. **35.** *Вказ.* Відображення $K \to K/(a) \oplus K/(b)$,

$x \mapsto (x+(a), x+(b))$, є епіморфізмом із ядром (ab). **36.** *Вказ.* Індукція за сумою $n+m$. Твердження тривіальне, якщо $n=m=1$. Нехай тепер $n+m>2$, причому можна вважати, що $n>1$. Тоді із $\alpha_1 a_1\cdots a_{n-1}+\beta_1 b_1\cdots b_m = 1$ і $\alpha_2 a_n+\beta_2 b_1\cdots b_m = 1$ випливає, що $\alpha_1\alpha_2 a_1\cdots a_{n_1}+(\beta_1\alpha_2 a_n+\alpha_1\beta_2 a_1\cdots a_{n-1}+\beta_1\beta_2 b_1\cdots b_m)b_1\cdots b_m=1$. **37.** a) $36=3\cdot 180-2\cdot 252$; b) $13=37\cdot 2873-16\cdot 6643$; c) $1=2639\cdot 1001-397\cdot 6654$. **38.** a) 11; b) 771; c) 112. **39.** a) $x\equiv 2 \pmod{36}$; b) $x\equiv 13 \pmod{18}$; c) $\varnothing$. **40.** a) x^3+I; b) $(x^4+x^2+x+1)+I$; c) x^4+I. **41.** *Вказ.* Покладіть $\sigma(a+bi\sqrt{2})=a^2+2b^2$. Для довільної точки прямокутника зі сторонами 1 і $\sqrt{2}$ знайдеться вершина, віддаль від якої до цієї точки менша 1. **42.** a) $1-2i$; b) $2-i$; c) 1; d) $4i-7$. **43.** 3, $2+i$ та $2+3i$. *Вказ.* $2=(1+i)(1-i)$; $5=(2+i)(2-i)$. **44.** a) $(2+i)^2(1-i)$; b) $(1-i)(1+2i)(1-2i)$; c) $(2+i)(1-i)(-1+4i)$; d) $(1-i)(1-2i)(-3+2i)$; e) $(1-i)(1-2i)(-2+3i)$; f) $(1+i)(3-2i)$; g) $(1+i)(5-2i)$); h) $(1-i)^3(1+2i)^2$. **45.** a) 9; b) 20; c) 16; d) 18; e) 32; f) 25; g) 64. *Вказ.* Розкладіть число на нерозкладні множники. **46.** *Вказ.* Якщо $I=(a)$, то в кожному класі суміжності за ідеалом I можна вибрати представника, норма якого менша $N(a)$. **47.** a) 2, поле; b) 4, не поле; c) 9, поле; d) 25, не поле. **48.** *Вказ.* Нехай a — простий і $a=bc$. Тоді $a\mid b$ або $a\mid c$. Якщо $a\mid b$, то $b=ad$ і з рівності $a=a\cdot 1=ad\cdot c$ випливає, що $1=dc$. Отже, c є дільником 1. **50.** *Вказ.* Якщо $x^2+y^2+z^2$ — звідний, то $x^2+y^2+z^2=(x+ay+bz)(x+cy+dz)$, звідки $ac=bd=1$ і $a+c=b+d=ad+bc=0$. Але тоді $a\neq 0$, $b\neq 0$, $c=-a$, $d=-b$ і $2ab=0$. **49.** *Вказ.* Якщо $f+yg$ розкладається в добуток многочленів p і q, то можна вважати, що $p\in\mathbb{R}[x]$ і $q=q_1+yq_2$, де $q_1,q_2\in\mathbb{R}[x]$. Але тоді f і g мають спільний дільник p. **51.** *Вказ.* b) Наприклад, якщо $c=a=1+i\sqrt{3}$, $b=1-i\sqrt{3}$, то НСД$(a,b)=1$, а НСД(ca,cb) чисел $ca=2(1-i\sqrt{3})$ і $cb=4$ не існує. Справді, спільними дільниками чисел 4 і $2-2\sqrt{-3}$ є ± 1, ± 2 і $\pm 1\pm\sqrt{-3}$. Але жодне з чисел $\pm 1\pm\sqrt{-3}$ не ділиться в K на 2, а жодне з чисел ± 2 не ділиться в K на $1+\sqrt{-3}$. **52.** *Вказ.* Якщо $\alpha>0$, то елемент x^α не є оборотним. З іншого боку, $x^\alpha=x^{\alpha/2}\cdot x^{\alpha/2}$. **53.** b) Дільники одиниці — $\pm 2^m$, де $m\in\mathbb{Z}$; нерозкладні елементи (з точністю до асоційованості) — непарні прості числа. *Вказ.* c) Покладіть $\sigma(2^m\cdot n)=|n|$, де n — непарне число. **55.** *Вказ.* Нехай I — мінімальний ідеал і $0\neq a\in I$. Тоді $\{0\}\neq(a)\subseteq I$, звідки $I=(a)$. Для довільного $0\neq b\in K$ маємо $\{0\}\neq(ab)\subseteq(a)$, звідки $I=(ab)$, $ab\sim a$ і $b\sim 1$. **56.** *Вказ.* Кожне з кілець є підкільцем поля $\mathbb{C}$, причому норма кожного ненульового елемента є натуральним числом. **57.** *Вказ.* Якщо елемент a — необоротний, то ідеал (x,a) не є головним. **58.** *Вказ.* Використайте зад. 2.44. **63.** *Вказ.* Факторкільце $\mathbb{Z}[i]/(q)$ буде полем порядку $N(q)$.

60. Наприклад, $\{(n,0) \mid n \in \mathbb{Z}\}$. **61.** *Вказ.* Доведіть, що у факторкільці для довільних ненульових a і b кожне з рівнянь $ax = b$ і $ya = b$ має єдиний розв'язок. **65.** $27 = 3\cdot 3\cdot 3 = (2+\sqrt{-23})\cdot(2-\sqrt{-23})$. **66.** *Вказ.* Нехай k — фіксоване натуральне число і K — кільце всіх многочленів вигляду

$$a_0 + a_2x^2 + a_4x^4 + \cdots + a_{2k-2}x^{2k-2} + a_{2k}x^{2k} + a_{2k+1}x^{2k+1} + \cdots + a_nx^n$$

із цілими коефіцієнтами, які не містять одночленів степенів 1, 3, 5, ..., $2k-1$. У цьому кільці елемент x^{2k+1} буде нерозкладним, а для елемента $a = x^{4k+2} = x^2\cdot x^2\cdots x^2 = x^{2k+1}\cdot x^{2k+1}$ маємо $m_a = 2$, $M_a = 2k+1$. Тому $M_a/m_a = k + 1/2$. **68.** *Вказ.* Кожен ненульовий ряд Лорана можна записати у вигляді $x^k\sum_{n=0}^{\infty} a_nx^n$, де $k \in \mathbb{Z}$, $a_0 \neq 0$. Множник $\sum_{n=0}^{\infty} a_nx^n$ є обротним елементом кільця $P[[x]]$. **69.** *Вказ.* Використайте теорему Вільсона. **71.** a),b) Так; c) ні. *Вказ.* a),b) Розгляньте норми. c) $61 = (4+3\sqrt{5}i)(4+3\sqrt{5}i)$. **72.** $4+5\sqrt{3}i = (1+2\sqrt{3}i)(2-\sqrt{3}i)$. **73.** *Вказ.* $6 = 2\cdot 3 = -\sqrt{-6}\cdot\sqrt{-6}$. **74.** *Вказ.* $P[x]$ — кільце головних ідеалів, а $P[x,y]$ — ні. **75.** $x \equiv 6 \pmod{41}$. **76.** a) 446; b) 1508. **77.** a) x^3+x^2; b) x^4+x^3+x. **78.** a) $1+i$; b) $7+6i$; c) $5-3i$. **79.** a) $1+2i$, $1-2i$; b) $\varnothing$; c) $1+i$, $1+2i$, $1-2i$, 2, 5, $1-3i$, $3-i$, $2+4i$, $2-4i$, $5+5i$; d) 3, 7.

