МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

О. О. БЕЗУЩАК
О. Г. ГАНЮШКІН
Є. А. КОЧУБІНСЬКА

НАВЧАЛЬНИЙ ПОСІБНИК ІЗ ЛІНІЙНОЇ АЛГЕБРИ

для студентів механіко-математичного факультету

КИЇВСЬКИЙ УНІВЕРСИТЕТ 2019

УДК 512.64(075.8)
Б40

Рецензенти:

д-р фіз.-мат. наук, проф. Б. В. Олійник
д-р фіз.-мат. наук, проф. Ю. В. Козаченко

Рекомендовано до друку вченою радою
механіко-математичного факультету
(протокол № 3 від 5 листопада 2018 року)

Ухвалено науково-методичною радою
Київського національного університету імені Тараса Шевченка
(протокол № 5-18/19 н. р. від 27 березня 2019 року)

Безущак О. О.

Б40 Навчальний посібник з лінійної алгебри для студентів механіко-математичного факультету / О. О. Безущак, О. Г. Ганюшкін, Є. А. Кочубінська. – К. : ВПЦ "Київський університет", 2019. – 224 с.

Наведено лекції з лінійної алгебри в обсязі, передбаченому планами механіко-математичного факультету. Посібник містить задачі та вправи, які дозволять читачеві краще опанувати лекційний матеріал.

Для студентів математичних спеціальностей університетів.

УДК 512.64(075.8)

© Безущак О. О., Ганюшкін О. Г., Кочубінська Є. А., 2019
© Київський національний університет імені Тараса Шевченка, ВПЦ "Київський університет", 2019

Зміст

Перелік позначень

НСД $(f(x), g(x))$ – найбільший спільний дільник многочленів $f(x)$ і $g(x)$;

НСК $(f(x), g(x))$ – найменше спільне кратне многочленів $f(x)$ і $g(x)$;

$|A|$ – визначник матриці A;

$\arg z$ – аргумент комплексного числа z;

A_φ – матриця лінійного відображення φ;

A^* – приєднана матриця до матриці A;

A_{ij} – алгебричне доповнення елемента a_{ij};

$a \equiv b \pmod{n}$ – числа a і b конгруентні (порівнянні) за модулем числа n;

$\mathbb{C}_n$ – множина всіх комплексних коренів n–го степеня з 1;

$\deg f(x)$ – степінь многочлена $f(x)$;

$\det A$ – визначник матриці A;

E_{ij}, $E_{ij}(a)$, $E_i(a)$ – елементарні матриці;

$f(x) \sim g(x)$ – многочлени $f(x)$ і $g(x)$ асоційовані;

$g(x) \mid f(x)$ – многочлен $g(x)$ ділить многочлен $f(x)$;

$\operatorname{Im} z$ – уявна частина b комплексного числа $z = a + bi$;

$\operatorname{Im} \varphi$ – образ лінійного відображення φ;

$\operatorname{Ker} \varphi$ – ядро лінійного відображення φ;

$K[x]$ – множина всіх многочленів із коефіцієнтами з кільця K;

$M^{\{j_1,\ldots,j_k\}}_{\{i_1,\ldots,i_k\}}$ – мінор порядку k, утворений рядками $i_1, \ldots, i_k$ і стовпцями $j_1, \ldots, j_k$;

$\overline{M}^{\,j}_i$ – доповняльний мінор елемента a_{ij} матриці;

$M/\!\sim$ – фактор-множина множини M за відношенням еквівалентності $\sim$;

$N(\pi)$ – кількість інверсій у підстановці π;

$P[x]$ – множина всіх многочленів із коефіцієнтами з поля P;

$P(x)$ – множина всіх раціональних функцій із коефіцієнтами з поля P;

$\operatorname{rank}(\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_n)$ або $r(\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_n)$ – ранг системи векторів $\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_n$;

$\operatorname{Re} z$ – дійсна частина a комплексного числа $z = a + bi$;

$r_{\min}(A)$ – мінорний ранг матриці A;

S_n – множина всіх підстановок на множині $\{1, 2, \ldots, n\}$ перших n натуральних чисел;

$\operatorname{sp} A$ – слід (сума діагональних елементів) матриці A;

$\operatorname{tr} A$ – слід (сума діагональних елементів) матриці A;

$|z|$ – модуль комплексного числа z;

$\mathbb{Z}_n$ – кільце класів лишків за модулем числа n;

$[\varphi]$ – матриця лінійного відображення φ.

1. Комплексні числа

1.1. Розвиток поняття числа

Поняття абстрактного числа стало для сучасної цивілізації звичним. Деяку настороженість ще викликають комплексні числа, але відчуття глибини поступово зникає. А натуральний ряд уже досяг межі тривіальності.

Проте так було не завжди. Поняття числа пройшло дуже довгу і складну еволюцію. У первісних племен запас чисел був дуже бідним. Наприклад, до появи в Австралії європейців у мовах деяких австралійських племен було всього 3 числівники: 1, 2, і "багато" (≥ 3). Наявність у багатьох мовах, зокрема, в українській, окрім однини і множини ще і двоїни, свідчить, що етап, на якому розрізнялися лише "один", "два" і "багато", був у розвитку поняття числа обов'язковим.

Поступово кількість числівників збільшувалася і в усіх культурних народів на момент виникнення у них писемності уже були досить розвинені поняття про числа, певні операції над ними і ті або інші системи числення. Спочатку розглядалися лише натуральні числа, хоча ще дуже довго натуральний ряд не мислився нескінченним. Але вже у древніх Вавилоні та Єгипті відбулося розширення поняття числа до множини $\mathbb{Q}^+$ додатних раціональних чисел. За кілька століть до нашої ери греки зробили наступний крок і розширили поняття числа до множини $\mathbb{R}^+$ додатних дійсних чисел.

Розширення поняття числа в інший бік – від'ємних чисел – відбулося ще пізніше. Перші кроки тут зробили індійці в VI–VII ст. нашої ери, трохи пізніше естафету перехопили араби, а на початку епохи Відродження підключилися і європейці. Таким чином, на середину минулого тисячоліття поняття числа розширилося до звичної нам зі школи множини $\mathbb{R}$ дійсних чисел.

У XVII ст. італійські математики відчули, що дійсних чисел їм недостатньо, а тому поняття числа потрібно розширювати далі. Головну роль у стимулюванні цього розширення відіграла знаменита формула Кардано[1] для коренів кубічного рівняння. Виявилося, що коли кубічне рівняння з дійсними коефіцієнти має три дійсні корені, то для їх знаходження потрі-

[1] Формула Кардано є класичним прикладом правильності **принципу Арнольда**: кожне іменне твердження чи поняття належить не тому, кому воно приписується. Цю формулу Кардано узнав від Тартальї, який і відкрив її (можливо, ще раніше цю формулу, принаймні деякі часткові випадки, уже знав Ферро) й опублікував без дозволу автора. До речі, Арнольд вважав свій принцип самозастосовним.

бно використовувати числа нового, невідомого досі, типу. На противагу дійсним ці нові числа назвали уявними. Пізніше сукупність чисел, породжених дійсними та уявними числами, об'єднали назвою комплексних чисел.

У XVII – XVIII ст. комплексними числами користуються все активніше, однак жодного логічного чи інтуїтивного обґрунтування вони все ще не мають. Таке обґрунтування з'явиться лише на межі XVIII – XIX ст. (Арган, Гаусс). Ще пізніше Гамільтон інтерпретує комплексні числа як упорядковані пари дійсних.

