КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

А.С. Олійник

Навчальні завдання до практичних занять з Алгебри для студентів 2 курсу спеціальності “комп’ютерна математика”

2018

Практичне заняття 1. Алгебраїчні дії

А1.1 Скількома способами можна визначити бінарну дію на n–елементній множині? Скільки серед цих дій a) будуть комутативними, b) мають нейтральний елемент?

А1.2 Скільки є різних рухів простору, які переводять в себе різносторонній прямокутний паралелепіпед?

А1.3 Побудуйте таблицю множення для множини рухів прямокутника.

А1.4 Як за таблицею Келі для дії $*$ на множині M з'ясувати: a) чи буде дія $*$ комутативною? b) чи є в M ліві(праві) нулі? c) чи є в M ліві (праві) одиниці? d) чи є даний елемент a оборотним зліва (справа)?

А1.5 З'ясуйте, чи буде асоціативною на множині $\mathbb{N}$ дія $m * n = \max(m, n)$.

А1.6 З'ясуйте, чи буде асоціативною на множині $\mathbb{R}$ дія $x * y = \ln(e^x + e^y)$.

А1.7 Чи будуть ізоморфними множини з діями $(\mathbb{N}, +)$ і $(-\mathbb{N}, +)$?

А1.8 Які серед даних множин з діями a) $((0,1), \cdot)$, b) $((0,1], \cdot)$, c) $([0,1), \cdot)$, d) $([0,1], \cdot)$, e) $((1,\infty), \cdot)$, f) $([1,\infty), \cdot)$, g) $((2,\infty), \cdot)$, h) $((3,\infty), \cdot)$ є ізоморфними?

Д1.1 Скільки є різних поворотів простору, які переводять в себе a) куб, b) правильний октаедр?

Д1.2 Побудуйте таблицю множення для множини рухів правильного трикутника.

Д1.3 У кожній з клітинок таблиці

	$\cup$	$\cap$	$\setminus$	$\triangle$
асоціативність				
комутативність				
існування нейтрального елемента				
існування обернених елементів				

поставте знак $+$ або $-$ в залежності від того, має місце чи ні дана властивість для даної дії на множині $\Omega(M)$ всіх підмножин непорожньої множини M.

Д1.4 З'ясуйте, які з наступних дій на множині $\mathbb{N}$ є асоціативними:
a) $m * n = m^n$; b) $m * n = \text{НСК}(m, n)$; c) $m * n = 2mn$; d) $m * n = m^2 + n^2$.

Д1.5 Для кожної з дій з набору $(+,\ -,\ \cdot,\ :)$ на кожній із множин з набору $(\mathbb{N},\ 2\mathbb{N},\ \mathbb{Z},\ 2\mathbb{Z},\ \mathbb{Q},\ \mathbb{Q}^+,\ \mathbb{R},\ \mathbb{R}^+,\ \mathbb{R}^-,\ \mathbb{R}^{>1})$ з'ясуйте, чи мають місце властивості: a) комутативності; b) асоціативності; c) існування нуля; d) існування нейтрального елемента; e) існування обернених елементів.

Д1.6 На множині M^2 визначено такі дії:

a) $(a,b) \circ_1 (c,d) = (a,c)$; b) $(a,b) \circ_2 (c,d) = (a,d)$;

c) $(a,b) \circ_3 (c,d) = (b,c)$; d) $(a,b) \circ_4 (c,d) = (b,d)$.

Які з множин з діями $(M^2, \circ_i), i = 1,2,3,4$, є ізоморфними? Які з цих дій є асоціативними?

Практичне заняття 2. Поняття групи. Порядок елемента

А2.1 Чи утворює групу множина: a) симетричних матриць відносно додавання; b) кососиметричних матриць відносно додавання; c) невироджених матриць відносно додавання; d) невироджених матриць відносно множення; e) матриць з фіксованим визначником d відносно множення; f) діагональних матриць відносно додавання; g) діагональних матриць відносно множення; h) верхніх трикутних матриць відносно множення; i) верхніх нільтрикутних матриць відносно множення; j) верхніх нільтрикутних матриць відносно додавання; k) верхніх унітрикутних матриць відносно множення; l) всіх ортогональних матриць відносно множення; m) верхніх нільтрикутних матриць відносно операції $X \circ Y = X + Y - XY$?

А2.2 Чи утворює групу відносно множення підстановок множина усіх підстановок з S_n, які: a) парні; b) непарні; c) мають принаймні 1 нерухому точку; d) мають не більше k інверсій (число $k > 0$ — фіксоване)?

А2.3 Доведіть, що a) множина $G = \{x \in \mathbb{R} : x > 1\}$ з дією $a * b = ab - a - b + 2$, b) множина $G = [0, 1)$ з дією $*$, де $a * b$ дорівнює дробовій частині числа $a + b$, c) множина $G = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ з дією $(x_1, y_1) * (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$ утворює групу.

А2.4 Побудуйте таблицю Келі групи K_4.

А2.5 Доведіть, що множина функцій $\{x, 1-x, \frac{1}{x}, \frac{1}{1-x} \frac{x-1}{x}, \frac{x}{x-1}\}$ утворює групу відносно суперпозиції функцій і побудуйте для цієї групи таблицю Келі.

А2.6 Знайдіть порядки всіх елементів даної групи: a) група поворотів правильного 12–кутника; b) $\mathbb{Z}_{16}$; c) $\mathbb{Z}_{13}^*$.

А2.7 Знайдіть кількість елементів кожного можливого порядку у групі a) D_4; b) Q_8; c) S_4.

А2.8 Який порядок можуть мати елементи групи S_6?

А2.9 Скільки елементів порядку 6 містить група A_7?

Д2.1 Чи утворює напівгрупу, моноїд або групу відносно композиції перетворень така множина перетворень площини: a) всі паралельні переноси; b) всі повороти навколо даної точки; c) всі повороти навколо довільних точок; d) всі центральні симетрії; e) усі паралельні переноси й осьові симетрії; f) усі паралельні переноси й повороти навколо довільних точок?