Заняття 4. **10.** a) $x \equiv 302 \pmod{7020}$; b) $x \equiv 601 \pmod{5060}$; c) $x \equiv 590 \pmod{3990}$. **11.** a) $x \equiv 863 \pmod{7182}$; b) $x \equiv 4835 \pmod{5520}$. **12.** a) 1085; b) 29; c) 262; d) 133. **13.** a) $a \equiv 17 \pmod{30}$; b) $\varnothing$; c) $a \equiv 47 \pmod{70}$. *Вказ.* b) Перша й третя конґруенції несумісні. **14.** a) 7; b) 53; c) 32; d) 51. **15.** a) 12; b) 6; c) 12; d) 20. *Вказ.* a) $\mathbb{Z}_{210}^* \simeq \mathbb{Z}_2^*\times\mathbb{Z}_3^*\times\mathbb{Z}_5^*\times\mathbb{Z}_7^* \simeq$ $\simeq \mathbb{Z}_2\oplus\mathbb{Z}_4\oplus\mathbb{Z}_6$; b) $\mathbb{Z}_{252}^* \simeq \mathbb{Z}_4^*\times\mathbb{Z}_9^*\times\mathbb{Z}_7^* \simeq \mathbb{Z}_2\oplus\mathbb{Z}_6\oplus\mathbb{Z}_6$; c) $\mathbb{Z}_{280}^* \simeq \mathbb{Z}_8^*\times\mathbb{Z}_5^*\times$ $\times\mathbb{Z}_7^* \simeq \mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_4\oplus\mathbb{Z}_6$; d) $\mathbb{Z}_{200}^* \simeq \mathbb{Z}_8^*\times\mathbb{Z}_{25}^* \simeq \mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_{20}$. **16.** Тільки 0 і 1. **17.** *Вказ.* Якщо $n = p_1^{k_1}\cdots p_m^{k_m}$, то $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}}\oplus\cdots\oplus\mathbb{Z}_{p_m^{k_m}}$. Із зад. 16 тепер випливає, що $x \in \mathbb{Z}_n$ буде ідемпотентом тоді й лише тоді, коли x є розв'язком системи $x \equiv \varepsilon_i \pmod{p_i^{k_i}}$ $(i = 1,2,\ldots,m)$, де $\varepsilon_i \in \{0,1\}$. **18.** $x = y = z = 0$. *Вказ.* Зведіть до випадку, коли x, y, z у сукупності взаємно прості, і застосуйте редукцію за модулем 4. **19.** *Вказ.* При діленні на 8 квадрат може давати в остачі лише 0, 1 або 4. **20.** a) Лишки — 1, 4, нелишки — 2, 3; b) лишки — 1, 2, 4, нелишки — 3 5, 6; c) лишки — 1, 2, 3, 5, 9, нелишки — 4, 6, 7, 8; d) лишки — 1, 2, 3, 9, 10, 12, нелишки — 4, 5, 6, 7, 8, 11. **21.** Ні. *Вказ.* Його степенями будуть лише квадратичні лишки. **23.** *Вказ.* a) Якщо $\mathbb{Z}_p^* = \langle a\rangle$, то $P_1 = a^2a^4a^6\cdots a^{p-1} = a^{\frac{p+1}{2}\cdot\frac{p-1}{2}}$. Крім того, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. b) За теоремою Вільсона $P_1P_2 \equiv -1 \pmod{p}$. **24.** *Вказ.* $(-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} = 2k$. **25**. *Вказ.* Використовуючи зад. 24, обчисліть $\left(\frac{-a}{p}\right)$. **26.** a) -1; b) 1; c) -1; d) 1. **27.** $p \equiv \pm 1 \pmod{5}$. *Вказ.*

$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = 1$, тому $\left(\frac{5}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{5}\right) = 1$. **30.** a) $\varnothing$; b) $\{9, 14\}$; c) $\{6, 17\}$. **31**. a) $\varnothing$; b) $n = 41k^2 \pm 12k$; c) $\varnothing$; d) $n = 53k^2 \pm 16k + 1$. *Вказ.* Якщо $an + b = m^2$, то b є квадратичним лишком за модулем a. **32**. a) $x \equiv 10, 11 \pmod{13}$; b) $x \equiv 1, 3 \pmod{19}$; c) $x \equiv 2, 9, 12, 19 \pmod{35}$; d) $x \equiv 1, 57, 79, 122 \pmod{143}$. **34**. *Вказ.* Сюр'єктивність φ рівносильна тому, що для довільних $a_1, \ldots, a_n$ існує такий $x \in K$, що $x - a_k \in I + k$ для всіх k. Необхідність умови випливає з того, що для елемента $a \notin (I_1 + I_2)$ набір $(a + I_1, I_2, \ldots, I_n)$ не має прообразу. Для доведення достатності покажіть, що $I_1 + I_2 \cap \cdots \cap I_n = K$ і застосуйте індукцію. **35.** *Вказ.* Нехай $k \geq \max(n, a_1, \ldots, a_n)$. Візьміть $b = k!$ і застосуйте китайську теорему про остачі. **36.** *Вказ.* Зробіть заміну $X = x/z$, $Y = y/z$ і знайдіть на кривій $f(X, Y) = 0$ яку–небудь раціональну точку A. Тоді для кожної прямої $Y = kX + b$ з раціональним кутовим коефіцієнтом k, що проходить через A, друга точка перетину прямої з кривою $f(X, Y) = 0$ буде мати раціональні координати. **37.** $x = 3$, $y = \pm 5$. *Вказ.* Нехай (x_0, y_0) — розв'язок. У кільці $\mathbb{Z}[\sqrt{-2}]$ $\quad x_0^3 = (y_0 - i\sqrt{2})(y_0 + i\sqrt{2})$. Якщо множники $y_0 - i\sqrt{2}$ і $y_0 + i\sqrt{2}$ не взаємно прості, то їх спільний дільник є дільником і числа $(y_0 + i\sqrt{2}) - (y_0 - i\sqrt{2}) = 2i\sqrt{2} = -(i\sqrt{2})^3$. Але якщо $y_0 + i\sqrt{2}$ ділиться на $i\sqrt{2}$, то y_0 — парне і тоді $y_0^2 \equiv 0 \pmod 4$, $x_0^3 \equiv 2 \pmod 4$, що неможливо. Отже, множники $y_0 - i\sqrt{2}$ і $y_0 + i\sqrt{2}$ взаємно прості. Кільце $\mathbb{Z}[\sqrt{-2}]$ — факторіальне, тому кожен із цих множників є кубом. З рівності $y_0 + i\sqrt{2} = (a + bi\sqrt{2})^3$ знаходимо: $b = 1$, $a = \pm 1$, $y_0 = \pm 5$. **38.** $x = 1$, $y = 0$. *Вказ.* y^2 за модулем 4 — це або 0 або 1. Конґруенція $x^5 \equiv 2 \pmod 4$ розв'язків не має. Тому y парне, а x непарне. Перепишіть рівняння у вигляді $x^5 = (1 + iy)(1 - iy)$ і перейдіть до кільця $\mathbb{Z}[i]$. Позаяк x непарне, то множники в правій частині взаємно прості. Тому $1 + iy = \varepsilon w^5$, де ε — оборотний елемент із $\mathbb{Z}[i]$. Оскільки $\varepsilon^5 = \varepsilon$, то $1 + iy = (\varepsilon w)^5 = (u + iv)^5$, де $u + iv = \varepsilon w$. Тоді $u^5 - 10u^3v^2 + 5uv^4 = 1$, звідки $u \mid 1$. Отже, $u = \pm 1$, а тому $1 - 10v^2 + 5v^4 = \pm 1$. Звідси $v = 0$, $u = 1$, $x = 1$, $y = 0$. **39.** *Вказ.* Розглянемо рівносильну конґруенцію $x^2 + b_1 y^2 \equiv c_1 \pmod p$. Якщо $\left(\frac{c_1}{p}\right) = 1$, то є розв'язок вигляду $(x_0, 0)$. Якщо $\left(\frac{c_1}{p}\right) = -1$, $\left(\frac{b_1}{p}\right) = -1$, то є розв'язок вигляду $(0, y_0)$. Якщо ж $\left(\frac{c_1}{p}\right) = -1$, $\left(\frac{b_1}{p}\right) = 1$, то можна перейти до рівносильної конґруенції $x^2 + y_1^2 \equiv c_1 \pmod p$. Досить довести, що остання конґруенція має розв'язок хоча б для одного такого c_1, що $\left(\frac{c_1}{p}\right) = -1$. Якби це було не так, то сума двох квадратів завжди була б квадратом. Але тоді квадратом було б і довільне число, як сума одиниць. **40.** *Вказ.* $ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2 - \frac{d}{4a}$. a) Якщо $p|d$, то $\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right) =$