Пізніше, розглядаючи так звану основну теорему алгебри, ми побачимо, що комплексні числа є неминучим фіналом розширення множини натуральних чисел. А позаяк величезна частина математики і її застосувань (як у повсякденному житті, так і в найсучасніших розділах інших наук) базується на понятті числа та арифметичних операціях над числами, то найкращим майданчиком для цих операцій є саме поле комплексних чисел. Тому не дивно, що комплексні числа постійно з'являються не тільки практично в усіх розділах математики, а й у багатьох суміжних областях (насамперед у фізиці).

1.2. Побудова поля комплексних чисел

Мотиви кожного з розширень $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$ і $\mathbb{R} \subset \mathbb{C}$ поняття числа були чисто алгебричними: певні класи рівнянь не мали розв'язків у старій системі чисел, а тому її розширювали, щоб у новій системі ці рівняння стали розв'язними.[2] До цих розширень ставилися (хоча зазвичай явно і не формулювалися) певні вимоги:

– нові числа мають включати старі;

– на нові числа мають поширитися арифметичні дії, причому дії над старими числами мають бути частковим випадком дій над новими;

– основні закони, які виконувалися для дій над старими числами, мають виконуватися і для дій над новими числами.

Ми вже говорили, що реальна еволюція поняття числа була дуже довгою і звивистою. Тому ми розглянемо дуже схематично лише основні етапи.

На множині $\mathbb{N}$ натуральних чисел визначені дії додавання і множення, для яких виконуються такі закони:

[2] У випадку $\mathbb{Q} \subset \mathbb{R}$ до алгебричних мотивів долучилися й геометричні (більше того, вони були основними), тому цей випадок ми розглядати не будемо.

(I) *комутативні* закони: $a + b = b + a$, $ab = ba$;
(II) *асоціативні* закони: $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$;
(III) *дистрибутивний* закон: $(a + b)c = ac + bc$.
Для множення ще є особливий елемент – *нейтральний*, або *одиниця*:

(IV) $1 \cdot a = a \cdot 1 = a$.

А для додавання такого елемента нема. Першими цією несправедливістю обурилися індійці і ввели *нуль* – нейтральний елемент для додавання:

(IV′) $0 + a = a + 0 = a$.

Поступово прийшло розуміння, що окрім додавання і множення необхідно вміти виконувати й *обернені операції*: за результатом операції й однією з її компонент знаходити іншу компоненту, тобто вміти розв'язувати рівняння вигляду

$$a + x = b \quad \text{і} \quad a \cdot y = b\,.$$

Операції знаходження розв'язків цих рівнянь – $x = b - a$ і $y = b : a$ – називаються відповідно *відніманням* і *діленням*.

Але обернені операції були лише *частковими*. Наприклад, рівняння $2 + x = 3$ і $3 + x = 2$ зовні дуже подібні, однак перше має розв'язок у множині натуральних чисел, а друге – ні. Бажання зробити обернені операції виконуваними завжди привело до двох перших розширень поняття числа.

Розширення $\mathbb{N} \subset \mathbb{Z}$. Це розширення викликане потребою зробити завжди виконуваним віднімання. При цьому для цілих чисел закони (I), (II), (III), (IV), (IV′) залишаються правильними і з'являється новий:

(V) наявність для додавання *протилежних елементів*: для кожного числа a існує таке число $-a$, що $a + (-a) = 0$.

Саме наявність протилежних елементів і робить віднімання у множині $\mathbb{Z}$ скрізь визначеним.

Означення 1. *Множина, в якій визначені додавання і множення елементів, причому ці операції задовольняють закони (I), (II), (III), (IV), (IV′) і (V), називається* ***комутативним кільцем***.

Таким чином, множина $\mathbb{Z}$ цілих чисел зі звичайними додаванням і множенням є комутативним кільцем. Це – історично перший і найважливіший приклад комутативного кільця.

Розширення $\mathbb{Z} \subset \mathbb{Q}$. Цілих чисел виявилося недостатньо. Обернена до множення дія – *ділення* – залишається в $\mathbb{Z}$ визначеною лише частково. Рівняння $2 \cdot x = 4$ розв'язується в $\mathbb{Z}$, а схоже рівняння $2 \cdot x = 5$ – ні. Щоб зробити рівняння $a \cdot x = b$ розв'язним для довільного $a \neq 0$, множина чисел знову розширюється. Розширення $\mathbb{Z} \subset \mathbb{Q}$ використовує кілька глибоких математичних ідей, з якими ми ще будемо зустрічатися неодноразово. Тому зупинимось на цьому розширенні докладніше.

Перша із цих ідей пов'язана з поняттям відношення еквівалентності на множині і пов'язаними із цим відношенням розбиттям на класи еквівалентності та фактор-множиною. Нехай $\sim$ – деяке відношення на множині M. Той факт, що елементи a і b множини M перебувають у відношенні $\sim$, позначаємо $a \sim b$. Відношення $\sim$ називається

(1) *рефлексивним*, якщо $a \sim a$ для всіх $a \in M$;

(2) *симетричним*, якщо для всіх a і b із $a \sim b$ випливає $b \sim a$;

(3) *транзитивним*, якщо для всіх a, b і c із $a \sim b$ та $b \sim c$ випливає $a \sim c$.

Відношення, яке має всі три вказані властивості, називається *відношенням еквівалентності*. Класичними прикладами відношень еквівалентності є відношення рівності елементів (на будь-якій множині) або відношення паралельності (на множині прямих площини або простору).

Множина $\overline{a} = \{b \in M \mid a \sim b\}$ всіх елементів, еквівалентних елементу a, називається *класом еквівалентності* елемента a.

Твердження 1. *Нехай $\overline{a}$ і $\overline{b}$ – два класи еквівалентності. Тоді або ці класи не перетинаються* (тобто $\overline{a} \cap \overline{b} = \varnothing$)*, або збігаються* (тобто $\overline{a} = \overline{b}$).

Доведення. Нехай $\overline{a} \cap \overline{b} \neq \varnothing$. Виберемо довільний елемент $c \in \overline{a} \cap \overline{b}$ і довільний елемент $x \in \overline{b}$. Тоді $c \sim a$, $c \sim b$ і $x \sim b$. Із цих співвідношень та симетричності і транзитивності відношення $\sim$ випливає, що $x \sim a$. Отже, $\overline{b} \subseteq \overline{a}$. Аналогічно доводиться, що $\overline{a} \subseteq \overline{b}$. Тому $\overline{a} = \overline{b}$. □

Отже, множина M розбивається на класи еквівалентності. Сукупність $\{\overline{a} \mid a \in M\}$ класів еквівалентності називається *фактор-множиною* множини M за відношенням еквівалентності $\sim$ і позначається $M/\sim$.

Розглянемо тепер множину $Q = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, елементами якої є впорядковані пари вигляду (m, n), де m є довільним цілим числом, а n – довільним ненульовим цілим числом. Пару (m, n) будемо записувати у вигляді $\dfrac{m}{n}$ і називати *раціональним дробом*. На множині Q раціональних дробів визначимо таке відношення:

$$\frac{m}{n} \sim \frac{p}{q} \quad \text{тоді й лише тоді, коли} \quad mq = np.$$

Вправа 1. *Перевірте, що відношення $\sim$ є відношенням еквівалентності.*

Фактор-множина $\mathbb{Q} = Q/\sim$ називається множиною *раціональних чисел*, а її елементи (тобто класи еквівалентності $\overline{(m, n)}$) — *раціональними числами*.

