

# Розділ 8.

## Алгебричні структури

- 8.1.** Доведіть, що множина усіх оборотних елементів моноїда є його підмоноїдом.
- 8.2.** Доведіть, що в групі нейтральний елемент єдиний.
- 8.3.** Довести, що в групі для кожного елемента існує єдиний обернений.
- 8.4.** Нехай  $(G, \cdot)$  — група,  $a, b, c \in G$ . Доведіть закон скорочення: для довільних елементів  $a, b, c$  групи  $(G, \cdot)$  ізожної з рівностей  $ab = ac$  і  $ba = ca$  випливає рівність  $b = c$ .
- 8.5.** Нехай  $(G, \cdot)$  — група,  $a, b \in G$ . Доведіть, що кожне з рівнянь  $ax = b$  і  $ya = b$  має єдиний розв'язок.
- 8.6.** Доведіть, що моноїд  $M$ , у якому для довільних елементів  $a, b \in M$  або рівняння **a)**  $ax = b$ , або **b)**  $ya = b$  має принаймні один розв'язок, є групою.
- 8.7.** Довести, що скінчена множина  $G$ , в якій визначена асоціативна операція множення і кожне з рівнянь  $ax = b$ ,  $ya = b$  для будь-яких  $a, b \in G$  має в  $G$  не більше одного розв'язку, буде групою.
- 8.8.** Нехай  $(G, \cdot)$  — група,  $e$  — її нейтральний елемент. Довести, що якщо  $a^2 = e$  для будь-якого елемента  $a$  групи  $G$ , то ця група абелева.
- 8.9.** Доведіть, що непорожня підмножина  $H \subseteq G$  є підгрупою групи  $G$  тоді і тільки тоді, коли  $a^{-1}b \in H$  для довільних елементів  $a, b \in H$ .
- 8.10.** Чи може в підгрупі групи  $G$  існувати нейтральний елемент, відмінний від нейтрального елемента групи  $G$ .
- 8.11.** Нехай  $H$  — підгрупа групи  $G$ . Довести, що обернений до довільного елемента  $h \in H$  в підгрупі  $H$  співпадає з оберненим до  $h$  в групі  $G$ .
- 8.12.** Довести, що у довільній групі  $G$ :
- а)** перетин довільної кількості підгруп є підгрупою;
  - б)** об'єднання двох підгруп є підгрупою тоді й тільки тоді, коли одна з підгруп міститься в іншій;
  - в)** якщо підгрупа  $H$  міститься в об'єднанні підгруп  $V$  і  $W$ , то або  $H \subseteq V$ , або  $H \subseteq W$ .
- 8.13.** Довести, що будь-яка нескінчена група має нескінчену кількість підгруп.
- 8.14.** Довести, що якщо елемент  $a$  групи  $G$  має нескінчений порядок, то  $a^k = a^m$  тоді і тільки тоді, коли  $k = m$ .
- 8.15.** Довести, що якщо елемент  $a$  групи  $G$  має порядок  $n$ , то
- а)**  $a^{-1} = a^{n-1}$ ;
  - б)**  $a^m = e$  тоді і лише тоді, коли  $m$  ділиться націло на  $n$ ;
  - в)**  $a^m = a^k$  тоді і лише тоді, коли  $(m - k)$  ділиться націло на  $n$ ;
  - г)**  $\text{ord}(a^m) = \frac{n}{\text{HCD}(n, m)}$ .
- 8.16.** Якщо елементи  $a, b$  групи  $G$  переставні ( $ab = ba$ ),  $\text{ord}(a) = n$ ,  $\text{ord}(b) = m$ , причому  $n, m$  — взаємно прості, то  $\text{ord}(ab) = \text{ord}(a) \cdot \text{ord}(b) = nm$ .