$= \sum_{x=1}^{p} \left(\frac{a\left(x+\frac{b}{2a}\right)^2}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{a}{p}\right) = (p-1)\left(\frac{a}{p}\right)$. b) Нехай тепер $p \nmid d$. Тоді $\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right) = \sum_{x=1}^{p} \left(\frac{ax^2+k}{p}\right) = \sum_{x=1}^{p} \left(\frac{a(x^2+m)}{p}\right) = \left(\frac{a}{p}\right) \cdot \sum_{x=1}^{p} \left(\frac{x^2+m}{p}\right)$. Але $\sum_{x=1}^{p} \left(\frac{x^2+m}{p}\right) = \sum_{x=1}^{p} (x^2+m)^{\frac{p-1}{2}} \bmod p \equiv \sum_{x=1}^{p} \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} m^{(\frac{p-1}{2}-k)} x^{2k} \equiv$ $\equiv \sum_{k=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} m^{(\frac{p-1}{2}-k)} \sum_{x=1}^{p} x^{2k} \pmod p$. Позаяк за модулем p

$$\sum_{x=1}^{p} x^{2k} \equiv \begin{cases} 0, & \text{якщо } 2k \nmid (p-1), \\ p-1, & \text{якщо } 2k \mid (p-1), \end{cases}$$

то $\sum_{x=1}^{p} \left(\frac{x^2+m}{p}\right) \equiv (p-1) \pmod p = -1$. Тому $\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right) = -\left(\frac{a}{p}\right)$. **41.** *Вказ.* $\mathbb{Z}_q^* = 2p$. Але $2^2 = 4 \not\equiv 1 \pmod q$ і $2^p \equiv \left(\frac{2}{q}\right) = -1 \not\equiv 1 \pmod q$. Тому $\langle 2 \rangle = \mathbb{Z}_q^*$. **42.** *Вказ.* $|\mathbb{Z}_q^*| = 2p$ і $5^2 = 25 \not\equiv 1 \pmod q$. $5^p \equiv \left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)$. Тому $5^p \equiv -1 \pmod q \Leftrightarrow q = 5m \pm 2$. Крім того, $q = 8k+3$. Отже, $\langle 5 \rangle = \mathbb{Z}_q^* \Leftrightarrow q \equiv 3, 27 \pmod{40}$. **43.** *Вказ.* Група $\mathbb{Z}_p^*$ є циклічною групою порядку 2^{2^k}. Тому її підгрупи утворюють за включенням ланцюг. Квадратичні лишки утворюють максимальну підгрупу порядку $2^{2^{k-1}}$. **44**. *Вказ.* Із зад. 5 випливає, що $2^{251} - 1$ ділиться на $2 \cdot 251 + 1 = 503$. **45.** *Вказ.* Якщо k — непарне, то $2^k \equiv 2 \pmod 3$. Тому $\left(\frac{3}{2^q-1}\right) = -\left(\frac{2^q-1}{3}\right) =$ $= -\left(\frac{1}{3}\right) = -1$. **46.** *Вказ.* Скористайтеся теоремою Вільсона. **47.** *Вказ.* $(a^{k+1})^2 = a^{2k+2} = a \cdot a^{(p-1)/2} = a$. **48.** *Вказ.* $a^{4k+2} \equiv 1 \pmod p$, тому $a^{2k+1} \equiv \pm 1 \pmod p$. Крім того, за квадратичним законом взаємності $2^{4k+2} \equiv 1 \pmod p$. Якщо $a^{2k+1} \equiv 1 \pmod p$, то $x \equiv \pm a^{k+1} \pmod p$, а якщо $a^{2k+1} \equiv -1 \pmod p$, то $x \equiv \pm a^{k+1} \cdot 2^{2k+1} \pmod p$. **49.** *Вказ.* a) Мультиплікативна група $\mathbb{Z}_n^*$ є циклічною. b) Якщо $n = 2^k$ $(k > 2)$, то розв'язками будуть $x \equiv \pm 1 \pmod n$ та $x \equiv \pm 1 + 2^{k-1} \pmod n$; якщо $n = p^k \cdot b$, де $(p, b) = 1$, $2 \nmid p$ і $b > 2$, то розв'язок кожної із систем $x \equiv \pm 1 \pmod{p^k}$, $x \equiv \pm 1 \pmod b$, буде і розв'язком конґруенції $x^2 \equiv 1 \pmod n$. **50.** *Вказ.* Оскільки всі $p_i \geq 3$, то жодне p_i не ділить одночасно $x+1$ та $x-1$. Тому $n \mid (x-1)(x+1)$ тоді й лише тоді, коли для деякої підмножини $\{i_1, \ldots, i_r\} \subseteq \{1, 2, \ldots, m\}$ буде $p_{i_1}^{k_{i_1}} \cdots p_{i_r}^{k_{i_r}} \mid (x-1)$ і $\left(n / p_{i_1}^{k_{i_1}} \cdots p_{i_r}^{k_{i_r}}\right) \mid (x+1)$. **51.** *Вказ.* Нехай p — простий дільник числа F_n. Оскільки $2^{2^n} \equiv -1 \pmod p$, то порядок 2 як елемента групи $\mathbb{Z}_p^*$ дорівнює 2^{n+1}. З іншого боку, за малою теоремою Ферма $2^{p-1} \equiv 1 \pmod p$. Тому $2^{n+1} \mid p-1$. **52.** a) $x \equiv 10852 \pmod{11040}$; b) $x \equiv 9677 \pmod{10800}$. **53.** a) $x \equiv 2079 \pmod{5850}$; b) $x \equiv 873 \pmod{11220}$. **54.** $a \equiv 3 \pmod{10}$. **55.** $x = 3, y = 5$. *Вказ.* Розгляньте остачі від ділення на 3. **56.** *Вказ.* Якщо $x^2 \equiv a$, то $(kx)^2 \equiv -a$.

57. a) -1; b) 1. **58.** $p \equiv 1 \pmod 3$. *Вказ.* $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) =$
$= (-1)^{\frac{p-1}{2}}(-1)^{\frac{(3-1)(p-1)}{4}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$. **59.** a) $\{8, 23\}$; b) $\varnothing$.

Заняття 5. **10.** a) Ні; b) так; c) так. **11.** *Вказ.* Якщо $|X| > 1$, то в кільці $\mathrm{Map}(X, P)$ є дільники 0. **12.** 1. *Вказ.* Адитивна група має порядок 4, тому для всіх x буде $(x + x)(x + x) = 0$, звідки $x + x = 0$. Множення в мультиплікативній групі $\{1, a, b\}$ визначається однозначно. **13.** 2. **14.** *Вказ.* Випливає із зад. 12. **15.** a), c), d), e) — так; b) — ні. **16.** a) $\varnothing$; b) 2; c) 2, 3; d) 3, 5, 6. *Вказ.* n має бути квадратичним нелишком за модулем p. **17.** Ні. *Вказ.* Поле $\mathbb{Q}$ не має власних підполів. **18.** Так. *Вказ.* Наприклад, поля раціональних функцій $P(x)$ і $P(x^2)$. **20.** *Вказ.* $a + \cdots + a = a(1 + \cdots + 1)$. **21.** Тоді й лише тоді, коли одне з підполів міститься в іншому. **22.** *Вказ.* Мультиплікативна група поля має порядок $n - 1$. **23.** a) $\{-1, 2\sqrt{2} - 3\}$; b) $\varnothing$; c) $\varnothing$; d) $\varnothing$. **24.** a) 7, b) 79. **25.** Наприклад, $\mathbb{Z}_p(x)$. **26.** *Вказ.* Доведіть, що $(a+b)^p = a^p + b^p$, і для p^n застосуйте індукцію за показником n. **27.** *Вказ.* Із зад. 26 випливає, що в полі $\mathbb{Z}_p$ $a^p = (1+\cdots+1)^p = 1^p+\cdots+1^p = a$. **28.** *Вказ.* $a^{pk} - 1 = (a^k - 1)^p$. **29.** Так, наприклад, $\mathbb{C}(x)$. **31.** *Вказ.* Мінімальним многочленом кожного з чисел $\sqrt{2 + \sqrt{3}}$ і $\sqrt{2 - \sqrt{3}}$ буде $x^4 - 4x^2 + 1$. Для доведення його незвідності зробіть заміну $x = y + 1$ і застосуйте ознаку Айзенштайна. **32.** b) Ні. *Вказ.* a) Нехай $\mathrm{char}(P) \neq 2$, $F = P(b)$ і $m_b(x) = x^2 + \alpha x + \beta$. Тоді $F = P(b + \frac{\alpha}{2})$ і $(b + \frac{\alpha}{2})^2 = \frac{\alpha^2}{4} - \beta \in P$. b) Розгляньте розширення степеня 2 поля $\mathbb{Z}_2$. **34.** *Вказ.* x є коренем многочлена $y^2 - x^2 \in P(x^2)[y]$. **36.** a) $x^2 - 3$; b) $x^{50} - 8$; c) $x - 1 - \sqrt{3}$; d) $x^2 - 2\sqrt{3}x + 1$. **36.** a) $18a^2 - 32a + 18$; b) $-81a^2 + 180a - 108$; c) $-\frac{1}{6}a^2 - \frac{1}{2}a + \frac{3}{2}$; d) $\frac{1}{17}(66a^2 - -151a+89)$. **36.** $x^3 + x^2 + 2x + 1$. **38.** *Вказ.* Полем розкладу буде $\mathbb{Q}(\sqrt{a})$. **39.** *Вказ.* Розгляньте вежу розширень $P(a, b) \supseteq P(a) \supseteq P$. **40.** *Вказ.* Розгляньте вежу розширень $P(a) \supseteq P(b) \supseteq P$. **41.** Ні. **42.** *Вказ.* Розгляньте вежу розширень $F \supseteq P(a) \supseteq P$. **43.** a) 2, база 1, $\sqrt{5}$; b) 3, база 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$; c) 4, база 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$; d) 2, база 1, i. **44.** a) 2, b) 6, c) 8, d) 2, e) 4. *Вказ.* c) Покажіть, що поле розкладу містить $\sqrt[4]{2}$ та i, а тому збігається з $\mathbb{Q}(\sqrt[4]{2})(i)$. d) Досить приєднати первісний корінь степеня 6 з 1, який є коренем многочлена $x^2 - x + 1$. **45.** a) $p-1$, b) $\varphi(n)$, c) $p(p-1)$. *Вказ.* c) Полем розкладу є $\mathbb{Q}(\sqrt[p]{a})(\varepsilon_p)$, де ε_p — первісний корінь степеня p з 1. **46.** *Вказ.* Якщо $P = \{a_1, \ldots, a_n\}$, то многочлен $f(x) = (x-a_1)\cdots(x-a_n)+1 \in P[x]$ не має в P коренів. **47.** *Вказ.* Замість перевірки аксіом можна зауважити, що $(x - 1) \oplus (y - 1) = (x + y) - 1$, $(x - 1) \odot (y - 1) = xy - 1$. **49.** *Вказ.* a) Сума не змінюється при множенні на $a \neq 1$; b) сума не змінюється при множенні на $a^2 \neq 1$. **50.** *Вказ.* Для кожного $a \neq 0$