Додавання і множення раціональних чисел визначимо такими правилами:

$$\overline{(m_1, n_1)} + \overline{(m_2, n_2)} = \overline{(m_1 n_2 + m_2 n_1, n_1 n_2)}, \tag{1.1}$$

$$\overline{(m_1, n_1)} \cdot \overline{(m_2, n_2)} = \overline{(m_1 m_2, n_1 n_2)}. \tag{1.2}$$

Зауваження. У зв'язку із правилами (1.1) і (1.2) виникає одне питання (подібне питання виникатиме в майбутньому часто): чи є ці правила коректними? Кожне раціональне число можна зобразити раціональним дробом нескінченною кількістю способів. Наприклад, раціональні дроби $\dfrac{1}{2}, \dfrac{2}{4}, \dfrac{3}{6}, \dfrac{4}{8}$ і т. д. визначають одне й те саме раціональне число. Правила (1.1) і (1.2) будуть коректними, якщо при заміні в лівих частинах цих правил дробів $\dfrac{m_1}{n_1}$ і $\dfrac{m_2}{n_2}$ еквівалентними результати дій із новими дробами будуть еквівалентними попереднім результатам. Це справді так:

Вправа 2. *Доведіть, що правила* (1.1) *і* (1.2) *є коректними, тобто що клас еквівалентності, в який попадає результат дії, не залежить від вибору представників класів еквівалентності $\overline{(m_1, n_1)}$ і $\overline{(m_2, n_2)}$.*

Якщо тепер ціле число m ототожнити із класом $\overline{(m,1)}$, то одержимо занурення $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Отже, нові числа містять старі. Крім того, для цілих чисел правила (1.1) і (1.2) набувають вигляду

$$\overline{(m_1,1)} + \overline{(m_2,1)} = \overline{(m_1+m_2,1)}, \quad \overline{(m_1,1)} \cdot \overline{(m_2,1)} = \overline{(m_1m_2,1)},$$

тобто додавання і множення цілих чисел як раціональних дає той самий результат, що й додавання і множення їх як цілих чисел.

Нейтральним елементом для додавання залишається число 0 (яке тепер ототожнюється із класом дробів вигляду $\frac{0}{m}$), а нейтральним елементом для множення — число 1 (яке тепер ототожнюється із класом дробів вигляду $\frac{m}{m}$). Крім того, на множині $\mathbb{Q}$ природно визначаються обернені дії віднімання та ділення:

$$\overline{(m_1,n_1)} - \overline{(m_2,n_2)} = \overline{(m_1n_2 - m_2n_1, n_1n_2)}, \tag{1.3}$$

$$\overline{(m_1,n_1)} : \overline{(m_2,n_2)} = \overline{(m_1n_2, n_1m_2)}. \tag{1.4}$$

Легко перевіряється, що сформульовані вище закони (I)–(V) для цілих чисел виконуються і для раціональних. Але тепер з'являється ще аналог закону (V) для множення:

(V′) наявність для множення *обернених елементів*: для кожного ненульового числа a існує таке число a^{-1}, що $a \cdot a^{-1} = 1$.

Означення 2. *Множина P, в якій визначені додавання і множення елементів, причому ці дії задовольняють закони (I), (II), (III), (IV), (IV′), (V), (V′), і $0 \neq 1$, називається* ***полем****. Якщо елементами множини P є числа, то поле називається* ***числовим****.*

Вправа 3. *Доведіть, що в кожному полі*
а) виконується рівність $a \cdot 0 = 0$;
б) із рівності $ab = 0$ випливає, що або $a = 0$, або $b = 0$.

Отже, множина $\mathbb{Q}$ раціональних чисел зі звичайними додаванням і множенням утворює поле. У полі всі чотири арифметичні дії – додавання, віднімання, множення, ділення (крім ділення на 0) – уже можна виконувати без жодних обмежень. Зокрема, у полі вже нема проблем із лінійними рівняннями: кожне рівняння вигляду $ax + b = 0$, $a \neq 0$, із коефіцієнтами з даного поля буде мати в цьому полі розв'язок.

Однак із рівняннями вищих степенів ситуація складніша. Навіть дуже прості рівняння з раціональними коефіцієнтами, наприклад, $x^2 = 2$, можуть не мати раціональних розв'язків. Тому поняття числа вимагає подальшого розширення. Щоб зробити такі рівняння розв'язними, математики винайшли інший метод, який називається *приєднанням кореня*: вводять новий символ, який оголошують коренем даного рівняння, а потім визначаються, які елементи ще треба ввести, щоб арифметичні дії можна було поширити і на цей корінь.

Зокрема, у випадку рівняння $x^2 = 2$ цей метод виглядає так: вводять новий символ $\sqrt{2}$, який оголошують коренем цього рівняння (тобто має виконуватися рівність $\sqrt{2} \cdot \sqrt{2} = 2$). Щоб додавання і множення можна було виконувати без обмежень, потрібно також розглянути всі числа вигляду $a + b\sqrt{2}$, де a і b – раціональні. Таких чисел уже досить, бо

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}, \tag{1.5}$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}. \tag{1.6}$$

Вправа 4. *Доведіть, що множина* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{a} \mid a, b \in \mathbb{Q}\}$ *утворює числове поле.*

Розширення $\mathbb{R} \subset \mathbb{C}$. Однак навіть розширення поля $\mathbb{Q}$ до множини $\mathbb{R}$ дійсних чисел не робить розв'язними всі рівняння вищих степенів. Рівняння $x^2 = 1$ має в $\mathbb{R}$ два корені – 1 і -1, – а рівняння $x^2 = -1$ – жодного. Щоб зробити розв'язним і це рівняння, знову використовується ідея приєднання кореня. Для цього введемо новий символ i, який будемо вважати коренем рівняння $x^2 = -1$ (тобто вважаємо, що $i^2 = -1$). Зауважимо, що символ i для позначення $\sqrt{-1}$ (від латинського imaginarius – уявний) уперше вжив у 1777 році Ойлер. Щоб поширити на новий символ арифметичні дії, розглянемо формальні вирази вигляду $a + bi$, де a, b – дійсні числа, і розглянемо множину

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

усіх таких виразів. Додавання і множення вказаних виразів визначимо правилами (ці правила є природними, якщо ми хочемо виконання комутативних і дистрибутивного законів та рівності $i^2 = -1$):

$$\begin{aligned} (a + bi) + (c + di) &:= (a + c) + (b + d)i; \\ (a + bi) \cdot (c + di) &:= (ac - bd) + (ad + bc)i. \end{aligned} \tag{1.7}$$

Вирази вигляду $a+bi$ будемо називати *комплексними числами*, а множину $\mathbb{C}$ – *полем комплексних чисел*.

Кожне дійсне число a ототожнимо з комплексним числом вигляду $a + 0i$. Це дає нам занурення $\mathbb{R} \hookrightarrow \mathbb{C}$. Для таких комплексних чисел правила (1.7) набувають вигляду

$$(a + 0i) + (c + 0i) = (a + c) + 0i, \quad (a + 0i) \cdot (c + 0i) = ac + 0i.$$

Отже, додавання і множення дійсних чисел як комплексних дає той самий результат, що й додавання і множення їх як дійсних чисел, тобто дії над дійсними числами є частковим випадком дій над комплексними.

Теорема 1. *Множина $\mathbb{C}$, в якій додавання і множення визначаються правилами* (1.7)*, задовольняє всі аксіоми поля.*

Доведення. Із правил (1.7) безпосередньо видно, що додавання і множення комплексних чисел є комутативним. Крім того, число $0 = 0 + 0i$ залишається нейтральним елементом для додавання, а число $1 = 1 + 0i$ – для множення:

$$(a + bi) + (0 + 0i) = (a + 0) + (b + 0)i = a + bi;$$
$$(a + bi) \cdot (1 + 0i) = (a \cdot 1 - b \cdot 0) + (a \cdot 0 + b \cdot 1)i = a + bi.$$

Для перевірки асоціативності множення розглянемо довільні комплексні числа $z_1 = a + bi$, $z_2 = c + di$ і $z_3 = e + fi$. Маємо

$$(z_1 z_2)z_3 = ((a + bi)(c + di))\,(e + fi) = ((ac - bd) + (ad + bc)i)\,(e + fi) =$$
$$= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i =$$
$$= (a + bi)\,((ce - df) + (cf + de)i) = (a + bi)\,((c + di)(e + fi)) = z_1(z_2 z_3).$$

Отже, множення комплексних чисел є асоціативним.