- 
- 8.17.** Довести, що множина  $S_n$  — усіх підстановок довжини  $n$  — утворює мультиплікативну групу, причому неаблеву при  $n \geq 3$ .
- 8.18.** Довести, що порядок симетричної групи  $S_n$  дорівнює  $n!$ .
- 8.19.** Довести, що кожна підстановка розкладається в добуток незалежних циклів, причому однозначно.
- 8.20.** Довести, що кожна підстановка розкладається в добуток транспозицій.
- 8.21.** Парна підстановка розкладається в добуток парного числа транспозицій, а непарна — в добуток непарного числа транспозицій.
- 8.22.** Нехай  $G$  — скінчена група,  $a \in G$ . Довести, що  $G = \langle a \rangle$  тоді і тільки тоді, коли порядок  $a$  дорівнює  $|G|$ .
- 8.23.** Нехай  $G = \langle a \rangle$  — скінчена циклічна група порядку  $n$ . Довести твердження:
- порядок будь-якої підгрупи групи  $G$  ділить число  $n$  (порядок цієї групи);
  - підгрупа  $H$  порядку  $m$  містить в ролі твірних елементів всі елементи порядку  $m$  групи  $G$ . Зокрема,  $H = \langle a^{\frac{n}{m}} \rangle$ .
- 8.24.** Чи існує нескінчена група, всі елементи якої мають скінчений порядок?
- 8.25.** Довести, що в абелевій групі множина елементів, порядки яких ділять фіксоване число  $n$ , є підгрупою. Чи правильне це твердження для неабелевої групи?
- 8.26.** Довести, що в довільній групі парного порядку існує елемент порядку 2.
- 8.27.** Довести, що:
- група додатних дійсних чисел щодо множення ізоморфна групі всіх дійсних чисел щодо додавання;
  - група додатних раціональних чисел щодо множення не ізоморфна групі всіх раціональних чисел щодо додавання.
- 8.28.** Нехай  $H \leq G$ . Довести, що якщо  $h \in H$ , то  $hH = H$ .
- 8.29.** Нехай  $H$  — підгрупа групи  $G$  і  $a, b \in G$ . Довести, що
- якщо  $b \in aH$ , то  $aH = bH$ ;
  - $aH = bH$  тоді і лише тоді, коли  $b^{-1}a \in H$ .
- 8.30.** Доведіть таке:
- будь-які дві підгрупи групи  $G$  взаємно простих порядків перетинаються по одиничній підгрупі;
  - якщо порядок групи  $G$  є добутком двох простих чисел, то будь-які дві різні власні підгрупи групи  $G$  перетинаються по одиничній підгрупі.
- 8.31.** Нехай  $H \leq G$ . Довести, що  $H \triangleleft G$  тоді і лише тоді, коли  $g^{-1}hg \in H$  для кожного  $g \in G$  і кожного  $h \in H$ .
- 8.32.** Довести, що в полі не існує дільників нуля.

# Розділ 9.

## Поле комплексних чисел

- 9.1.** Довести, що  $\bar{\bar{z}} = z$  для довільного комплексного числа  $z \in \mathbb{C}$ .
- 9.2.** Довести, що  $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$ ,  $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$  для довільних комплексних чисел  $z_1, z_2$ .
- 9.3.** Довести, що відображення  $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ , де  $\varphi(z) = \bar{z}$  для довільного  $z \in \mathbb{C}$ , є автоморфізмом поля  $\mathbb{C}$ .
- 9.4.** Довести, що:
- комплексне число  $z$  є дійсним тоді і тільки тоді, коли  $\bar{z} = z$ ;
  - комплексне число  $z$  є чисто уявним тоді і тільки тоді, коли  $\bar{z} = -z$ .

- 9.5.** Довести, що:
- добуток двох комплексних чисел є дійсним числом тоді і тільки тоді, коли одне з них відрізняється від спряженого до другого дійсним множником;
  - сума і добуток двох комплексних чисел є дійсним тоді і тільки тоді, коли дані числа або спряжені, або обидва дійсні.

- 9.6.** Довести, що визначник

$$\begin{vmatrix} z_1 & \bar{z}_1 & a \\ z_2 & \bar{z}_2 & b \\ z_3 & \bar{z}_3 & c \end{vmatrix},$$

де  $z_1, z_2, z_3$  — комплексні і  $a, b, c$  — дійсні числа, є чисто уявним числом.

- 9.7.** Нехай  $\sqrt{a+bi} = \pm(\alpha + \beta i)$ . Чому дорівнює  $\sqrt{-a-bi}$ ?

- 9.8.** Довести тотожність

$$|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2(|z_1|^2 + |z_2|^2);$$

який геометричний зміст цієї тотожності?

- 9.9.** Довести, що будь-яке комплексне число  $z$ , відмінне від  $-1$  і модуль якого дорівнює 1, може бути зображене у вигляді  $z = \frac{1+ir}{1-ir}$ , де  $r$  — дійсне число.

- 9.10.** Довести, що  $|z| \geq 0$  для довільного комплексного числа  $z \in \mathbb{C}$ , причому  $|z| = 0$  тоді і лише тоді, коли  $z = 0$ .

- 9.11.** Довести, що  $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$  для довільних  $z_1, z_2 \in \mathbb{C}$ .

- 9.12.** Довести такі властивості модуля комплексних чисел:

- $|z_1 \pm z_2| \leq |z_1| + |z_2|$ ;
- $||z_1| - |z_2|| \leq |z_1 \pm z_2|$ ;
- $|z_1 + z_2| = |z_1| + |z_2|$  тоді і тільки тоді, коли вектори  $z_1$  і  $z_2$  мають однакові напрямки;
- $|z_1 + z_2| = ||z_1| - |z_2||$  тоді і тільки тоді, коли вектори  $z_1$  і  $z_2$  мають протилежні напрямки.