відображення $K \setminus \{0\} \to K \setminus \{0\}$, $x \mapsto ax$, є бієкцією. **53.** c) Наприклад, $\mathbb{Z}_p(x)$. **54.** *Вказ.* Використовуючи теорему Вільсона і рівність $(p-1)! = (p-k)!(p-(k-1))(p-(k-2))\cdots(p-2)(p-1) \equiv (p-k)!\times$ $\times(k-1)!(-1)^{k-1}$, доведіть, що $\binom{p-1}{k} \equiv (-1)^k \pmod p$. **55.** *Вказ.* Адитивна група власного підполя повинна мати порядок p і містити одиницю поля. **56.** *Вказ. a)* $\Rightarrow$ *b).* Якщо $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$ — ізоморфізм, то із $a \in \mathbb{Q}$ випливає, що $\varphi(a) = a$ і $(\varphi(\sqrt{a}))^2 = a$. А тому або $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}) = \mathbb{Q}$, або існують такі раціональні числа u і v, що $u + v\sqrt{b} = \sqrt{a}$. *b)* $\Rightarrow$ *c).* Якщо $\sqrt{a} \in \mathbb{Q}$, то $\sqrt{a} = \frac{p}{q}$, $\sqrt{b} = \frac{m}{n}$ і $\frac{a}{b} = \frac{p^2n^2}{q^2m^2}$. Якщо ж $\sqrt{a} \notin \mathbb{Q}$, то з рівності $u + v\sqrt{b} = \sqrt{a}$, де $u, v \in \mathbb{Q}$, випливає, що $2uv\sqrt{b} = a^2 - v^2b^2 - u^2$. Але тоді $uv = 0$. Рівність $v = 0$ суперечить припущенню, що $\sqrt{a} \notin \mathbb{Q}$. Тому $u = 0$ і $a^2 = v^2b^2$. Імплікації *c)* $\Rightarrow$ *b)* і *b)* $\Rightarrow$ *a)* очевидні. **57.** *Вказ.* Нехай $a_0 + a_1x + \cdots + x^n \in A[x]$ — мінімальний многочлен для a. Тоді розширення $P(a, a_0, a_1, \ldots, a_{n-1}) \supseteq P$ є скінченним. **58.** b) Ні. *Вказ.* a) Розгляньте вежу розширень $P(a) \supseteq$ $\supseteq P(a^2) \supseteq P$ і врахуйте, що $[P(a) : P(a^2)] \leq 2$. b) Розгляньте $P = \mathbb{R}$ і $a = 1+i$. **59.** *Вказ.* База розширення $L \supseteq P$ буде також базою розширення $L(x) \supseteq P(x)$. **60.** *Вказ.* Якщо $a = \frac{f(x)}{g(x)}$, то x є коренем многочлена $ag(y) - f(y) \in P(a)[y]$. **61.** *Вказ.* $P(t_1, \ldots, t_n) = P(t_1, \ldots, t_{n-1})(t_n)$. Далі використайте зад. 7 та індукцію за n. **62.** *Вказ.* Нехай ізоморфізм $\varphi : \mathbb{Q}(x, y) \to \mathbb{Q}(x)$ існує і $\varphi(x) = \frac{g(x)}{h(x)} = a$. Згідно зад. 60 поле $\mathbb{Q}(x)$ є простим алгебричним розширенням поля $\mathbb{Q}(a) = \varphi(\mathbb{Q}(x))$. Зокрема, $[\mathbb{Q}(x) : \mathbb{Q}(a)] < \infty$. З іншого боку, $\mathbb{Q}(x) = \varphi(\mathbb{Q}(x, y))$ і $[\mathbb{Q}(x) : \mathbb{Q}(a)] =$ $= [\varphi(\mathbb{Q}(x, y)) : \varphi(\mathbb{Q}(x))] = [\mathbb{Q}(x, y) : \mathbb{Q}(x)] = \infty$. **63.** a) $p-1$; база 1, ε_p, ε_p^2, $\ldots$, ε_p^{p-2}. b) 2; база 1, ε_6. c) 6; база 1, $\sqrt[3]{3}$, $\sqrt[3]{9}$, ε_3, $\varepsilon_3\sqrt[3]{3}$, $\varepsilon_3\sqrt[3]{9}$. *Вказ.* a) ε_p є коренем незвідного многочлена $\frac{x^p-1}{x-1} = 1+x+\cdots+x^{p-1}$. b) ε_6 є коренем незвідного многочлена $\frac{x^6-1}{(x^3-1)(x+1)} = 1 - x + x^2$. c) Розгляньте вежу розширень $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{Q}(\varepsilon_3, \sqrt[3]{3})$. **64.** *Вказ.* Застосуйте індукцію за степенем многочлена $f(x)$. **65.** *Вказ.* a) Позаяк $[P(a,b) : P] =$ $= [P(a,b) : P(a)]\cdot[P(a) : P] = [P(a,b) : P(b)]\cdot[P(b) : P]$ то $m \,\big|\, [P(a,b) : P]$, $n \,\big|\, [P(a,b) : P]$, звідки $mn \,\big|\, [P(a,b) : P]$ і $mn \leq [P(a,b) : P]$. З іншого боку, $[P(a,b) : P(a)] \leq [P(b) : P]$, тому $[P(a,b) : P] \leq mn$. b) Напр., $a = \sqrt{2}$, $b = \sqrt[4]{2}$ або $a = \sqrt[6]{2}$, $b = \sqrt[10]{2}$. **66.** *Вказ.* Нехай a — корінь многочлена $f(x)$. До розширень $F \supseteq P$ і $P(a) \supseteq P$ застосуйте міркування із вказ. до зад. 65.a). **67.** Збігається з $\mathbb{Q}$. *Вказ.* За основною теоремою про симетричні многочлени $a_1^{19} + a_2^{19} + a_3^{19}$ є многочленом із цілими коефіцієнтами від коефіцієнтів многочлена $x^3 - x + 1$. **68.** *Вказ.* У своєму полі розкладу