Нехай тепер $z = a + bi$ – ненульове комплексне число. Оскільки в цьому випадку принаймні одне з дійсних чисел a і b є ненульовим, то й сума $a^2 + b^2$ буде ненульовою. Покажемо, що число

$$\frac{a}{a^2 + b^2} + \left(-\frac{b}{a^2 + b^2}\right) i$$

буде оберненим до z. Справді,

$$(a + bi)\left(\frac{a}{a^2 + b^2} + \left(-\frac{b}{a^2 + b^2}\right) i\right) = \frac{a^2 + b^2}{a^2 + b^2} + \frac{-ab + ab}{a^2 + b^2} i = 1 + 0i = 1.$$

Таким чином, для кожного ненульового комплексного числа існує обернене. Перевірку решти аксіом поля залишаємо читачеві як вправу. □

Зауваження. Оскільки

$$a + bi = (a + 0i) + (b + 0i) \cdot (0 + 1i),$$

а комплексні числа $a + 0i$ і $b + 0i$ ми ототожнили з дійсними числами a і b відповідно, то число $0 + 1i$ зручно ототожнити із символом i.

Зображення комплексного числа у вигляді $z = a + bi$, де $a, b \in \mathbb{R}$, називається *алгебричною формою* його запису. При цьому a називається *дійсною частиною* числа z (записується $\mathrm{Re} z = a$), а b – *уявною частиною* (записується $\mathrm{Im} z = b$).

Із правил (1.7) та властивостей дій випливають такі правила для обернених дій:

- *віднімання* задається правилом

$$(a + bi) - (c + di) = (a - c) + (b - d)i;$$

- *ділення* задається правилом

$$\frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\, i.$$

Досить громіздку формулу для ділення запам'ятовувати не варто, бо ділення комплексних чисел фактично зводиться до множення чисельника і знаменника дробу $\dfrac{a + bi}{c + di}$ на число $c - di$. Справді,

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\, i.$$

1.3. Геометрична інтерпретація[3]

Візьмемо площину із прямокутною декартовою системою координат. Оскільки комплексне число $z = a + bi$ можна розглядати як впорядковану пару (a, b) дійсних чисел, то його можна ототожнити із точкою (a, b) цієї площини (рис. 1).

Таким чином, поле $\mathbb{C}$ комплексних чисел природно ототожнюється з множиною точок площини (яку часто називають *комплексною площиною* і також позначають символом $\mathbb{C}$). При цьому вісь абсцис часто називають *дійсною* віссю, а вісь ординат – *уявною*.

[3] До геометричної інтерпретації комплексних чисел і дій над ними незалежно прийшли видатний німецький математик Гаусс (1797, опубліковано в 1831), данець Вессель (1799), швейцарець Арган (1806). Гауссу ж належить і термін "комплексне число".

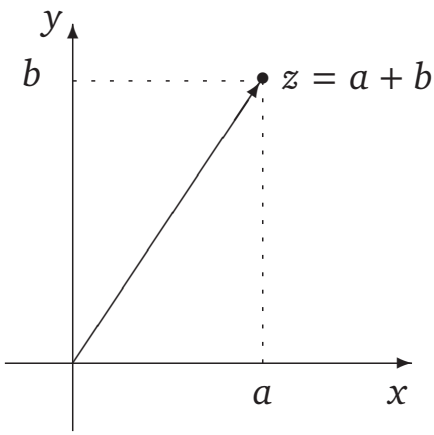


Рис. 1

Часом зручніше зображувати число $z = a + bi$ не точкою площини, а вектором із координатами (a, b). Зокрема, при такому зображенні дуже просту геометричну інтерпретацію отримує додавання комплексних чисел: із правила (1.7) випливає, що воно збігається із звичайним додаванням векторів.

Довжина вектора, яким зображується число $z = a + bi$, називається *модулем* числа z і позначається $|z|$. Очевидно, що $|z| = \sqrt{a^2 + b^2}$.

Поруч із декартовою часто використовується так звана полярна система координат, у якій положення точки на площині характеризується довжиною радіус-вектора цієї точки та кутом між додатним напрямком осі Ox і радіус-вектором. Перехід на площині від декартової до полярної системи приведе до ще однієї форми запису комплексних чисел. Для точки, якою зображується комплексне число z, довжина радіус-вектора дорівнює модулю $|z|$ цього числа, а кут між додатним напрямком осі Ox і цим вектором називається *аргументом* числа z і позначається $\arg z$. Аргумент комплексного числа визначений із точністю до доданка, який є цілим кратним повного кута 2π. Аргумент числа 0 не визначений.

Якщо модуль і аргумент числа $z = a + bi$ дорівнюють відповідно r і φ, то з рис. 2 одразу видно, що $a = r\cos\varphi$, $b = r\sin\varphi$. Тому

$$z = r(\cos\varphi + i\sin\varphi)\,. \tag{1.8}$$

Запис комплексного числа у вигляді (1.8) називається *тригонометричною формою* запису.

Щоб перейти від алгебричної форми запису комплексного числа $z = a + bi$ до тригонометричної, потрібно знайти модуль r та аргумент

φ числа z. Із рис. 2 легко бачити, що

$$r = \sqrt{a^2 + b^2}, \tag{1.9}$$

$$\cos\varphi = \frac{a}{r}, \qquad \sin\varphi = \frac{b}{r}. \tag{1.10}$$

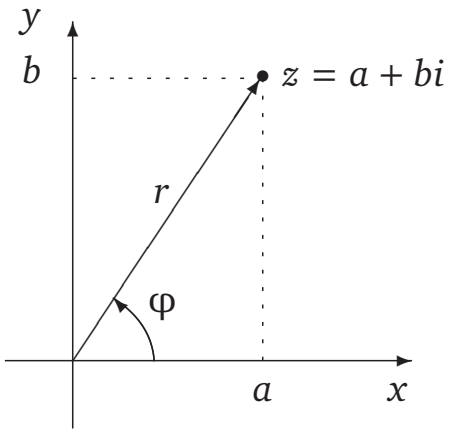


Рис. 2

Оскільки на проміжку $[0, 2\pi)$ функції cos і sin майже всіх своїх значень набувають двічі, то для правильного визначення аргументу комплексного числа потрібно використовувати обидва співвідношення (1.10). Можна обмежитися одним із цих співвідношень, якщо додатково враховувати знаки коефіцієнтів a і b.

Тригонометрична форма добре пристосована до множення комплексних чисел (і таких похідних операцій, як ділення, піднесення до степеня, добування кореня). Справді,

$$r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= r_1r_2\big((\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)\big) =$$

$$= r_1r_2\big(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\big). \tag{1.11}$$

Таким чином, *при множенні комплексних чисел їх модулі перемножаються, а аргументи додаються*.