Д2.2 Чи утворює групу відносно множення підстановок множина тих підстановок з S_n, які a) рухають не більше k елементів (число $k > 0$ — фіксоване), b) є транспозиціями?

Д2.3 Доведіть, що: a) множина $\mathbb{R} \setminus \{-1\}$ з дією $x * y = x + y + xy$, b) множина $\mathbb{Z}$ з дією $m * n = m + n + 2003$, c) множина $\mathbb{Z}$ з дією $m \circ n = m + (-1)^m n$ утворює групу.

Д2.4 Побудуйте таблицю Келі групи D_4.

Д2.5 Знайдіть порядок елемента групи:

$$a)\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})\ ; \quad b)\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{C})\ ; \quad c)\frac{1}{2} - \frac{\sqrt{3}}{2}i \in \mathbb{C}^*\ ;$$

$$d) - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \in \mathbb{C}^*\ ; \quad e)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 1 & 8 & 4 & 3 & 6 \end{pmatrix} \in S_8\ .$$

Д2.6 Нехай елемент a має порядок n, b — порядок m і $ab = ba$. a) Доведіть, що коли числа m і n — взаємно прості, то порядок елемента ab дорівнює mn, і що порядок елемента ab завжди є дільником числа НСК(m, n).
b) Наведіть приклад, коли порядок елемента ab не дорівнює НСК(m, n).
c) Доведіть, що існують такі показники k і l, що порядок елемента $a^k b^l$ дорівнює НСК(m, n).

Д2.7 Знайдіть кількість елементів кожного можливого порядку у групі a) D_6; b) A_5.

Д2.8 Доведіть, що довільна скінченна напівгрупа M містить ідемпотент.

Д2.9 Доведіть, що порядок групи поворотів правильного многогранника дорівнює подвоєній кількості його ребер.

Практичне заняття 3. Підгрупи

А3.1 Доведіть, що підмножина $G \subseteq \mathbb{Z}$ буде підгрупою групи $\mathbb{Z}$ тоді й лише тоді, коли G замкнена відносно віднімання.

А3.2 У кожній з наступних множин вкажіть найменше додатне число і з'ясуйте, чи утворює ця множина підгрупу групи $\mathbb{Z}$: a) всі цілі числа, певний степінь яких ділиться на 32; b) всі цілі числа, взаємно прості з числом 5; c) всі цілі числа, на які ділиться число 24; d) всі цілі числа, які діляться на 10 і квадрат яких ділиться на 40; e) всі такі цілі числа m, що $10m$ ділиться на 8.

А3.3 Чи буде підгрупою в групі $\mathbb{Q}^*$ підмножина всіх тих додатних раціональних чисел, у нескоротному записі яких знаменник є степенем числа 3?

А3.4 Знайдіть усі підгрупи групи: a) S_3; b) Q_8.

А3.5 Доведіть, що група $\mathbb{Z}$ не має власних неодиничних скінченних підгруп.

А3.6 Знайдіть у групі S_4 підгрупу G_f тих підстановок, які не змінюють многочлен f, якщо: a) $f = x_1^2 + x_2x_3x_4$; b) $f = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$.

А3.7 Знайдіть кількість тих підстановок з групи S_9, які комутують із підстановкою π: a) $\pi = (123456789)$; b) $\pi = (123)(456789)$.

Д3.1 Чи буде підгрупою групи $S_{\mathbb{N}}$ усіх взаємно однозначних перетворень множини $\mathbb{N}$ множина всіх тих перетворень σ, що $\sigma(k) \geq k$ для всіх $k \in \mathbb{N}$?

Д3.2 Знайдіть усі підгрупи групи D_4.

Д3.3 Доведіть, що в довільній групі: a) перетин довільного набору підгруп є підгрупою; b) якщо підгрупа G міститься в об'єднанні двох підгруп A та B, то або $C \subseteq A$, або $C \subseteq B$.

Д3.4 Знайдіть усі елементи групи $SL_2(R)$, що комутують з даним елементом $g = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \in SL_2(R)$.

Д3.5 Знайдіть у групі S_4 підгрупу G_f тих підстановок, які не змінюють многочлен f, якщо: a) $f = x_1x_2 + x_3x_4$; b) $f = x_1x_2x_3x_4$.

Д3.6 Сформулюйте необхідну й достатню умову для того, щоб об'єднання $A \cup B$ підгруп A, B групи G також було підгрупою групи G.

Практичне заняття 4. Системи твірних. Циклічні групи

А4.1 Доведіть, що множина $\{(123),(234),(345),\ldots,(n-2,n-1,n)\}$ є системою твірних групи $A_n, n \geq 3$.

А4.2 Доведіть, що множина всіх осьових симетрій площини є системою твірних групи всіх рухів площини.

А4.3 Доведіть що група $\mathbb{Q}$ не має скінченних систем твірних.

А4.4 Вкажіть серед даних груп циклічні: a) $\mathbb{Z}_{10}^*$; b) $\mathbb{Z}_{11}^*$; c) $\mathbb{Z}_{12}^*$; d) $\mathbb{Z}_{14}^*$; e) $\mathbb{Z}_{15}^*$.

А4.5 Скількома способами можна вибрати твірний елемент в циклічній групі порядку: a) 6120; b) 8700; c) 2820?

А4.6 Скільки різних підгруп має циклічна група порядку: a) 6120; b) 8700; c) 2820?

А4.7 Опишіть усі 2–елементні незвідні системи твірних групи $\mathbb{Z}$.

А4.8 Скількома способами можна вибрати незвідну 2–елементну систему твірних у циклічній групі порядку: a) 15; b) 18; c) 25?

Д4.1 Доведіть, що кожна з наступних множин є системою твірних групи A_n: a) множина всіх циклів довжини 5 $(n \geq 5)$; b) $\{(12345), (23456), \ldots, (n-4,n-3,n-2,n-1,n)\}$ $(n > 5)$.