- 9.13.** Нехай  $z_1, z_2$  — комплексні числа і  $u = \sqrt{z_1 z_2}$ . Довести, що

$$|z_1| + |z_2| = \left| \frac{z_1 + z_2}{2} - u \right| + \left| \frac{z_1 + z_2}{2} + u \right|.$$

**9.14.** Довести, що:

- а) при множенні двох комплексних чисел у тригонометричній формі їхні модулі множаться, а аргументи додаються;
- б) при діленні двох комплексних чисел  $z_1$  на  $z_2$  ( $z_2 \neq 0$ ) у тригонометричному вигляді їхні модулі діляться, а аргументи віднімаються.

**9.15.** Довести формулу Muавра

$$(r(\cos \varphi + i \sin \varphi))^n = r^n (\cos(n\varphi) + i \sin(n\varphi))$$

для цілих  $n \neq 0$ .

**9.16.** Довести, що якщо  $z + \frac{1}{z} = 2 \cos \varphi$ , то  $z^m + \frac{1}{z^m} = 2 \cos m\varphi$  для довільного цілого  $m$ .

**9.17.** Чи утворює групу:

- а) множина  $\mathbb{C}^*$  — ненульових комплексних чисел — стосовно множення;
- б) множина комплексних чисел з фіксованим модулем  $r$  стосовно множення;
- в) множина ненульових комплексних чисел з модулем, не більшим за фіксоване число  $r$ , стосовно множення;
- г) множина матриць  $\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$  стосовно множення?

**9.18.** Чи утворює кільце стосовно операцій додавання та множення комплексних чисел:

- а) множина комплексних чисел вигляду  $a + bi$ , де  $a, b \in \mathbb{Z}$ ;
- б) множина комплексних чисел вигляду  $a + bi$ , де  $a, b \in \mathbb{Q}$ ?

**9.19.** Чи утворює кільце множина комплексних матриць вигляду  $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \in M_2(\mathbb{C})$  стосовно звичайних операцій додавання та множення матриць?

**9.20.** Довести, що множина комплексних чисел утворює поле стосовно операцій додавання та множення комплексних чисел.

**9.21.** Довести, що поле комплексних чисел містить підполе, ізоморфне полю дійсних чисел.

**9.22.** Довести, що поле комплексних чисел ізоморфне полю матриць вигляду  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ , де  $a, b$  — дійсні числа.

**9.23.** Довести, що якщо комплексне число  $z$  є одним з коренів степеня  $n$  з дійсного числа  $a$ , то й спряжене число  $\bar{z}$  є одним з коренів степеня  $n$  з  $a$ .

**9.24.** Довести, що якщо  $\sqrt[n]{z} = \{z_1, z_2, \dots, z_n\}$ , то  $\sqrt[n]{\bar{z}} = \{\bar{z}_1, \bar{z}_2, \dots, \bar{z}_n\}$ .

**9.25.** Довести, що об'єднання множин  $\sqrt[n]{z}$  і  $\sqrt[n]{-z}$  є множина  $\sqrt[2n]{z^2}$ .

**9.26.** Чи правильна рівність  $\sqrt[n^k]{z^k} = \sqrt[n]{z}$  ( $k > 1$ )?

**9.27.** Нехай  $\epsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$  ( $0 \leq k < n$ ). Довести, що:

- а)  $\sqrt[n]{1} = \{\epsilon_0, \epsilon_1, \epsilon_2, \dots, \epsilon_{n-1}\}$ ;
- б)  $\epsilon_k = \epsilon_1^k$  ( $0 \leq k < n$ );
- в)  $\epsilon_k \epsilon_m = \begin{cases} \epsilon_{k+m}, & \text{якщо } k+m < n, \\ \epsilon_{k+m-n}, & \text{якщо } k+m \geq n \end{cases}$  ( $0 \leq k < n, 0 \leq m < n$ );

г) множина  $\mathbb{C}_n$  всіх коренів  $n$ -го степеня з 1 є циклічною групою порядку  $n$  щодо операції множення комплексних чисел.

**9.28.** Довести, що наступні твердження рівносильні:

- a)**)  $\epsilon$  — первісний корінь з 1 степеня  $n$ ;
- б)**) порядок  $\epsilon$  в групі  $\mathbb{C}_n$  дорівнює  $n$ ;
- в)**)  $\epsilon$  — твірний елемент групи  $\mathbb{C}_n$ .

**9.29.** Обчислити суму  $1 + \epsilon + \epsilon^2 + \dots + \epsilon^{n-1}$ , де  $\epsilon$  — первісний корінь степеня  $2n$  з 1.