Оскільки $1 = 1(\cos 0 + i\sin 0)$, то із правила множення комплексних чисел у тригонометричній формі одразу одержуємо такі формули:

$$\big(r(\cos\varphi + i\sin\varphi)\big)^{-1} = r^{-1}\big(\cos(-\varphi) + i\sin(-\varphi)\big), \tag{1.12}$$

$$\frac{r_1(\cos\varphi_1 + i\sin\varphi_1)}{r_2(\cos\varphi_2 + i\sin\varphi_2)} = \frac{r_1}{r_2}\big(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)\big)\,. \qquad (1.13)$$

За допомогою індукції легко доводиться, що для кожного натурального числа n виконується рівність

$$\big(r(\cos\varphi + i\sin\varphi)\big)^n = r^n(\cos n\varphi + i\sin n\varphi)\,. \qquad (1.14)$$

Враховуючи (1.12), можна стверджувати, що рівність (1.14) виконується для всіх цілих чисел. Ця рівність – правило піднесення комплексного числа до цілого степеня – називається *формулою Муавра*.

Наслідок 1. *а)* $\cos n\varphi = \sum\limits_{k\geqslant 0}(-1)^k\binom{n}{2k}\cos^{n-2k}\varphi\cdot\sin^{2k}\varphi$*;*

б) $\sin n\varphi = \sum\limits_{k\geqslant 0}(-1)^k\binom{n}{2k+1}\cos^{n-2k-1}\varphi\cdot\sin^{2k+1}\varphi$.

Доведення. Обчислюючи $(\cos\varphi + i\sin\varphi)^n$ двома способами – за формулою бінома Ньютона і за формулою Муавра – одержуємо

$$\cos n\varphi + i\sin n\varphi = \sum_{k=0}^{n}\binom{n}{k}\cos^{n-k}\varphi\cdot i^k\sin^k\varphi\,.$$

Для завершення доведення лишилося порівняти дійсні й уявні частини обох частин цієї рівності. □

На завершення цього параграфа розглянемо деякі властивості модуля комплексного числа.

Теорема 2.

а) $|z|\geq 0$*, причому* $|z| = 0$ *тоді й лише тоді, коли* $z = 0$;

б) $|z|\geq|\operatorname{Re} z|\geq\operatorname{Re} z$*,* $|z|\geq|\operatorname{Im} z|\geq\operatorname{Im} z$;

в) $|z_1z_2| = |z_1|\cdot|z_2|$*,* $|z_1/z_2| = |z_1|/|z_2|$;

г) якщо $|z|\neq 0$*, то* $|z^n| = |z|^n$ *для довільного* $n\in\mathbb{Z}$;

д) $\big||z_1| - |z_2|\big|\leq|z_1\pm z_2|\leq|z_1| + |z_2|$.

Доведення. а) і б) очевидним чином випливають із геометричної інтерпретації комплексних чисел.

в) Це випливає з рівностей (1.11) та (1.13) відповідно.

г) випливає з рівності (1.14).

д) є переформулюванням в термінах комплексних чисел відомої нерівності трикутника: третя сторона трикутника не менша за різницю двох інших і не більша за їх суму. □

Вправа 5. *Доведіть, що для довільних комплексних чисел* $z_1, z_2, \ldots, z_n$ *виконується нерівність* $|z_1 + z_2 + \ldots + z_n|\leq|z_1| + |z_2| + \ldots + |z_n|$.

1.4. Спряженість

Спряженим до комплексного числа $z = a + bi$ називається число $\overline{z} = a - bi$. Зокрема, число збігається зі своїм спряженим (тобто $\overline{z} = z$) тоді й лише тоді, коли воно є дійсним.

Перехід до спряженого числа має дуже просту геометричну інтерпретацію: це симетрія відносно дійсної осі (рис. 3).

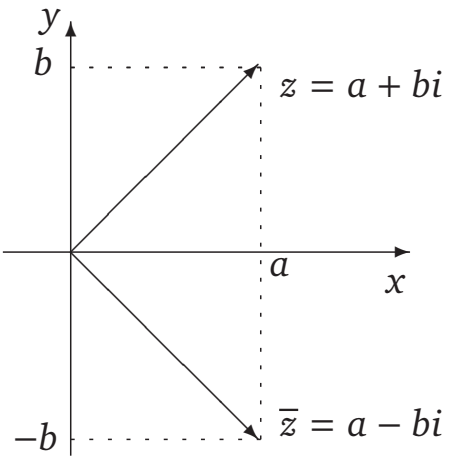


Рис. 3

Із геометричної інтерпретації спряження одразу випливають такі його властивості:

$$\overline{\overline{z}} = z, \quad |\overline{z}| = |z|, \quad \arg \overline{z} = -\arg z. \tag{1.15}$$

Крім того, з означення спряженого числа одразу випливає, що

$$\operatorname{Re} z = \frac{z + \overline{z}}{2}, \qquad \operatorname{Im} z = \frac{z - \overline{z}}{2i}. \tag{1.16}$$

Безпосередньо перевіряється, що $z \cdot \overline{z} = |z|^2$. Тому для кожного ненульового числа z

$$z^{-1} = \frac{\overline{z}}{|z|^2}. \tag{1.17}$$

Твердження 2. *Спряження зберігає арифметичні операції*:

$$\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}, \quad \overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}, \quad \overline{z^{-1}} = \overline{z}^{-1}, \quad \overline{z_1/z_2} = \overline{z_1}/\overline{z_2}\,.$$

Доведення. Перевіримо, наприклад, другу рівність. Нехай $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$. Тоді $\overline{z}_1 = a_1 - b_1 i$, $\overline{z}_2 = a_2 - b_2 i$ і

$$\overline{z_1} \cdot \overline{z_2} = (a_1 - b_1 i) \cdot (a_2 - b_2 i) = (a_1 a_2 + b_1 b_2) - (a_1 b_2 + a_2 b_1) i = \overline{z_1 z_2}.$$

Інші рівності перевіряються аналогічно. □

Наслідок 2. *Якщо многочлен $f(x)$ із дійсними коефіцієнтами має комплексний корінь z (тобто $f(z) = 0$), то спряжене число $\overline{z}$ також буде коренем $f(x)$.*

Доведення. Справді, нехай $f(x) = a_n x^n + \ldots + a_1 x + a_0$ і $f(z) = 0$. Тоді

$$0 = \overline{0} = \overline{a_n z^n + \ldots + a_1 z + a_0} = \overline{a_n z^n} + \ldots + \overline{a_1 z} + \overline{a_0} =$$
$$= \overline{a_n}\,\overline{z^n} + \ldots + \overline{a_1}\,\overline{z} + \overline{a_0} = a_n \overline{z}^{\,n} + \ldots + a_1 \overline{z} + a_0. \qquad \square$$

Якщо $z = a + ib$, то $z \cdot \overline{z} = a^2 + b^2 = |z|^2$. Число $a^2 + b^2$ називають *нормою* числа z і позначають $N(z)$. Із означення норми одразу випливає, що

$$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{\overline{z}}{N(z)}; \qquad \frac{z}{u} = \frac{z \cdot \overline{u}}{N(u)}. \tag{1.18}$$

Оскільки $N(z) = |z|^2$ і $|z_1 z_2| = |z_1| \cdot |z_2|$, то $N(z_1 z_2) = N(z_1) \cdot N(z_2)$. Звідси для чисел $z_1 = a + ib$ і $z_2 = c + id$ маємо цікаву арифметичну тотожність:

$$(a^2 + b^2) \cdot (c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \tag{1.19}$$

Зокрема, *якщо кожне з натуральних чисел m і n є сумою двох квадратів, то їх добуток mn також розкладається в суму двох квадратів*. Цей факт і різні його узагальнення відіграють важливу роль у теорії чисел.