Д4.2 Скільки різних циклічних підгруп містить група Q_8?

Д4.3 Доведіть, що в групі $\mathbb{Q}$ кожна скінченно–породжена підгрупа є циклічною.

Д4.4 Скільки різних 2-елементних систем твірних має група D_4?

Д4.5 Скількома способами можна вибрати твірний елемент у групі $\mathbb{C}_n$ і скільки різних підгруп містить група $\mathbb{C}_n$, якщо: a) $n = 8610$; b) $n = 4662$.

Д4.6 Скількома способами можна вибрати незвідну 2–елементну систему твірних у циклічній групі порядку a) 20, b) 27?

Д4.7 Зобразіть групу $\mathbb{Q}$ у вигляді об'єднання зростаючого ланцюга циклічних підгруп.

Практичне заняття 5. Класи суміжності і нормальні підгрупи

А5.1 Опишіть класи суміжності групи G за підгрупою H, якщо: a) $G = \mathbb{R}$, $H = \mathbb{Z}$; b) $G = \mathbb{C}$, $H = \mathbb{R}$; c) $G = \mathbb{C}^*$, $H = \mathbb{R}^*$; d) $G = GL_n(\mathbb{R})$, $H = SL_n(\mathbb{R})$.

А5.2 Опишіть ліві і праві класи суміжності: a) циклічної групи $G = \langle a \rangle$ порядку 24 за підгрупою $H = \langle a^4 \rangle$; b) групи кватерніонів Q_8 за підгрупою $H = \{1, -1\}$.

А5.3 Опишіть ліві і праві класи суміжності групи S_4 a) за підгрупою H, породженою циклом (1234); b) за підгрупою $H = \{\pi \in S_4 : \pi(1) = 1\}$.

А5.4 Доведіть, що в групі S_4 для кожного дільника k порядку групи існує підгрупа порядку k.

А5.5 З'ясуйте, скільки підгруп індексу 2 має група: a) K_4; b) D_4.

А5.6 Чи буде нормальною підгрупою групи $GL_n(\mathbb{R})$ підгрупа a) всіх невироджених матриць з раціональними коефіцієнтами; b) всіх скалярних матриць; c) всіх діагональних матриць; d) всіх верхніх трикутних матриць; e) всіх матриць з додатними визначниками; f) всіх ортогональних матриць?

А5.7 З'ясуйте, чи буде нормальною в групі всіх рухів площини a) підгрупа всіх паралельних переносів; b) підгрупа всіх поворотів навколо фіксованої точки.

А5.8 Опишіть усі нормальні підгрупи групи: a) D_4; b) S_4.

А5.9 Знайдіть в групі D_4 такі три підгрупи A, B, C, що $A \lhd B, B \lhd C$, але $A \ntriangleleft C$.

Д5.1 Опишіть ліві і праві класи суміжності групи D_4 за підгрупою H, породженою: a) поворотом на 180° навколо центра квадрата; b) осьовою симетрією, що проходить через протилежні вершини квадрата; c) осьовою симетрією, що проходить через середини двох протилежних сторін квадрата.

Д5.2 Доведіть, що в групі D_{12} для кожного дільника k порядку групи існує підгрупа порядку k.

Д5.3 З'ясуйте, скільки підгруп індексу 2 має група: a) D_5; b) D_6?

Д5.4 Чи буде нормальною підгрупою групи $GL_n(\mathbb{C})$ підгрупа: a) $GL_n(\mathbb{R})$; b) всіх матриць з дійсними визначниками; c) всіх матриць, визначники яких є коренями 13–го степеня з 1; d) всіх унітарних матриць?

Д5.5 Опишіть усі нормальні підгрупи групи D_5.

Д5.6 Доведіть, що в групі Q_8 кожна підгрупа є нормальною.

Практичне заняття 6. Факторгрупи та гомоморфізми

А6.1 Доведіть, що H — нормальна підгрупа групи G, опишіть класи суміжності групи G за підгрупою H та побудуйте таблицю Келі факторгрупи G/H, якщо: a) $G = 3\mathbb{Z},\ H = 12\mathbb{Z}$; b) $G = D_4,\ H = \{0°, 180°\}$.

А6.2 Опишіть факторгрупу групи G за підгрупою H, якщо: a)$G = \mathbb{Q},\ H = \mathbb{Z}$; b) $G = \mathbb{C}^*,\ H = (\mathbb{R}^+, \cdot)$; c) $G = GL_n(\mathbb{R})\ H = SL_n(\mathbb{R})$.

А6.3 Чи буде гомоморфізмом групи $\mathbb{Z}$ в себе відображення: a) $n \mapsto 3n$;
b) $n \mapsto 5n + 1$; c) $n \mapsto n^2$; d) $n \mapsto 1$?

А6.4 Перевірте, що задане відображення буде гомоморфізмом, знайдіть його ядро і образ: a) $\varphi : \mathbb{R} \to \mathbb{R}^*,\ x \mapsto e^x$;
b) $\varphi : \mathbb{R} \to \mathbb{C}^*,\ x \mapsto \cos x + i \sin x$.

А6.5 Опишіть усі гомоморфізми $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_{12}$ і для кожного з них вкажіть ядро та образ.

А6.6 За допомогою основної теореми про гомоморфізм доведіть, що:
a) $T/\mathbb{C}_n \simeq T,\ T = \{z \in \mathbb{C} : |z| = 1\}$; b) $\mathbb{C}^*/\mathbb{C}_n \simeq \mathbb{C}^*$; c) $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$;
d) $\mathbb{Z}[1/p]/\mathbb{Z} \simeq \mathbb{C}_{p^\infty}$, де $\mathbb{Z}[1/p]$ — підгрупа тих раціональних чисел, знаменник яких не ділиться на жодне просте число, відмінне від p.

Д6.1 Доведіть, що H — нормальна підгрупа групи G, опишіть класи суміжності групи G за підгрупою H та побудуйте таблицю Келі факторгрупи G/H, якщо: a) $G = Q_8,\ H = \{1, -1\}$; b) $G = \mathbb{C}_{16},\ H = \mathbb{C}_4$.