x^p-a має розклад $x^p-a=(x-b)(x-\varepsilon b)\cdots(x-\varepsilon^{p-1}b)$, де $b^p=a$, а $\varepsilon\neq 1$ — корінь степеня p з 1. Якщо x^p-a є звідним, то розклад має вигляд $x^p-a=(x^k+\cdots+b^k\varepsilon^q)(x^{p-k}+\cdots+b^{n-k}\varepsilon^r)$. НСД$(k,p-k)=1$, тому $uk+v(p-k)=1$ для деяких u і v. Але тоді корінь $b^{uk}\varepsilon^{uq}\cdot b^{v(p-k)}\varepsilon^{vr}=$ $=b\varepsilon^{uq+vr}$ многочлена x^p-a належить P. **69.** *Вказ.* Многочлен x^4-2 незвідний над $\mathbb{Q}$ і його коренями є $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. $\mathbb{Q}(\sqrt[4]{2},-\sqrt[4]{2})=\mathbb{Q}(\sqrt[4]{2})$ і $[\mathbb{Q}(\sqrt[4]{2},-\sqrt[4]{2}):\mathbb{Q}]=4$. У той же час розширення $\mathbb{Q}(\sqrt[4]{2},i\sqrt[4]{2})\supset\mathbb{Q}$ має степінь 8, тому $\mathbb{Q}(\sqrt[4]{2},-\sqrt[4]{2})\not\supset\mathbb{Q}(\sqrt[4]{2},i\sqrt[4]{2})$. **70.** *Вказ.* $a=\left(\frac{1+a}{2}\right)^2-\left(\frac{1-a}{2}\right)^2$. **71.** *Вказ.* Використайте зад. 70. **72.** Наприклад, $\mathbb{Q}(x^4)\subset\mathbb{Q}(x^2)\subset\mathbb{Q}(x)$. **73.** *Вказ.* Якщо ε — первісний корінь степеня n з 1, то $-\varepsilon$ — первісний корінь степеня $2n$ з 1. **75.** a) Ні; b) ні; c) ні. *Вказ.* b) $(i,1)\odot(1,i)=(0,0)$; c) $(\sqrt{2},1)\odot(\sqrt{2},-1)=(0,0)$. **76.** a) Так; b) ні. **77.** 2 або 461. **78.** Ні. *Вказ.* Рівняння $x^2=3$ має розв'язок у першому полі і не має в другому. **79.** a) a^2+a+1, a^2-1, a^2-2; b) x^3-2x^2-3x-1. **80.** a) 4; база 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$. b) 6; база 1, $\sqrt[6]{3}$, $\sqrt[6]{9}$, $\sqrt[6]{27}$, $\sqrt[6]{81}$, $\sqrt[6]{243}$. c) 4; база 1, $\sqrt{3}$, i, $i\sqrt{3}$. **81.** a) 4; база 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$. b) 6; база 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$, ε, $\varepsilon\sqrt[3]{2}$, $\varepsilon\sqrt[3]{4}$, де ε — первісний корінь степеня 3 з 1. d) 8; база 1, $\sqrt[4]{5}$, $\sqrt[4]{5^2}$, $\sqrt[4]{5^3}$, i $i\sqrt[4]{5}$, $i\sqrt[4]{5^2}$, $i\sqrt[4]{5^3}$. *Вказ.* c) Полем розкладу є $\mathbb{Q}(\sqrt[4]{5},i)$.

Заняття 6. **14.** Тільки тотожний і $z\mapsto\overline{z}$. **15.** a) 2 автоморфізми: тотожний і $a+b\sqrt{3}\mapsto a-b\sqrt{3}$; b) тільки тотожний; c) 2 автоморфізми: тотожний і $a+b\sqrt[4]{2}+b\sqrt[4]{4}+b\sqrt[4]{8}\mapsto a-b\sqrt[4]{2}+b\sqrt[4]{4}-b\sqrt[4]{8}$. **16.** Кількість автоморфізмів поля розкладу многочлена дорівнює степеню розширення. a) Поле розкладу збігається з $\mathbb{Q}(\sqrt[3]{2},\varepsilon_3)$, де ε_3 — первісний корінь степеня 3 з 1, тому досить вказати дію автоморфізмів на $\sqrt[3]{2}$ і ε_3:

	id	φ_2	φ_3	φ_4	φ_5	φ_6
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\varepsilon_3\sqrt[3]{2}$	$\varepsilon_3^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\varepsilon_3\sqrt[3]{2}$	$\varepsilon_3^2\sqrt[3]{2}$
ε_3	ε_3	ε_3^2	ε_3	ε_3^2	ε_3	ε_3^2

.

b) Поле розкладу збігається з $\mathbb{Q}(\sqrt[4]{2},i)$, тому досить вказати дію автоморфізмів на $\sqrt[4]{2}$ і i:

	id	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

. **17.** a) Наприклад, $P=\mathbb{Q}(\sqrt[n]{2})$. b) Ні. *Вказ.* b) Розгляньте розширення $P\supset\mathbb{Q}$ степеня 2. **18.** Ні. *Вказ.* $\mathrm{Aut}(\mathbb{R})=E$ (див. зад. 2), але $\mathbb{R}$ містить багато підполів із нетривіальною групою автоморфізмів. **19.** *Вказ.* Кожен автоморфізм однозначно визначається образом елемента ε_n. Образом первісного кореня має бути первісний корінь, тобто елемент ε_n^k, де k взаємно просте з n. **20.** a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\varepsilon_5)$; c) $\mathbb{Q}(\sqrt{2},\sqrt{3})$; d) $\mathbb{Q}(\varepsilon_7)$.

Вказ. b),d) Використайте зад. 19; c) використайте розв'язання зад. 3.c. **22.** a) правильна, b) і c) — ні. *Вказ.* a) F є полем розкладу деякого $f(x) \in P[x]$. Але $f(x) \in K[x]$ і F лишається його полем розкладу. b) Розгляньте $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ і використайте зад. 21. c) Розгляньте $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$, де ε_3 — первісний корінь степеня 3 з 1, або $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$. **23.** a), d), e) так; b), c) ні. *Вказ.* a),d),e) Дані поля є полями розкладів многочленів x^2-2, $(x^2-2)(x^2+1)$, x^3-2 відповідно; b) x^3-2 має в полі $\mathbb{Q}(\sqrt[3]{2})$ лише 1 корінь, c) x^4-2 має в полі $\mathbb{Q}(\sqrt[4]{2})$ лише 2 корені. **24.** a) S_2; b) K_4. *Вказ.* a) $x^4+x^2+1 = (x^2+x+1)(x^2-x+1)$; коренями першого множника є ε_6^2, ε_6^4, а другого — ε_6, ε_6^5, де ε_6 — первісний корінь степеня 6 з 1. Тому дане поле збігається з полем розкладу многочлена x^2-x+1. b) Коренями x^4+1 є ε_8, ε_8^3, ε_8^5, ε_8^7, де ε_8 — первісний корінь степеня 8 з 1. **25.** a) $\mathbb{Q}(\sqrt{2})$, b) $\mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$, де ε_3 — первісний корінь степеня 3 з 1, c) $\mathbb{Q}(\sqrt[4]{2}, i)$. **26.** *Вказ.* Розширення $K \supseteq \mathbb{Q}$ є нормальним. За теоремою про примітивний елемент $K = \mathbb{Q}(a)$. За f можна взяти мінімальний многочлен $\min_a(x)$. **27.** Тільки $GF_{p^{11}}$ і $\mathbb{Z}_p$. **28.** *Вказ.* У полі немає нетривіальних ідеалів, тому такий ендоморфізм є ін'єктивним. **29.** Ні. *Вказ.* Над кожним полем існує нескінченно багато незвідних многочленів. **30.** *Вказ.* $F = P(a)$, де a — твірний елемент циклічної групи P^*. **31.** *Вказ.* Поле F є полем розкладу многочлена $x^{|F|} - x$. **32.** c) $f(x) = (x+a)(x+a^2)(x+a^2+a)$; d) $a+1 = a^3$, $a^2+a = a^4$, $a^2+a+1 = a^5$, $a^2+1 = a^6$; e) a^2. **33.** c) $a+1$, $2a+1$, $2a+2$, $a+2$; d) $x^2+1 = (x+a)(x+2a)$, $x^2+x+1 = (x+2)^2$, $x^2+2x+2 = (x-a+1)(x+a+1)$. **34.** a) a, $a+1$, a^2, a^2+1, a^2+a, a^2+a+1; $g(x) = (x^2+x+1)^2$, $h(x) = (x+a+1)(x+a^2+1)(x+a^2+a)$. b) a, $a+1$, a^2, a^2+1, a^2+a, a^2+a+1; $g(x) = (x+1)^2(x^2+x+1)$, $h(x) = (x+a+1)(x+a^2+1)(x+a^2+a+1)$. c) a, $a+1$, $2a$, $2a+2$; $g(x) = (x+2)(x^3+2x+2)$, $h(x) = (x+a+1)(x+a)$. d) a, $2a+1$, $2a$, $a+2$; $g(x) = (x+2)(x^3+x^2+2)$, $h(x) = (x+a+1)(x+2a+2)$. **35.** a) $\alpha a+\beta \mapsto \alpha b+(\alpha+\beta)$, 2 способи; b) $\alpha a^2+\beta a+\gamma \mapsto (\alpha+\beta)b^2+(2\alpha+\beta)b+\gamma$, 3 способи. *Вказ.* a має переходити в корінь многочлена $f(x)$ у полі $\mathbb{Z}_3(b)$. **36.** $(a, a+1)$. **37.** a) x^3+x+1, x^3+x^2+1; b) x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$. **38.** a) 6; b) 9; c) 18. **39.** a) Так, b) ні. *Вказ.* b) $x^4+3x^3+3x^2+3x+3 = (x^2+x+2)(x^2+2x-1)$. **40.** a) 36; b) 240; c) 1620. **41.** a) $(x^2+1)(x^2+2x+2)$; b) $(x+3)(x^2+4x+2)$; c) $(x+2)(x^2+2x+3)$. **42.** a) α, α^2, α^3+1, $\alpha^3+\alpha^2+\alpha$; b) $\alpha+1$, α^2+1, α^3, $\alpha^3+\alpha^2+\alpha+1$. **43.** Тільки тотожний і $z \mapsto \overline{z}$. **44.** a) $\mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$; b) $\mathbb{Q}(\varepsilon_7 + \overline{\varepsilon_7})$; c) $\mathbb{Q}(\varepsilon_{11} + \overline{\varepsilon_{11}})$, де ε_n — первісний корінь степеня n з 1. *Вказ.* a) Поле $\mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$ є полем розкладу многочлена x^3-2, а його група автоморфізмів індукує всі перестановки множини коренів цього многочлена. b) $\mathbb{Q}(\varepsilon_7 + \overline{\varepsilon_7})$ є