1.5. Корені

Означення 3. *Нехай z – комплексне число, а n – натуральне. Комплексне число w називається* ***коренем n-го степеня із*** *z, якщо $w^n = z$.*

Для натурального числа n і дійсного числа a кількість дійсних коренів n-го степеня з a може дорівнювати 0, 1 або 2. Зокрема, якщо $a > 0$, то завжди існує рівно один додатний корінь n-го степеня з a (це доводиться в курсі математичного аналізу), який називається *арифметичним коренем* n-го степеня з a і позначається $\sqrt[n]{a}$ або $a^{1/n}$. У полі $\mathbb{C}$ ситуація складніша: коли коренів даного степеня з даного числа кілька, то виділити із цих коренів якийсь канонічний не можна. Зокрема, тому, що в полі $\mathbb{C}$ не можна визначити природного відношення порядку. Справді, для відношення порядку $<$ на $\mathbb{C}$ на множині додатних чисел

$$\mathbb{C}^+ = \{z \in \mathbb{C} \mid z > 0\}$$

потрібно вимагати виконання таких двох умов:

1) для будь-якого ненульового числа $z \in \mathbb{C}$ рівно одне із чисел z і $-z$ є додатним;

2) добуток довільних двох додатних чисел u і w є додатним числом.

Але друга умова суперечить першій: у кожній із пар $(1, -1)$ та $(i, -i)$ є додатне число, а тому додатними будуть і числа

$$1 = 1 \cdot 1 = (-1) \cdot (-1) \quad \text{та} \quad -1 = i \cdot i = (-i) \cdot (-i),$$

що суперечить першій умові.

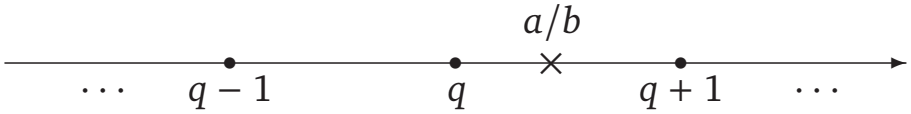
Для подальшого викладу нам знадобиться один факт з арифметики.

Теорема 3 (про ділення з остачею)**.** *Для кожної пари цілих чисел a і b, $b \neq 0$, існують такі цілі числа q і r, які задовольняють умови*

$$a = qb + r\,, \qquad 0 \leqslant r < |b|\,. \tag{1.20}$$

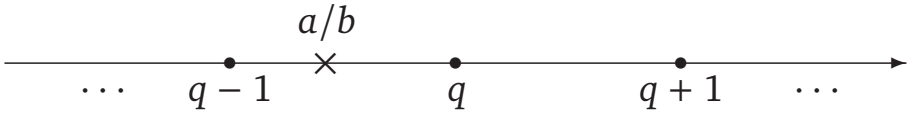
Числа q і r визначені однозначно.

Доведення. Нехай спочатку $b > 0$. Позначимо через q цілу частину числа a/b.



Тоді $a/b = q + \alpha$, де $0 \leqslant \alpha < 1$. Після множення обох частин на b отримуємо $a = qb + r$, де $r = \alpha \cdot b$. Очевидно, що $0 \leqslant r < b$.

Нехай тепер $b < 0$. Позначимо через q ціле число, яке найближче до a/b справа (тобто $q - 1 < a/b \leqslant q$).



Тоді $a/b = q + \alpha$, де $-1 < \alpha \leqslant 0$. Після множення обох частин на b отримуємо: $a = qb + r$, де $r = \alpha \cdot b$. Знову маємо, що $0 \leqslant r < |b|$.

Для доведення єдиності пари q, r припустимо, що

$$a = q_1 b + r_1 = q_2 b + r_2\,.$$

Очевидно, що, коли $r_1 = r_2$, то $q_1 = q_2$. Якщо ж $r_1 \neq r_2$, то можна вважати, що $r_1 < r_2$. Але тоді $r_2 - r_1 = b(q_1 - q_2)$, причому $0 < r_2 - r_1 < |b|$ і $|b(q_1 - q_2)| \geqslant |b| \cdot 1 = |b|$, що неможливо. □

Числа q і r із теореми 3 називаються відповідно *часткою* та *остачею* від ділення a на b.

Наслідок 3. *Різниця $a_1 - a_2$ ділиться на b тоді й лише тоді, коли a_1 і a_2 при діленні на b дають однакові остачі.*

Доведення. Нехай $a_1 = q_1 b + r_1$, $a_2 = q_2 b + r_2$. Тоді

$$b \mid (a_1 - a_2) \;\Leftrightarrow\; b \mid \big((q_1 - q_2)b + (r_1 - r_2)\big) \;\Leftrightarrow$$

$$\Leftrightarrow\quad b \mid (r_1 - r_2) \;\Leftrightarrow\; r_1 - r_2 = 0 \;\Leftrightarrow\; r_1 = r_2\,. \qquad \square$$

Очевидно, що для кожного натурального числа n рівняння $w^n = 0$ має лише нульовий розв'язок, а тому для довільного n є тільки один корінь n-го степеня з 0 – це 0. Для коренів із ненульових чисел картина цікавіша.

Теорема 4. *Кожне ненульове комплексне число $z = r(\cos\varphi + i\sin\varphi)$ має рівно n різних коренів n-го степеня. Ці корені мають вигляд*

$$\sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right),\ k = 0, 1, \ldots, n-1. \tag{1.21}$$

Доведення. Нехай $w = t(\cos\psi + i\sin\psi)$ є коренем n-го степеня із z. Тоді за формулою Муавра

$$t^n = r \quad \text{і} \quad n\psi = \varphi + 2k\pi, k \in \mathbb{Z},$$

звідки

$$t = \sqrt[n]{r} \quad \text{і} \quad \psi = \frac{\varphi + 2k\pi}{n},\quad k \in \mathbb{Z}\,.$$

Однак аргумент комплексного числа визначений лише з точністю до доданка, кратного 2π. Тому треба ще з'ясувати, коли різним k відповідає одне й те ж комплексне число:

$$\frac{\varphi + 2k_1\pi}{n} - \frac{\varphi + 2k_2\pi}{n} = 2m\pi \quad \Leftrightarrow$$

$$\Leftrightarrow\quad \frac{2\pi(k_1 - k_2)}{n} = 2m\pi \quad \Leftrightarrow \quad n \mid (k_1 - k_2)\,.$$

Але різниця $k_1 - k_2$ ділиться на n тоді й лише тоді, коли k_1 і k_2 мають однакові остачі від ділення n. Тому різних коренів буде стільки, скільки є різних остач від ділення на n, тобто n. Зокрема, щоб одержати всі корені, можна взяти $k = 0, 1, \ldots, n-1$. $\square$

Із теореми 4 випливає, що, коли $z \neq 0$, то корені n-го степеня із z є вершинами правильного n-кутника, вписаного в коло радіуса $\sqrt[n]{|z|}$ із центром у початку координат (рис. 4). Оскільки усі вершини правильного n-кутника рівноправні, то й усі корені n-го степеня із z рівноправні.

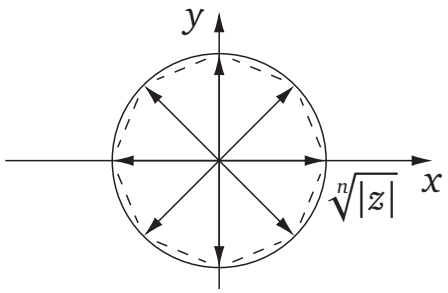


Рис. 4

1.6. Корені з 1

Особливу роль відіграють корені з 1. За теоремою 4 корені степеня n з 1 мають вигляд

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = 0, 1, \ldots, n-1. \tag{1.22}$$

Із геометричної інтерпретації комплексних чисел випливає, що ці корені розташовані у вершинах правильного n-кутника, вписаного у коло радіуса 1 із центром у початку координат, причому одна з вершин (яка відповідає кореню $\varepsilon_0 = 1$) лежить у точці $(1, 0)$. На рис. 5 зображено корені 6-го степеня з одиниці.