Д6.2 Опишіть факторгрупу групи $\mathbb{C}^*$ за підгрупою $T = \{z \in \mathbb{C}^* : |z| = 1\}$.

Д6.3 Чи буде гомоморфізмом групи $\mathbb{C}^*$ в себе відображення a) $z \mapsto z/|z|$, b) $z \mapsto \overline{z}/z$,
c) $z \mapsto |z|$?

Д6.4 Доведіть, що перетворення φ групи $\mathbb{C}^*$ є ендоморфізмом, і знайдіть його ядро і образ: a) $\varphi(z) = z^n,\ n \in \mathbb{N}$; b) $\varphi(z) = \cos(\arg z) + i \sin(\arg z)$; c) $\varphi(z) = z/|z|$;
d) $\varphi(z) = z^{-1}\overline{z}$; e) $\varphi(z) = |z|$.

Д6.5 Опишіть усі гомоморфізми $\varphi : \mathbb{Z}_{18} \to \mathbb{Z}_{12}$ і для кожного з них вкажіть ядро та образ.

Д6.6 Знайдіть усі гомоморфізми групи $\mathbb{Z}$ в себе. Які з них будуть ізоморфізмами?

Д6.7 За допомогою основної теореми про гомоморфізм доведіть, що:
a) $\mathbb{R}/\mathbb{Z} \simeq T$; b) $\mathbb{C}^*/\mathbb{R}^* \simeq T$; c) $\mathbb{C}^*/T \simeq \mathbb{R}^+$.

Практичне заняття 7. Дія групи на множині

A7.1 Для групи *a)* S_n, *b)* A_n, що природно діє на множині всіх підмножин множини $\{1, 2, \ldots, n\}$, опишіть усі орбіти та підрахуйте їх кількість і потужності.

A7.2 Знайдіть усі класи спряжених елементів у групі Q_8.

A7.3 Знайдіть кількість класів спряжених елементів у групі S_6.

A7.4 Знайдіть кількість елементів групи S_6, які спряжені з елементом: a) (123456); b) $(123)(456)$.

A7.5 Скількома геометрично різними способами можна розфарбувати ребра a) правильного тетраедра, b) куба, c) правильної n–кутної піраміди, якщо є фарби k кольорів?

A7.6 Обчисліть, скільки істотно різних разків намиста можна скласти, якщо кожний разок має містити 5 жовтих і 5 зелених намистинок.

Д7.1 Знайдіть стабілізатор діагоналі куба при природній дії групи поворотів куба на діагоналях.

Д7.2 Знайдіть усі класи спряжених елементів у групі: a) D_4; b) A_4.

Д7.3 Знайдіть кількість елементів групи S_6, які спряжені з елементом $(12)(34)(56)$.

Д7.4 Скількома геометрично різними способами можна розфарбувати грані a) правильного тетраедра, b) куба, c) правильної n–кутної піраміди, якщо є фарби k кольорів?

Д7.5 Обчисліть, скільки істотно різних разків намиста можна скласти, якщо кожний разок має містити 4 жовтих і 8 зелених намистинок.

Практичне заняття 8. Кільця.

A8.1 Доведіть, що для будь-яких елементів кільця R мають місце рівності:

а) $a \cdot 0 = 0 \cdot a = 0$;

б) $(-a) \cdot (-b) = a \cdot b$;

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

A8.2 Чи утворюють кільця відносно звичайних операцій додавання та множення такі числові множини:

а) множина всіх цілих невід'ємних чисел;

б) $\{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}$;

в) $\{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$;

г) множина всіх тих раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p.

A8.3 Нехай M— непорожня множина, $\mathcal{B}(M)$ — множина всіх її підмножин. Доведіть, що $(\mathcal{B}(M), \triangle, \cap)$ є комутативним кільцем (тут $\triangle$ і $\cap$ — операції симетричної різниці та перетину множин, що розглядаються як додавання і множення відповідно).

A8.4 Перевірте, чи є множина A підкільцем кільця $\mathrm{C}[a, b]$:

а) $A = \{f \in \mathrm{C}[a, b] : f(b) = 0\}$;

б) $A = \{f \in \mathrm{C}[a, b] : f(a) = f(b)\}$.

A8.5 Перевірте, чи є множина A підкільцем кільця $M_2(\mathbb{R})$:

$$A = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in M_2(\mathbb{R}) : a, b, c \in \mathbb{R} \right\}.$$

A8.6 Доведіть, що підкільце $\mathbb{Z}\left[\frac{1}{p}\right]$ кільця $\mathbb{Q}$ рівне кільцю із задачі **A8.2г**). (Для підкільця A кільця R і довільної підмножини $B \subset R$ символом $A[B]$ тут і далі позначається найменше підкільце кільця R, котре містить A і B.)

A8.7 Знайдіть найменше натуральне число n таке, що кільце $\mathbb{Z}\left[\frac{1}{n}\right]$ рівне кільцю:

$$\mathbb{Z}\left[\frac{1}{9}\right]; \quad \mathbb{Z}\left[\frac{7}{12}\right].$$

А8.8 Доведіть, що кільце, в якому для кожного елемента x виконана рівність $x^2 = x$, є комутативним.

А8.9 Наведіть приклад кільця і лівого дільника нуля в ньому, який не є правим дільником нуля.

А8.10 Доведіть, що у кільці з одиницею жоден лівий дільник нуля не є правим дільником одиниці.

А8.11 Доведіть, що у кільці з одиницею множина всіх оборотних елементів утворює групу відносно множення.

А8.12 Опишіть дільники нуля, оборотні та нільпотентні елементи кільця

а) $\mathbb{Z}_n$, $n \geq 2$;

б) $\mathbb{Z}_{98}$;

в) $\mathbb{Z}\left[i\sqrt{7}\right]$;

г) $\mathbb{Z}\left[\frac{1}{7}\right]$.