полем розкладу многочлена x^3+x^2-2x-1 з коренями $a_1=\varepsilon_7+\overline{\varepsilon_7}$, $a_2=a_1^2-2=\varepsilon_7^2+\overline{\varepsilon_7}^2$, $a_3=a_2^2-2=\varepsilon_7^4+\overline{\varepsilon_7}^4$. Зокрема, $[\mathbb{Q}(\varepsilon_7+\overline{\varepsilon_7}):\mathbb{Q}]=3$. c) $\mathbb{Q}(\varepsilon_{11}+\overline{\varepsilon_{11}})$ є полем розкладу многочлена $x^5+x^4-4x^3-3x^2+3x+1$ з коренями $a_1=\varepsilon_{11}+\overline{\varepsilon_{11}}$, $a_2=a_1^2-2=\varepsilon_{11}^2+\overline{\varepsilon_{11}}^2$, $a_3=a_2^2-2=\varepsilon_{11}^4+\overline{\varepsilon_{11}}^4$, $a_4=a_3^2-2=\varepsilon_{11}^8+\overline{\varepsilon_{11}}^8=\varepsilon_{11}^3+\overline{\varepsilon_{11}}^3$, $a_5=a_4^2-2=\varepsilon_{11}^6+\overline{\varepsilon_{11}}^6$. Зокрема, $[\mathbb{Q}(\varepsilon_{11}+\overline{\varepsilon_{11}}):\mathbb{Q}]=5$. **45.** A_3 і S_3. *Вказ.* Група автоморфізмів точно діє на множині коренів многочлена. **46.** Ізоморфна групі $\mathbb{Z}_p^*$. *Вказ.* $f(x)$ незвідний і коренями його є всі первісні корені $\varepsilon_p,\varepsilon_p^2,\dots,\varepsilon_p^{p-1}$ степеня p з 1. Тому $P=\mathbb{Q}(\varepsilon_p)$ і $\mathrm{Aut}(P)=\{\varphi_1,\dots,\varphi_{p-1}\}$, де $\varphi_i(\varepsilon_p)=\varepsilon_p^i$. **47.** Група дробово–лінійних перетворень $t\to\frac{at+b}{ct+d}$, $ad-bc\neq 0$. **48.** *Вказ. I спосіб.* Розширення $\mathbb{Q}\subseteq K$ є простим алгебричним, отже, $K=\mathbb{Q}(a)$. Степінь мінімального многочлена $m_a(x)$ дорівнює $[K:\mathbb{Q}]$, отже, $m_a(x)$ має дійсний корінь b. Із нормальності розширення $\mathbb{Q}\subseteq K$ випливає, що $\mathbb{Q}(a)=\mathbb{Q}(b)$. Тому $K\subseteq\mathbb{R}$. *II спосіб.* K є полем розкладу многочлена з раціональними коефіцієнтами. Якщо $\mathbb{Q}\not\subseteq K$, то відображення $z\mapsto\overline{z}$ є автоморфізмом порядку 2 поля K. Але з нормальності розширення $\mathbb{Q}\subseteq K$ випливає, що $|\mathrm{Aut}(K)|=[K:\mathbb{Q}]$. **49.** C_4. *Вказ.* Коренями многочлена x^5+1 є ε_{10}, ε_{10}^3, ε_{10}^7, ε_{10}^9 і -1, де ε_{10} — первісний корінь степеня 10 з 1. Тому $P=\mathbb{Q}(\varepsilon_{10})$. Група породжується автоморфізмом $\varphi(\varepsilon_{10})=\varepsilon_{10}^3$. **51.** $\varphi(n)$. *Вказ.* $P=\mathbb{Q}(\varepsilon_n)$, де ε_n — первісний корінь степеня n з 1. Тому $[P:\mathbb{Q}]=|\mathrm{Aut}\mathbb{Q}(\varepsilon_n)|$. Далі див. зад. 19. **52.** *Вказ.* Над полем розкладу $x^p-a=(x-\alpha)^p$. Якщо x^p-a звідний над P, то із факторіальності $P[x]$ випливає, що $x^p-a=(x-\alpha)^m(x-\alpha)^n$, звідки $\alpha^m,\alpha^n\in P$. Але тоді m і n взаємно прості і $\alpha\in P$. **53.** b) $f(x)=(x-a)^p$. **54.** b) Ні. *Вказ.* a) У полі характеристики p $(a+b)^p=a^p+b^p$, а в полі $\mathbb{Z}_p$ відображення $a\mapsto a^p$ є тотожним. b) Якщо $|P|>p$, то відображення $a\mapsto a^p$ не є тотожним. **55.** *Вказ.* Мультиплікативна група F^* нескінченного поля характеристики p містить підгрупу порядку $p-1$, а поля характеристики 0 — нециклічну підгрупу $\mathbb{Q}^*$. **56.** *Вказ.* Використовуючи циклічність групи $\mathbb{Z}^*$, покажіть, що $\sum_{a\in\mathbb{Z}_p}a^i=0$ для кожного $0\leq i<p-1$. **57.** *Вказ.* b) H є ядром гомоморфізму $x\mapsto x^{(q-1)/2}$ групи GF_q^*. **58.** a) $GF_{p^{\text{НСД}(n,m)}}$; b) $GF_{p^{\text{НСК}(n,m)}}$. **59.** *Вказ.* b) Із $[K:P]=n$, випливає, що $|\mathrm{Aut}\,(K:P)|\leq n$. Щоб показати, що φ, φ^2, …, φ^n — попарно різні, розгляньте образи при цих відображеннях твірного елемента a групи K^*. **60**. a) $\frac{q^2-q}{2}$; b) $\frac{q^3-q}{3}$; c) $\frac{q^4-q^2}{4}$. **61.** a) 99; b) 186; c) 335. **62.** *Вказ.* Розгляньте мінімальний многочлен $m_a(x)$, де a — примітивний елемент розширення $GF_{p^{nk}}\supseteq GF_{p^n}$. **63.** *Вказ.* x^p-x не має кратних коренів і розкладається над $\mathbb{Z}_p$ на лінійні множники.