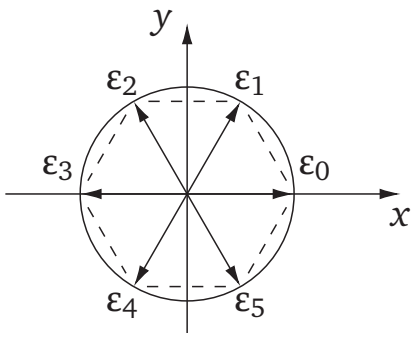


Рис. 5

Множину всіх коренів n-го степеня з 1 будемо позначати $\mathbb{C}_n$.

Лема 1. *Якщо $\varepsilon^n = 1$, то $\varepsilon^{kn+r} = \varepsilon^r$ для довільних цілих чисел k і r.*

Доведення. $\varepsilon^{kn+r} = \varepsilon^{kn} \cdot \varepsilon^r = (\varepsilon^n)^k \cdot \varepsilon^r = 1^k \cdot \varepsilon^r = \varepsilon^r$. □

Твердження 3 (про мультиплікативну замкненість множини $\mathbb{C}_n$)**.** *Якщо $u, v \in \mathbb{C}_n$, то кожне із чисел uv, u^{-1}, u/v також належить множині $\mathbb{C}_n$.*

Доведення. Нехай $u, v \in \mathbb{C}_n$. Тоді $u^n = 1$ і $v^n = 1$. Користуючись комутативністю множення, отримуємо

$$(uv)^n = u^n v^n = 1 \cdot 1 = 1, \quad \left(\frac{u}{v}\right)^n = \frac{u^n}{v^n} = \frac{1}{1} = 1, \quad (u^{-1})^n = \left(\frac{1}{u}\right)^n = \frac{1}{u^n} = 1.$$

□

Твердження 4. *Якщо w – фіксований корінь n-го степеня із числа $z \neq 0$, то множина всіх коренів n-го степеня із z збігається із множиною*

$$\{\varepsilon_0 w,\ \varepsilon_1 w,\ \varepsilon_2 w,\ \ldots,\ \varepsilon_{n-1} w\}.$$

Доведення. Нехай ε – довільний корінь степеня n з 1. Тоді

$$(\varepsilon w)^n = \varepsilon^n w^n = 1 \cdot z = z,$$

тобто εw також є коренем степеня n із числа z.

Отже, кожне із чисел $\varepsilon_0 w$, $\varepsilon_1 w$, …, $\varepsilon_{n-1} w$ є коренем степеня n із z. Оскільки числа ε_0, ε_1, …, ε_{n-1} попарно різні і $w \neq 0$, то попарно різними є також числа $\varepsilon_0 w$, $\varepsilon_1 w$, …, $\varepsilon_{n-1} w$. Оскільки їх рівно n, то це всі корені n-го степеня із z. □

Таким чином, при добуванні коренів n-го степеня з комплексних чисел корені n-го степеня з 1 відіграють таку ж роль, як знаки ± при добуванні квадратних коренів із дійсних чисел.

Твердження 5. $\varepsilon_k = \varepsilon_1^k$.

Доведення. За формулою Муавра маємо

$$\varepsilon_1^k = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \varepsilon_k.$$

□

Отже, всі корені n-го степеня з 1 є степенями кореня ε_1. Крім ε_1 таку властивість можуть мати й деякі інші корені n-го степеня з 1.

Означення 4. *Число ε називається* ***первісним*** *коренем n-го степеня з 1, якщо множина $\mathbb{C}_n$ усіх коренів n-го степеня з 1 збігається із множиною степенів $\varepsilon^0 = 1, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}$ цього кореня.*

Нехай ε є коренем якогось степеня з 1. Натуральне число m називається *порядком* кореня ε, якщо m є найменшим натуральним числом, для якого $\varepsilon^m = 1$.

Твердження 6. *Число ε буде первісним коренем n-го степеня з 1 тоді й лише тоді, коли його порядок дорівнює n.*

Доведення. Необхідність. Нехай ε – первісний корінь n-го степеня з 1. Оскільки $\varepsilon^n = 1$, то порядок ε не перевищує n. Припустимо, що його порядок дорівнює $m < n$. Візьмемо довільне ціле число k і розділимо його на m з остачею: $k = mq + r$, $0 \le r < m$. Тоді за лемою 1 $\varepsilon^k = \varepsilon^r$. Звідси випливає, що кожен степінь ε збігається з одним із чисел $\varepsilon^0 = 1$, $\varepsilon^1, \ldots, \varepsilon^{m-1}$, тобто різних чисел серед степенів ε буде не більше, ніж m. Але це суперечить первісності ε. Отже, ε має порядок n.

Достатність. Нехай ε – корінь n-го степеня з 1 і має порядок n. Тоді всі його степені $\varepsilon^0, \varepsilon^1, \ldots, \varepsilon^{n-1}$ є попарно різними. Справді, якби для якихось показників $0 \le k < m < n$ виконувалась рівність $\varepsilon^k = \varepsilon^m$, то після ділення обох частин на ε^k отримали б рівність $1 = \varepsilon^{m-k}$, яка суперечить тому, що ε має порядок n. Оскільки всі ці степені є коренями n-го степеня з 1 та їх n, то одержуємо всі корені степеня n з 1. Тому ε є первісним коренем n-го степеня з 1. □

Зауважимо, що інколи за означення первісного кореня з 1 беруть твердження 6. Тоді означення 4 стає твердженням.

Твердження 7. *Число ε_k буде первісним коренем n-го степеня з 1 тоді й лише тоді, коли числа k і n – взаємно прості.*

Доведення. Необхідність. Нехай числа k і n не є взаємно простими та $d > 1$ – їх спільний дільник. Тоді $k = k_1 d$, $n = n_1 d$ і

$$\varepsilon_k^{n_1} = (\varepsilon_1^k)^{n_1} = \varepsilon_1^{k_1 d n_1} = (\varepsilon_1^{n_1 d})^{k_1} = (\varepsilon_1^n)^{k_1} = 1^{k_1} = 1\,.$$

Оскільки $n_1 < n$, то за твердженням 6 ε_k не є первісним коренем n-го степеня з 1.

Достатність. Нехай тепер числа k і n – взаємно прості. Припустимо, що для деякого натурального числа m виконується рівність

$$\varepsilon_k^m = (\varepsilon_1^k)^m = \varepsilon_1^{km} = 1\,.$$

Тоді із твердження 5 і леми 1 випливає, що km ділиться на n. Але k і n взаємно прості, тому на n має ділитися m. Отже, $m \geq n$, тобто порядок ε_k є не меншим, ніж n. З іншого боку, ε_k є коренем n-го степеня з 1, а тому його порядок не більший, ніж n. Таким чином, ε_k має порядок n і за твердженням 6 є первісним коренем n-го степеня з 1. □

Із твердження 7 випливає, що кількість первісних коренів степеня n з 1 збігається з кількістю тих натуральних чисел, які менші за n і взаємно прості з n. Ця кількість позначається через $\varphi(n)$ і називається *функцією Ойлера* числа n. З означення одразу випливає, що для кожного простого числа p $\varphi(p) = p - 1$. Не набагато складніше обчислюються значення функції Ойлера для степенів простих чисел:

Лема 2. *Якщо p – просте число і $k > 0$, то* $\varphi(p^k) = (p-1)p^{k-1}$.