**9.30.** Знайти добуток всіх коренів  $n$ -го степеня з одиниці.

**9.31.** Знайти суму  $k$ -их степенів всіх коренів  $n$ -го степеня з одиниці.

**9.32.** Довести, що усі корені  $n$ -го степеня з комплексного числа отримуються шляхом домноження одного з них на всі корені  $n$ -го степеня з 1.

# Розділ 10.

## Кільце поліномів

**10.1.** Нехай  $F$  — поле і  $f(x), g(x), h(x) \in F[x]$ . Довести правильність таких властивостей:

- а) якщо  $f(x)$  ділиться на  $g(x)$ , а  $g(x)$  ділиться на  $h(x)$ , то  $f(x)$  ділиться на  $h(x)$ ;
- б) якщо  $f(x)$  і  $h(x)$  діляться на  $g(x)$ , то  $f(x) \pm h(x)$  також ділиться на  $g(x)$ ;
- в) якщо  $f(x)$  ділиться на  $g(x)$ , то для довільного  $p(x) \in F[x]$  добуток  $p(x)f(x)$  також ділиться на  $g(x)$ ;
- г) якщо кожен з поліномів  $f_1(x), \dots, f_k(x) \in F[x]$  ділиться на  $g(x)$ , то на  $g(x)$  буде ділитися й поліном  $p_1(x)f_1(x) + \dots + p_k(x)f_k(x)$ , де  $p_1(x), \dots, p_k(x)$  — довільні поліноми  $F[x]$ ;
- і) будь-який поліном  $f(x)$  ділиться на довільний ненульовий елемент поля  $F$ ;
- д) якщо  $f(x)$  ділиться на  $g(x)$ , то  $f(x)$  також ділиться на  $cg(x)$ , де  $c$  — довільний ненульовий елемент поля  $F$ ;
- е) поліноми  $cf(x)$ , де  $c \in F \setminus \{0\}$ , і лише вони будуть дільниками полінома  $f(x)$ , які мають ту ж степінь, що й  $f(x)$ ;
- є)  $f(x)$  та  $g(x)$  одночасно діляться один на одного тоді і лише тоді, коли  $g(x) = cf(x)$ , де  $c$  — довільний ненульовий елемент  $F$ ;
- ж) довільний дільник одного з двох поліномів  $f(x)$  та  $cf(x)$ , де  $c \in F \setminus \{0\}$ , буде дільником і для другого полінома.

**10.2.** Нехай  $d(x)$  — найбільший спільний дільник поліномів  $f(x)$  і  $g(x)$ . Довести:

- а) існують такі поліноми  $u(x), v(x)$ , що  $\deg u(x) < \deg g(x) - \deg d(x)$ , причому  $d(x) = f(x)u(x) + g(x)v(x)$ ;
- б) у випадку а) маємо також  $\deg v(x) < \deg f(x) - \deg d(x)$ ;
- в) поліноми  $u(x), v(x)$  із а) визначаються однозначно.

**10.3.** Нехай  $f(x)u(x) + g(x)v(x) = d(x)$ , де  $d(x)$  — найбільший спільний дільник  $f(x)$  і  $g(x)$ . Чому дорівнює найбільший спільний дільник  $u(x)$  і  $v(x)$ ?

**10.4.** Довести, що поліноми

- а)  $f(x) = x^{2n} - nx^{n+1} + nx^{n-1} - 1$ ,
  - б)  $g(x) = x^{2n+1} - (2n+1)x^{n+1} + (2n+1)x^n - 1$ ,
  - в)  $h(x) = (n-2m)x^n - nx^{n-m} + nx^m - (n-2m)$
- мають число 1 потрійним коренем.

**10.5.** Довести, що поліном

$$1 + \frac{x}{1!} + \frac{x^2}{3!} + \cdots + \frac{x^n}{n!}$$

не має кратних коренів.

**10.6.** Довести, що поліном

$$a_1x^{n_1} + a_2x^{n_2} + \cdots + a_kx^{n_k}, \quad n_1 < n_2 < \dots < n_k,$$

не має відмінних від нуля коренів кратності, більшої  $k - 1$ .

**10.7.** Довести, що для того, щоб поліном

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

ділиться на  $(x - 1)^{k+1}$ , необхідно і достатньо, щоб виконувались умови:

$$\begin{aligned} a_0 + a_1 + a_2 + \dots + a_n &= 0, \\ a_1 + 2a_2 + \dots + na_n &= 0, \\ a_1 + 4a_2 + \dots + n^2a_n &= 0, \\ \dots &\dots \\ a_1 + 2^ka_2 + \dots + n^ka_n &= 0. \end{aligned}$$