А8.13 Опишіть дільники нуля, оборотні та нільпотентні елементи кільця $(\mathcal{B}(M), \triangle, \cap)$ із задачі **А8.3**.

Д8.1 Доведіть, що для будь-яких елементів кільця R мають місце рівності:

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

б) $a \cdot (b_1 + \cdots + b_n) = a \cdot b_1 + \ldots a \cdot b_n$;

в) $(b_1 + \cdots + b_n) \cdot a = b_1 \cdot a + \cdots + b_n \cdot a$.

Д8.2 Чи утворюють кільця відносно звичайних операцій додавання та множення такі числові множини:

а) $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$;

б) $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Z}\}$;

в) $\{a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{n-1}\varepsilon^{n-1} \in \mathbb{C} : a_i \in \mathbb{Z}$ для $i \in \{0, 1, \ldots, n-1\}$, ε — первісний корінь степеня n з $1\}$.

г) множина A_D всіх комплексних чисел вигляду $\frac{x+y\sqrt{D}}{2}$, (D — фіксоване ціле число, що не ділиться на квадрат простого числа, x, y — цілі числа однакової парності).

Д8.3 Чи утворює кільце множина всіх многочленів з дійсними коефіцієнтами відносно звичайного додавання та множення "$\circ$", визначеного рівністю $(f \circ g)(t) = f(g(t))$?

Д8.4 Перевірте, чи є множина A підкільцем кільця $\mathrm{C}[a, b]$:

а) $A = \{f \in \mathrm{C}[a, b] : f(\frac{a+b}{2}) \in \mathbb{Q}\}$;

б) $A = \{f \in \mathrm{C}[a,b] : \int_a^b f(x)dx = 0\}$.

Д8.5 Перевірте, чи є множина A підкільцем кільця $M_2(\mathbb{R})$:

а) $A = M_2(\mathbb{Q})$;

б) $A = M_2(\mathbb{Z})$;

в) $A = \{T \in M_2(\mathbb{R}) : \det T = 0\}$.

Д8.6 Знайдіть найменше натуральне число n таке, що кільце $\mathbb{Z}\left[\frac{1}{n}\right]$ рівне кільцю:

$$\mathbb{Z}\left[\frac{11}{36}, \frac{8}{57}\right]; \quad \mathbb{Z}\left[\frac{4}{25}, \frac{7}{60}, \frac{11}{18}\right].$$

Д8.7 Наведіть приклад кільця R з одиницею 1 і його підкільця S, яке також є кільцем з одиницею e, причому $e \neq 1$.

Д8.8 Доведіть, що коли елемент a^2 кільця є дільником нуля, то і a є дільником нуля.

Д8.9 Нехай R — кільце з одиницею без дільників нуля. Доведіть, що кожен елемент кільця R, котрий має односторонній обернений, є оборотним.

Д8.10 Опишіть дільники нуля, оборотні та нільпотентні елементи кільця

а) $\mathbb{Z}_{45}$;

б) $\mathbb{Z}_{30}$;

в) $\mathbb{Z}_{p^2}$, p — просте число;

г) $\mathbb{Z}_p \times \mathbb{Z}_p$, p — просте число;

д) $\mathbb{Z}[i]$;

е) $\mathbb{Z}\left[\frac{1}{10}\right]$;

ж) $\mathbb{Z} \times \mathbb{Z}$;

и) $\mathbb{R} \times \mathbb{R}$;

к) $\mathbb{R} \times \mathbb{Z}$.

Практичне заняття 9. Евклідові кільця

A9.1 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}$, обчисліть обернений для заданого елемента a кільця $\mathbb{Z}_{1938}$:

а) $a = 625$;

б) $a = 161$.

A9.2 Користуючись алгоритмом Евкліда, обчисліть НСД многочленів $f, g \in \mathbb{Z}_{11}[x]$, а також знайдіть лінійний вираз НСД$(f, g) = hf + kg$, $h, k \in \mathbb{Z}_{11}[x]$, якщо $f = x^4 + 4x^3 + 5x + 3$, $g = x^3 + 2x^2 + 7x + 8$.

A9.3 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}_7[x]$, обчисліть у факторкільці $\mathbb{Z}_7[x]/I$, $I = (x^4 + 2x + 1)$, обернені до елементів:

а) $(x^2 + x + 2) + I$;

б) $(2x^3 + x^2 + 1) + I$.

A9.4 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}[i]$, обчисліть НСД таких пар елементів цього кільця:

а) $9 + 2i, 4 - 7i$;

б) $2 + 8i, -2 + 10i$.

A9.5 Доведіть, що кільце $\mathbb{Z}[i\sqrt{2}]$ є евклідовим.

A9.6 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}[i\sqrt{2}]$, обчисліть НСД таких пар елементів цього кільця:

а) $-15 - 3i\sqrt{2}, -9$;

б) $12 - 3i\sqrt{2}, 19 + 3i\sqrt{2}$.

A9.7 Доведіть, що кільце $\mathbb{Z}[\sqrt{3}]$ є евклідовим.

A9.8 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}[\sqrt{3}]$, обчисліть НСД таких пар елементів цього кільця:

а) $-7 - 5\sqrt{3}, -14 + 3\sqrt{3}$;

б) $22 + 4\sqrt{3}, -1 + 11\sqrt{3}$.

A9.9 При яких n кільце $\mathbb{Z}_n$ є евклідовим?

A9.10 Доведіть, що кільце $\mathbb{Z}[i\sqrt{5}]$ не є евклідовим.

Д9.1 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}$, обчисліть обернений для заданого елемента a кільця $\mathbb{Z}_{1938}$:

а) $a = 533$;

б) $a = 1831$.

Д9.2 Користуючись алгоритмом Евкліда, обчисліть НСД многочленів $f, g \in \mathbb{Z}_{11}[x]$, а також знайдіть лінійний вираз НСД$(f, g) = hf + kg$, $h, k \in \mathbb{Z}_{11}[x]$, якщо $f = x^4 + 2x^2 + 3x + 2$, $g = x^4 + 2x^3 + 7x + 4$.