64. $n-1$. *Вказ.* Відображення $y \mapsto y^p + y$ є лінійним перетворенням GF_{p^n} як векторного простору над GF_p. Ядром цього перетворення є GF_p. **65.** *Вказ.* Якщо -1 і 2 є квадратичними нелишками за модулем p, то -2 є квадратичним лишком. Далі скористайтесь рівностями $x^4+1 = x^4-(-1) = (x^4 \pm 2x^2+1) \mp 2x^2$. **66.** $c_n(q) = \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)\cdots$ $\cdots\left(1-\frac{1}{q^n}\right)$. *Вказ.* Послідовність $c_n(q)$ є обмеженою монотонно спадною, тому має границю, додатність якої випливає з існування границі для суми $\frac{1}{q}+\frac{1}{q^2}+\cdots+\frac{1}{q^n}+\cdots$. **67.** *Вказ.* Усі елементи поля $\mathbb{Z}_p[x]/(f(x))$, відмінні від 0, 1 і -1, розбийте на пари (a, a^{-1}). **68.** c) $q+1$. *Вказ.* a) Можна вважати, що перші 3 вектори — це $(1,0,0)$, $(0,1,0)$ і $(0,0,1)$, а решта вибраних векторів мають вигляд $(1,a,b)$, де $a \neq 0$, $b \neq 0$. Покажіть, що коли $(1,a_1,b_1) \neq (1,a_2,b_2)$, то $a_1 \neq a_2$. b) Розгляньте вектори $(1,a^k,a^{2k})$, де a — твірний мультиплікативної групи поля GF_q^3. **69.** $f(x) = (x-a)(x-a^p)\cdots(x-a^{p^{n-1}})$. *Вказ.* a) Елементи a, a^p, a^{p^2}, $\ldots$, $a^{p^{n-1}}$ є коренями $f(x)$ і попарно різні. Справді, нехай $a^{p^m} = a^{p^k}$, де $0 \leq m < k < n$. Тоді $a^{p^k-p^m} = 1$. $f(x)$ є мінімальним многочленом для a і a лежить у деякому підполі $K \subseteq P$ порядку p^n. Позаяк порядок a є дільником p^n-1, то $a^{p^{k-m}-1} = 1$. Отже, a є коренем многочлена $x^{p^{k-m}} - x$ лежить у деякому підполі $P_1 \subseteq P$ порядку p^{k-m}. $[P_1 : \mathbb{Z}_p] = k-m$, тому мінімальний многочлен $m_a(x)$ має степінь $\leq k-m$. b) $|a|$ є дільником числа p^n-1, отже, $|a|$ і p взаємно прості. Тому для довільного кореня a^{p^k} многочлена $f(x)$ буде $|a^{p^k}| = |a|$. **70.** *Вказ.* Множина коренів многочлена $x^{p^n}-x$ утворює підполе порядку p^n. Навпаки, за кожен елемент підполя порядку p^n є коренем цього многочлена. **71.** *Вказ.* Доведіть, що в кільці $\mathbb{Q}[[x]]$ степеневих рядів з коефіцієнтами з поля $\mathbb{Q}$ виконується рівність $1-qz = \prod_{n=1}^{\infty}(1-z^n)^{I_n}$ (де I_n кількість незвідних унітарних многочленів із $GF_q[x]$ степеня n), і скористайтеся нею. **72.** 4 автоморфізми, які діють на $\sqrt{2}$ і $\sqrt{3}$ наступним чином:

	id	φ_2	φ_3	φ_4
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

. *Вказ.* Полем розкладу є $\mathbb{Q}(\sqrt{2},\sqrt{3})$ і степінь розширення $\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}$ дорівнює 4. **73.** a) $\operatorname{Aut}\mathbb{Q}(\varepsilon_7) \simeq \mathbb{Z}_7^* \simeq C_6$; b) $\operatorname{Aut}\mathbb{Q}(\varepsilon_9) \simeq \mathbb{Z}_9^* \simeq C_6$. *Вказ.* Використайте зад. 19. **74.** a) Ні; b) так. *Вказ.* a) Незвідний над $\mathbb{Q}$ многочлен x^3-3 має в полі $\mathbb{Q}(\sqrt[3]{3})$ лише 1 корінь. b) $\mathbb{Q}(\sqrt[3]{3})$ є полем розкладу многочлена $(x^2-2)(x^2-3)$. **75.** -1. *Вказ.* Обчисліть вільний член многочлена $x^{q-1}-1$ за формулою Вієта.

76. a)

	1	a	$a{+}1$	a^2	$a^2{+}1$	$a^2{+}a$	$a^2{+}a{+}1$
1	1	a	$a{+}1$	a^2	$a^2{+}1$	$a^2{+}a$	$a^2{+}a{+}1$
a	a	a^2	$a^2{+}a$	$a{+}1$	1	$a^2{+}a{+}1$	$a^2{+}1$
$a{+}1$	$a{+}1$	$a^2{+}a$	$a^2{+}1$	$a^2{+}a{+}1$	a^2	1	a
a^2	a^2	$a{+}1$	$a^2{+}a{+}1$	$a^2{+}a$	a	$a^2{+}1$	1
$a^2{+}1$	$a^2{+}1$	1	a^2	a	$a^2{+}a{+}1$	$a{+}1$	$a^2{+}a$
$a^2{+}a$	$a^2{+}a$	$a^2{+}a{+}1$	1	$a^2{+}1$	$a{+}1$	a	a^2
$a^2{+}a{+}1$	$a^2{+}a{+}1$	$a^2{+}1$	a	1	$a^2{+}a$	a^2	$a{+}1$

.

b) $x^3+x+1=(x+a)(x+a^2)(x+a^2+a)$, $x^3+x^2+1=(x+a+1)(x+$ $+a^2+1)(x+a^2+a+1)$. c) 7. d) $\alpha a^2+\beta a+\gamma\mapsto\alpha b^2+\beta b+(\alpha+\beta+\gamma)$. *Вказ.* d) a має переходити в корінь многочлена x^3+x+1 у полі $\mathbb{Z}_2(b)$. **77.** 1. **78.** x^3+2x+1, x^3+x^2+1, x^3+x^2+2x+1, x^3+2x^2+1, x^3+2x+2, x^3+x^2+2, x^3+x^2+x+2, x^3+2x^2+2x+2. **79.** $(x+1)^3(x^2+x+1)$. **80.** $\alpha^3+\alpha+1$, $\alpha^3+\alpha$.

Заняття 7. **9.** *Вказ.* Якщо a — корінь многочлена $f(x)$, то b — корінь многочлена $f(x^n)$. **10.** 1, якщо $\sqrt{c}\in\mathbb{Q}$, і 2, якщо $\sqrt{c}\notin\mathbb{Q}$. **11.** a),b),d) — алгебричні, c),e) — трансцендентні. **12.** a) x^4-24x^2+4, b) x^4-22x^2+25, c) x^4+4x^2+36. **13.** a) x^4-10x^2+1; b) x^4-14x^2+81; c) $x^6-9x^4+9x^2-48$; d) x^4+2x^2+25; e) $x^6-6x^5+15x^4-24x^3+27x^2-$ $-18x+6$; f) $x^4+x^3+x^2+x+1$; g) $x^{p-1}+x^{p-2}+\cdots+1$. *Вказ.* c), e) незвідність многочлена випливає з критерію Айзенштайна; f), g) незвідність многочлена випливає з критерію Айзенштайна після заміни $x=y+1$. **15.** *Вказ.* Якщо $z=a+bi$ — алгебричне, то $\overline{z}=a-bi$ — також алгебричне. Але $a=\frac{1}{2}(z+\overline{z})$, $b=\frac{1}{2i}(z-\overline{z})$. **16.** a) $\frac{1}{23}(2+5\sqrt{2}-3\sqrt{3}+4\sqrt{6})$; b) $\frac{1}{284}(-40-27\sqrt{2}+42\sqrt{3}+39\sqrt{6})$; c) $\frac{1}{3}(1+\sqrt[3]{2})$; d) $\frac{1}{3}(-1+\sqrt[3]{4})$; e) $\frac{1}{43}(5+$ $+9\sqrt[3]{2}-\sqrt[3]{4})$; f) $\frac{1}{2}(-1+\sqrt[3]{3})$. **17.** Цілі числа. **18.** a), b), c), e), g) — так; d), f) — ні. **19.** *Вказ.* Нехай $e=\sum_{k=0}^{\infty}1/k!=p/q$. Тоді $e\cdot q!\in\mathbb{N}$. Але $0<\frac{1}{q+1}+\frac{1}{(q+1)(q+2)}+\cdots<\frac{1}{2}+\frac{1}{4}+\cdots<1$. **20.** *Вказ.* Оскільки $a=\frac{1}{2}(e+e^{-1})$, то e є розв'язком рівняння $x^2-2ax+1=0$. **21.** *Вказ.* a) $\sin 18^\circ$ є коренем рівняння $4x^2+2x-1$; b) використайте a); c),d) використайте b). **22.** Лише кути, кратні 3°. *Вказ.* Побудовність кутів, кратних 3°, випливає із зад. 21. Непобудовність 1°, 2°, 4°, 5°, 10° випливає із непобудовності 20°; непобудовність 7° — із непобудовності $2^\circ=30^\circ-4\cdot 7^\circ$; непобудовність 8° і 16° — із непобудовності 4°; непобудовність 11° — із непобудовності $1^\circ=11\cdot 11^\circ-120^\circ$; непобудовність 14° — із непобудовності 7°; непобудовність 17° — із непобудовності $4^\circ=2\cdot 17^\circ-30^\circ$; непобудовність 19° — зад. 7.b; непобудовність 13° — із