Д9.3 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}_7[x]$, обчисліть у факторкільці $\mathbb{Z}_7[x]/I$, $I = (x^4 + 2x + 1)$, обернені до елементів:

а) $(2x^2 + 2x + 1) + I$;

б) $(3x^2 + 4x + 1) + I$.

Д9.4 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}[i]$, обчисліть НСД таких пар елементів цього кільця:

а) $7 - 7i, 11 + 5i$;

б) $-6 + 3i, 8 + 4i$;

в) $7 - 14i, -7 - 21i$.

Д9.5 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}[i\sqrt{2}]$, обчисліть НСД таких пар елементів цього кільця:

а) $-5 + 8i\sqrt{2}, -6 + 2i\sqrt{2}$;

б) $25 + 25i\sqrt{2}, 17 - 14i\sqrt{2}$.

Д9.6 Користуючись алгоритмом Евкліда для кільця $\mathbb{Z}[\sqrt{3}]$, обчисліть НСД таких пар елементів цього кільця:

а) $6 + \sqrt{3}, -4 + 2\sqrt{3}$;

б) $14 + 2i\sqrt{3}, 8 - 6\sqrt{3}$.

Д9.7 Доведіть, що в евклідовому кільці норми асоційованих елементів рівні. Чи правильне обернене твердження?

Д9.8 Доведіть, що кільце $\mathbb{Z}[x]$ не є евклідовим.

Д9.9 Доведіть, що кільце $\mathbb{R}[x, y]$ не є евклідовим.

Д9.10 Доведіть, що у підкільці кільця многочленів $\mathbb{R}[x]$, яке складається з усіх многочленів з нульовим коефіцієнтом при x, ідеал, породжений x^2 та x^3, не є головним.

Практичне заняття 10. Симетричні многочлени

A10.1 Перевірте, що заданий многочлен є симетричним і виразіть його через елементарні симетричні многочлени

а) $x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$;

б) $(x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3)$.

A10.2 Обчисліть значення многочлена

$$G(x_1, x_2, x_3) = x_1^3(x_2 + x_3) + x_2^3(x_1 + x_3) + x_3^3(x_1 + x_2)$$

від коренів многочлена

$$f(t) = t^3 - t^2 - 4t + 1.$$

A10.3 Знайдіть унітарний многочлен четвертого степеня з дійсними коефіцієнтами, який має

а) прості корені $1, -2, 3, -4$;

б) корінь $1 + i$ кратності 2.

A10.4 Обчисліть суму квадратів, добуток і суму чисел, обернених до комплексних коренів многочлена $f(x) = 3x^3 + 2x^2 - 1$.

A10.5 Знайдіть λ, для якого один з коренів многочлена $f(x) = x^3 - 7x + \lambda$ дорівнює подвоєному іншому.

A10.6 Обчисліть результант многочленів $f(x)$ та $g(x)$

а) $f(x) = x^3 - 3x^2 + 2x + 1$, $g(x) = 2x^2 - x - 1$;

б) $f(x) = 2x^3 - 3x^2 - x + 1$, $g(x) = x^4 - 2x^2 - 3x + 4$.

A10.7 Знайдіть усі значення λ, при яких многочлени

$$f(x) = x^3 - \lambda x + 2 \quad \text{та} \quad g(x) = x^2 + \lambda x + 2$$

мають спільний корінь.

A10.8 Обчисліть дискримінант многочлена $f(x)$

а) $f(x) = ax^2 + bx + c$;

б) $f(x) = x^3 + a_1x^2 + a_2x + a_3$.

A10.9 Знайдіть усі значення λ, при яких многочлен $f(x) = x^3 - 3x + \lambda$ має кратний корінь.

Д10.1 Перевірте, що заданий многочлен є симетричним і виразіть його через елементарні симетричні многочлени

а) $x_1^4 + x_2^4 + x_3^4 - 2x_1^2x_2^2 - 2x_1^2x_3^2 - 2x_2^2x_3^2$;

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

Д10.2 Обчисліть значення многочлена

$$G(x_1, x_2, x_3, x_4) = x_1^3(x_2x_3 + x_2x_4 + x_3x_4) + x_2^3(x_1x_3 + x_1x_4 + x_3x_4) + x_3^3(x_1x_2 + x_1x_4 + x_2x_4) + x_4^3(x_1x_2 + x_1x_3 + x_2x_3)$$

від коренів многочлена

$$f(t) = t^4 + t^3 - 2t^2 - 3t + 1.$$

Д10.3 Знайдіть унітарний многочлен четвертого степеня з дійсними коефіцієнтами, який має

а) прості корені $2, i, -i, -3$;

б) корінь $2 - i$ кратності 2.

Д10.4 Обчисліть суму квадратів, добуток і суму чисел, обернених до комплексних коренів многочлена $f(x) = x^4 - x^2 - x - 1$.

Д10.5 Знайдіть значення всіх елементарних симетричних многочленів від коренів з одиниці n-того степеня.

Д10.6 Знайдіть λ, для якого сума двох коренів многочлена $f(x) = 2x^3 - x^2 - 7x + \lambda$ дорівнює 1.

Д10.7 Обчисліть результант многочленів $f(x)$ та $g(x)$

а) $f(x) = 2x^3 - 3x^2 + 2x + 1$, $g(x) = x^2 + x + 3$;

б) $f(x) = 3x^3 + 2x^2 + x + 1$, $g(x) = 2x^3 + x^2 - x - 1$.

Д10.8 Знайдіть усі значення λ, при яких многочлени

$$f(x) = x^3 + \lambda x^2 - 9 \quad \text{та} \quad g(x) = x^2 + \lambda x - 3$$

мають спільний корінь.

Д10.9 Обчисліть дискримінант многочлена $f(x)$

а) $f(x) = x^3 + px + q$;

б) $f(x) = x^4 - x^3 - 3x^2 + x + 1$.

Д10.10 Знайдіть усі значення λ, при яких многочлен $f(x) = x^4 - 4x + \lambda$ має кратний корінь.

Практичне заняття 11. Поля

A11.1 Чи утворюють поле відносно звичайних операцій додавання та множення такі числові множини:

а) $\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$;

б) $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Q}\}$;

в) $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Q}\}$?

A11.2 Опишіть поле часток області цілісності R, якщо:

а) $R = \mathbb{Z}[\sqrt{3}]$;

б) $R = \mathbb{Z}[i]$;

в) $R = \mathbb{Z}\left[\frac{1}{2}\right]$.

A11.3 Нехай R — комутативне кільце з одиницею. Доведіть, що ідеал I цього кільця є максимальним (тобто не міститься в жодному іншому ідеалі, відмінному від R) тоді й лише тоді, коли факторкільце R/I є полем.

A11.4 Побудуйте таблиці додавання та множення для поля з 4 елементів.

A11.5 Чи буде полем прямий добуток полів?

A11.6 Доведіть, що у полі потужності n виконується тотожність $x^n = x$.

A11.7 Знайдіть характеристику поля, в якому виконується рівність $(1+1+1+1+1)^2 = (1+1)^5$.

A11.8 Доведіть, що кожне скінченне поле має додатну характеристику.

A11.9 Доведіть, що існують нескінчені поля додатної характеристики.

A11.10 Нехай F — поле додатної характеристики p. Доведіть, що для довільних $a, b \in F$ і $n \in \mathbb{N}$ виконуються рівності:

а) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$;

б) $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.

Д11.1 Чи утворюють поле відносно звичайних операцій додавання та множення такі числові множини:

а) $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$;

б) $\{z \in \mathbb{C} : |z| \leq 1\}$?

Д11.2 Нехай n — ціле число. Доведіть, що множина $M_n = \left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} : x, y \in \mathbb{Q} \right\}$ утворює поле відносно звичайних операцій додавання та множення матриць тоді й лише тоді, коли число n не є квадратом цілого числа.

Д11.3 Опишіть поле часток області цілісності R, якщо:

а) $R = \mathbb{Z}[\sqrt{3}, \sqrt{5}]$;

б) $R = \mathbb{Z}[i\sqrt{7}]$;

в) $R = \mathbb{Z}[x]$;

г) $R = \mathbb{Z}[x^2, x^3]$.

Д11.4 Побудуйте таблиці додавання та множення для полів з 8 та 9 елементів.

Д11.5 Доведіть, що в кожному полі є рівно два ідеали.

Д11.6 Якою може бути характеристика поля, в якому виконується рівність $(1+1+1+1+1)^2 = (1+1)^2$?

Д11.7 Доведіть, що не існує скінченного поля, число елементів якого має більше одного простого дільника.

Д11.8 Доведіть, що всі підполя поля F мають характеристику, рівну $charF$.

Д11.9 Нехай F — поле додатної характеристики p і для деяких $a, b \in F$ виконується рівність $a^p = b^p$. Доведіть, що $a = b$.

Практичне заняття 12. Розширення полів

А12.1 Визначте, чи буде елемент α алгебраїчним над полем F. Якщо так, знайдіть його мінімальний многочлен:

а) $\alpha = 2 + i$, $F = \mathbb{R}$;

б) $\alpha = 1 + \sqrt{3}$, $F = \mathbb{Q}$;

в) $\alpha = \sqrt[4]{5} + \sqrt{5}$, $F = \mathbb{Q}$.

А12.2 Нехай q — раціональне число. Доведіть, що числа $\sin(q\pi)$ і $\cos(q\pi)$ алгебраїчні.

А12.3 Доведіть, що комплексне число z є алгебраїчним тоді й лише тоді, коли число $\overline{z}$ є алгебраїчним.

А12.4 Доведіть, що дійсні числа a і b є алгебраїчними тоді й лише тоді, коли число $z = a + bi$ алгебраїчне.

А12.5 Знайдіть базиси таких розширень поля $\mathbb{Q}$:

а) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$;

б) $\mathbb{Q}(\epsilon)$, $\epsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, p — просте число;

в) $\mathbb{Q}(\sqrt{3}, i)$.

А12.6 Доведіть, що розширення $\mathbb{R} \supset \mathbb{Q}$ є нескінченним.

А12.7 Нехай u — корінь многочлена $x^3+3x^2-9x+6 \in \mathbb{Q}[x]$. Подайте у вигляді лінійної комбінації з раціональними коефіцієнтами елементів $1, u, u^2$ такі елементи поля $\mathbb{Q}(u)$:

а) $u^4 + u$;

б) $\dfrac{u^2}{u^2 + 2u - 11}$.

Д12.1 Визначте, чи буде елемент α алгебраїчним над полем F. Якщо так, знайдіть його мінімальний многочлен:

а) $\alpha = 1 + 2i$, $F = \mathbb{C}$;

б) $\alpha = 1 + \sqrt{2} + \sqrt{3}$, $F = \mathbb{Q}$;

в) $\alpha = \sqrt{2 - \sqrt{3}}$, $F = \mathbb{Q}$;

г) $\alpha = \sqrt[6]{3} + \sqrt{3}$, $F = \mathbb{Q}$

д) $\alpha = 1 + \sqrt{2} + \cdots + \sqrt{2^{n-1}}$, $F = \mathbb{Q}$.

Д12.2 Знайдіть базиси таких розширень поля $\mathbb{Q}$:

а) $\mathbb{Q}(\epsilon)$, $\epsilon = \frac{-1+i\sqrt{3}}{2}$;

б) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$;

в) $\mathbb{Q}(\epsilon, \sqrt[3]{3})$, $\epsilon = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$.

Д12.3 Нехай u — корінь многочлена $x^3+3x^2-9x+6 \in \mathbb{Q}[x]$. Подайте у вигляді лінійної комбінації з раціональними коефіцієнтами елементів $1, u, u^2$ такі елементи поля $\mathbb{Q}(u)$:

а) u^5;

б) $\dfrac{1}{u}$;

в) $\dfrac{u^4+3u+1}{u^2+2u-11}$.