непобудовності $19^\circ = 13\cdot 13^\circ - 150^\circ$. **23.** *Вказ.* Використайте побудовність кута 18°(зад. 21.a). **24.** Ні. *Вказ.* Якби можна було побудувати правильний 9–кутник, то можна було б побудувати кут 20°. **25.** *Вказ.* Побудуйте спочатку рівновеликий прямокутник, більша сторона якого дорівнює найбільшій стороні трикутника. Потім від прямокутника зі сторонами a і b перейдіть до квадрата зі стороною $\sqrt{ab}$. **26.** *Вказ.* Обчисліть кут при основі трикутника. **27.** Наприклад, $y = x + \pi$, $y = \pi x$ і $y = x$. *Вказ.* Якщо пряма містить конструктивні точки A і B, то довільна точка C цієї прямої, для якої $\frac{|AC|}{|AB|} \in \mathbb{Q}$, також буде конструктивною. **28.** a) $\sqrt{2}$ і $\sqrt[3]{3}$; b) $\frac{-1+i\sqrt{3}}{2}$ і $\sqrt[3]{3}$. *Вказ.* a) $\mathbb{Q}(\sqrt[3]{3}, \sqrt{2}) = \mathbb{Q}(\sqrt[3]{3}\sqrt{2})$. b) Розгляньте многочлен $x^3 - 3$. **29.** $x^3 - x^2 - 2x + 1$. *Вказ.* Довжина сторони правильного 14–кутника дорівнює $2\sin\frac{\pi}{14} = -2\cos\frac{4\pi}{7} = -2(\varepsilon + \varepsilon^{-1})$, де $\varepsilon = \cos\frac{4\pi}{7} + i\sin\frac{4\pi}{7}$ — корінь 7–го степеня з 1. Після ділення обох частин рівняння $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ на x^3 одержимо $\left(x+\frac{1}{x}\right)^3 + \left(x+\frac{1}{x}\right)^2 - 2\left(x+\frac{1}{x}\right) - 1 = 0$. Тому число $z = 2\cos\frac{4\pi}{7}$ задовольняє рівнянню $z^3 + z^2 - 2z - 1 = 0$. Але тоді $x = 2\sin\frac{\pi}{14} = -2\cos\frac{4\pi}{7}$ задовольняє рівнянню $x^3 - x^2 - 2x + 1 = 0$. **30.** Для $n > 1$ — ні. *Вказ.* $\sqrt{2} + \sqrt{3}$ має степінь 4. Якщо $n > 2$ і a та b — алгебричні числа степенів n та $n - 1$ відповідно, то $[\mathbb{Q}(a, b) : \mathbb{Q}] = n(n - 1)$, а тому примітивний елемент розширення $\mathbb{Q}(a, b) \supset \mathbb{Q}$ має степінь $n(n - 1)$. **31.** *Вказ.* a є власним числом матриці (α_{ij}) порядку k. **32.** *Вказ.* Нехай $a \in \mathbb{C}$ трансцендентне число. Множина $\mathbb{Q}_a$ всіх чисел, алгебричних відносно поля $\mathbb{Q}(a)$, є зліченним алгебрично замкненим полем. Оскільки $\mathbb{C} = \bigcup_a \mathbb{Q}_a$, то серед полів $\mathbb{Q}_a$ є континуум різних. **33.** *Вказ.* Випливає із зад. 5. **34.** *Вказ.* Використайте твердження **3**. **35.** *Вказ.* Використайте зад. 34 і те, що α є коренем многочлена $x^n + a_1x^{n-1} + \cdots + a_n$ тоді й лише тоді, коли α^{-1} є коренем многочлена $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + 1$. **36.** *Вказ.* За допомогою основної теореми про симетричні многочлени доведіть, що многочлен $\prod(x^n + a_1^{(i_1)}x^{n-1} + \cdots + a_n^{(i_n)})$ має цілі коефіцієнти (коефіцієнти $a_1^{(i_1)}, \ldots, a_n^{(i_n)}$ незалежно пробігають всі корені відповідно мінімальних многочленів $\min_{a_1}(x)$, $\ldots$, $\min_{a_n}(x)$). **38.** *Вказ.* a) Із рівності $\cos(4\cdot 36^\circ) = -\cos 36^\circ$ випливає, що $\cos 36^\circ$ задовольняє рівняння $2(2x^2 - 1)^2 - 1 = -x$, розв'язками якого є числа -1, $1/2$ і $(1 \pm \sqrt{5})/4$. **39.** *Вказ.* Правильний n-кутник побудовний тоді й лише тоді, коли первісний корінь ε_n степеня n з 1 є конструктивним. Для простого числа p ε_p є коренем незвідного многочлена $x^{p-1} + x^{p-2} + \cdots + x + 1$, тому $[\mathbb{Q}(\varepsilon_p) : \mathbb{Q}] = p - 1$. **40.** Ні. *Вказ.* Із побудовності трикутника випливала б і побудовність його висоти h, опущеної на основу. Із подібності

трикутників для висоти легко одержати співвідношення $\frac{h-1}{5} = \frac{1}{\sqrt{25-h^2}}$, звідки $h^3 - h^2 - 24h + 50 = 0$. Незвідність над $\mathbb{Q}$ цього многочлена випливає з відсутності раціональних коренів. Позаяк степінь многочлена дорівнює 3, то висота h не є побудовною. **41.** Наприклад, $x^2 + y^2 = \pi^2$, $(x-\pi)^2 + y^2 = \pi^2$, $(x-1)^2 + (y-\sqrt{\pi^2-1})^2 = \pi^2$, $x^2 + y^2 = 1$. *Вказ.* Якщо коло містить 3 конструктивні точки, то його центр також буде конструктивною точкою, і для кожної прямої вигляду $y = kx + b$ ($k \in \mathbb{Q}$), яка перетинає коло в конструктивній точці, друга точка перетину також буде конструктивною. **43.** *Вказ.* Використайте твердження **8.** **44.** $n = 2^k$. *Вказ.* Досить довести неможливість поділу довільного кута на p рівних частин для простих $p \neq 2$. Але з можливості такого поділу випливала б можливість побудови правильного p^2–кутника. **45.** Будь–який кут вигляду $\frac{360^\circ}{3n+1}$, де n вибирається так, щоб побудова правильного $(3n+1)$–кутника була неможлива (наприклад, $n = 2$ або $n = 4$). *Вказ.* Якщо кут x задовольняє рівність $\frac{x}{3} = \alpha - nx$, де кут α — побудовний, то його трисекція можлива. Зокрема, при $\alpha = 120^\circ$ маємо $x = \frac{360^\circ}{3n+1}$. **46.** a) $x^4 - 20x^2 + 16$; b) $x^4 - 14x^2 + 81$. **47.** a) $x^5 - 3$; b) $x^2 - 4x + 13$; c) $x^4 - 4x^3 - 4x^2 + 16x - 8$. *Вказ.* c) $[\mathbb{Q}(1+\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. **48.** *Вказ.* Якщо число a — алгебричне, то число $\sqrt{1-a^2}$ також алгебричне. **49.** a) $\frac{1}{2}(4\sqrt{2}+2\sqrt{6}-3\sqrt{3}-5)$; b) $5+4\sqrt[3]{2}+3\sqrt[3]{4}$; c) $\frac{1}{10}(-1+2\sqrt[3]{3}+\sqrt[3]{9})$. **50.** *Вказ.* a) $90^\circ - 72^\circ = 18^\circ$; b) $2 \cdot 72^\circ - 120^\circ = 24^\circ$.