Д12.4 Наведіть приклад алгебраїчних чисел a і b степенів відповідно 2 і 3 таких, що добуток ab є алгебраїчним степеня:

a) 3; b) 6.

Д12.5 Нехай a — алгебраїчний над F елемент непарного степеня. Доведіть, що $F(a) = F(a^2)$.

Д12.6 Нехай a — алгебраїчний над F елемент і $F(a) = F(a^2)$. Чи випливає звідси, що a має непарний степінь над F?

Д12.7 Доведіть, що будь-яке скінченне розширення поля $\mathbb{R}$ ізоморфне або $\mathbb{R}$, або $\mathbb{C}$.

Практичне заняття 13. Скінченні поля

А13.1 Знайдіть усі незвідні многочлени степенів 2, 3 і 4 над полями $\mathbb{Z}_2$ і $\mathbb{Z}_3$.

А13.2 Знайдіть всі твірні елементи мультиплікативної групи поля з 16 елементів.

А13.3 Нехай F — скінченне поле, $char F = p$. Доведіть, що відображення $x \mapsto x^p$ є автоморфізмом цього поля.

А13.4 Доведіть, що факторкільце $\mathbb{Z}_3[x]/(x^3 + 2x + 2)$ є полем та знайдіть усі автоморфізми цього поля.

А13.5 З'ясуйте, чи буде полем факторкільце $\mathbb{Z}_5[x]/(f(x))$ у кожному з випадків:

а) $f(x) = x^2 + 2$;

б) $f(x) = x^3 + 2x + 1$.

А13.6 Над кожним з полів $\mathbb{Z}_3$ та $\mathbb{Z}_{13}$ розв'яжіть систему рівнянь

$$\begin{cases} x + 2z = 1 \\ y + 2z = 2 \\ 2x + z = 1 \end{cases}$$

А13.7 Доведіть, що факторкільце $\mathbb{Z}_2[x]/(x^3+x+1)$ є полем. Для кожного $f(x) \in \mathbb{Z}_2[x]$ позначимо через $\overline{f(x)}$ клас еквівалентності за ідеалом $(x^3 + x + 1)$, що містить $f(x)$. Над цим полем розв'яжіть рівняння $t^2 + \overline{x^2 + x + 1} = 0$.

Д13.1 Знайдіть усі незвідні многочлени степенів 2, 3 і 4 над полем $\mathbb{Z}_5$.

Д13.2 а) Визначте, для яких унітарних многочленів $f(x) \in \mathbb{Z}_3[x]$ другого степеня факторкільце $\mathbb{Z}_3[x]/(f(x))$ буде полем.

б) Знайдіть твірні елементи мультиплікативних груп для кожного з цих полів.

в) Побудуйте ізоморфізми між усіма парами так отриманих полів.

Д13.3 З'ясуйте, чи буде полем факторкільце $\mathbb{Z}_5[x]/(f(x))$ у кожному з випадків:

а) $f(x) = x^2 + 4x + 1$;

б) $f(x) = x^3 + 4x + 2$.

Д13.4 Над кожним з полів $\mathbb{Z}_5$ та $\mathbb{Z}_{11}$ розв'яжіть систему рівнянь

$$\begin{cases} x + 2z = 1 \\ y + 2z = 2 \\ 2x + z = 1 \end{cases}$$

Д13.5 Доведіть, що факторкільце $\mathbb{Z}_2[x]/(x^3+x+1)$ є полем. Для кожного $f(x) \in \mathbb{Z}_2[x]$ позначимо через $\overline{f(x)}$ клас еквівалентності за ідеалом (x^3+x+1), що містить $f(x)$. Над цим полем розв'яжіть рівняння $t^2 + t + \overline{x^2+1} = 0$.

Д13.6 Доведіть, що у полі $\mathbb{Z}_p$ виконуються рівності:

а) $\displaystyle\sum_{k=1}^{p-1} k^{-1} = 0,$ якщо $p > 2$;

б) $\displaystyle\sum_{k=1}^{\frac{p-1}{2}} k^{-2} = 0,$ якщо $p > 3$.

Практичне заняття 14. Еліптичні криві

А14.1 Обчисліть суму точок $P = (13, 1)$ і $Q = (4, 3)$ еліптичної кривої $y^2 = x^3 + 2x + 5$ над полем $\mathbb{F}_{17}$.

А14.2 Для точок еліптичної кривої $y^2 = x^3 + 10x$ над $\mathbb{F}_{11}$ розв'яжіть рівняння

$$(x_1, x_2) + (1, 0) = (4, 4).$$

А14.3 Для еліптичної кривої $y^2 = x^3 - 9x$ над $\mathbb{R}$ знайдіть всі точки 2-го та 4-го порядків.

А14.4 Знайдіть порядок точки $P = (5, 2)$ на кривій $y^2 = x^3 + x$ над полем $\mathbb{F}_7$.

А14.5 Знайдіть всі точки кривої $y^2 + xy = x^3$ над $\mathbb{F}_4$.

Д14.1 Обчисліть суму точок $P = (9, 2)$ і $Q = (3, 7)$ еліптичної кривої $y^2 = x^3 + 3x + 13$ над полем $\mathbb{F}_{17}$.

Д14.2 Для точок еліптичної кривої $y^2 = x^3 + 10x$ над $\mathbb{F}_{11}$ розв'яжіть рівняння

$$(x_1, x_2) + (10, 0) = (4, 4).$$

Д14.3 Для еліптичної кривої $y^2 = x^3 - 4x$ над $\mathbb{R}$ знайдіть всі точки 2-го та 4-го порядків.

Д14.4 Знайдіть порядок точки $P = (0, 16)$ на кривій $y^2 = x^3 + 256$ над $\mathbb{Q}$.

Д14.5 Знайдіть всі точки кривої $y^2 + xy = x^3 + 1$ над $\mathbb{F}_4$.