Доведення. Число m є взаємно простим із p^k тоді й лише тоді, коли m не ділиться на p. У проміжку від 1 до p^k на p ділиться кожне p-те число, тобто всього $\dfrac{p^k}{p} = p^{k-1}$ чисел. Решта $p^k - p^{k-1}$ чисел із цього проміжку на p не діляться, а тому є взаємно простими з p^k. Отже,

$$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}.$$

□

Теорема 5. *Функція Ойлера мультиплікативна, тобто для довільних взаємно простих чисел n і m виконується рівність* $\varphi(nm) = \varphi(n)\varphi(n)$.

Доведення. Позначимо множини $\{0, 1, 2, \ldots, n-1\}$, $\{0, 1, 2, \ldots, m-1\}$ і $\{0, 1, 2, \ldots, nm-1\}$ відповідно через A, B і C. Кожному числу c із множини C зіставимо пару $(r_1(c), r_2(c))$, де $r_1(c)$ і $r_2(c)$ є остачами від ділення c на n і m відповідно. Відображення

$$C \to A \times B, \quad c \mapsto (r_1(c), r_2(c)),$$

є бієктивним. Справді, ін'єктивність випливає з того, що коли $f(c_1) = f(c_2) = (r_1, r_2)$, то $c_2 - c_1$ ділиться і на n, і на m. Оскільки n і m – взаємно прості, то $c_2 - c_1$ ділиться на nm. Але c_1 і c_2 належать проміжку $[0, nm-1]$, тому $|c_2 - c_1| < nm$. Отже, $c_2 - c_1 = 0$ і $c_2 = c_1$. Сюр'єктивність тепер випливає з того, що множини A і $B \times C$ мають однакову кількість елементів, а саме nm.

Число c буде взаємно простим із добутком nm тоді й лише тоді, коли воно буде взаємно простим із кожним із множників, тобто тоді й лише тоді, коли остачі $r_1(c)$ і $r_2(c)$ взаємно прості відповідно з n і m. Але тоді

з бієктивності відображення $A \to B \times C$ випливає, що кількість $\varphi(nm)$ таких чисел дорівнює кількості пар (r_1, r_2), в яких перша компонента r_1 взаємно проста з n, а друга компонента r_2 – взаємно проста з m. За комбінаторним правилом множення кількість таких пар дорівнює $\varphi(n)\varphi(n)$. □

Наслідок 4. *Якщо $n = p_1^{k_1} \cdots p_m^{k_m}$ – канонічний розклад числа n, то*

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_m^{k_m} - p_m^{k_m-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Доведення. Оскільки множники $p_1^{k_1}, \ldots, p_m^{k_m}$ попарно взаємно прості, то, використовуючи послідовно теорему 5 і лему 2, отримуємо

$$\varphi(n) = \varphi(p_1^{k_1} \cdots p_m^{k_m}) = \varphi(p_1^{k_1}) \cdots \varphi(p_m^{k_m}) =$$
$$= (p_1 - 1)p_1^{k_1-1} \cdots (p_m - 1)p_m^{k_m-1} = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right). \qquad \square$$

1.7. Показникова форма запису

У курсі математичного аналізу доводиться, що $\lim\limits_{n\to\infty}\left(1 + \dfrac{x}{n}\right)^n = e^x$. Спираючись на це, для довільного комплексного числа $z = a + bi$ покладемо

$$e^z := e^a \cdot e^{bi}, \quad \text{де} \quad e^{bi} = \lim_{n\to\infty}\left(1 + \frac{bi}{n}\right)^n.$$

Для модуля числа $\left(1 + \frac{bi}{n}\right)^n$ маємо

$$\left|\left(1 + \frac{bi}{n}\right)^n\right| = \left(1 + \frac{b^2}{n^2}\right)^{n/2} = \left(1 + \frac{b^2}{n^2}\right)^{n^2\cdot(1/2n)}.$$

Оскільки $\left(1 + \dfrac{b^2}{n^2}\right)^{n^2} \to e^{\,b^2}$ і $\dfrac{1}{2n} \to 0$, то $\left|\left(1 + \dfrac{bi}{n}\right)^n\right| \to 1$.

Із рис. 6 видно, що для достатньо великих n для аргументу φ_n числа $\left(1 + \dfrac{bi}{n}\right)^n$ маємо

$$\varphi_n = n\psi = n \arcsin \frac{b/n}{\sqrt{1 + b^2/n^2}}.$$

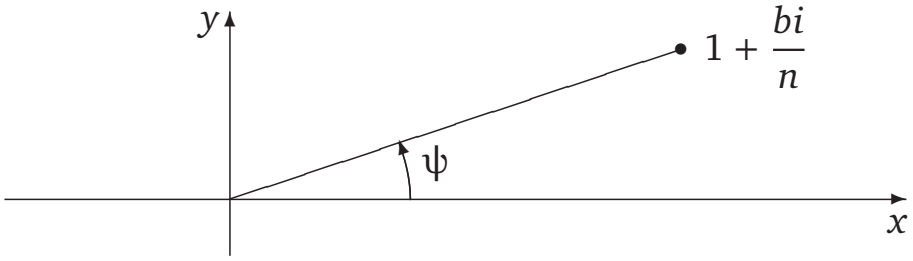


Рис. 6

Позначимо $A_n = \dfrac{b/n}{\sqrt{1 + b^2/n^2}}$. Тоді

$$\varphi_n = n \arcsin A_n = nA_n \cdot \frac{\arcsin A_n}{A_n} = nA_n \cdot \frac{\arcsin A_n}{\sin(\arcsin A_n)} .$$

Легко бачити, що $A_n \to 0$, $nA_n \to b$, $\arcsin A_n \to 0$ і $\dfrac{\arcsin A_n}{\sin(\arcsin A_n)} \to 1$. Тому $\varphi_n \to b$ і

$$\left(1 + \frac{bi}{n}\right)^n \to \cos b + i \sin b .$$

Отже,

$$e^{ib} = \cos b + i \sin b .$$

Таким чином, $e^{a+bi} = e^a(\cos b + i \sin b)$. За такої домовленості тригонометрична форма числа $z = |z| \cdot (\cos \arg z + i \sin \arg z)$ може бути переписана у вигляді

$$z = |z| \cdot e^{i \arg z} . \tag{1.23}$$

Запис комплексного числа у вигляді (1.23) називається *показниковою формою* запису.

Зокрема, при $z = -1$ одержуємо одну з найфантастичніших формул математики:

$$-1 = e^{i\pi} . \tag{1.24}$$

Зауваження. Із показникової форми (1.23) безпосередньо випливають відомі нам правила (1.11) поведінки модулів і аргументів комплексних чисел при множенні.

1.8. Задачі

1.1.°* [4] На множині $\mathbb{N}\times\mathbb{N}$ визначимо відношення еквівалентності

$$(m,n)\sim(p,q) \quad \text{тоді й лише тоді, коли} \quad m+q=n+p\,,$$

а на фактор-множині $(\mathbb{N}\times\mathbb{N})/\!\sim$ – дії

$$\overline{(m,n)}+\overline{(p,q)}:=\overline{(m+p,n+q)}\,;$$
$$\overline{(m,n)}\cdot\overline{(p,q)}:=\overline{(mp+nq,mq+np)}\,.$$

Доведіть, що

а) дії на фактор-множині $(\mathbb{N}\times\mathbb{N})/\!\sim$ визначені коректно;

б) кожен клас еквівалентності містить пару вигляду $(m,1)$, причому тільки одну;

в) після ототожнення класу $\overline{(n+1,1)}$ із цілим числом n фактор-множина $(\mathbb{N}\times\mathbb{N})/\!\sim$ перетворюється в кільце цілих чисел зі звичайними додаванням і множенням.

1.2. Інколи числове поле визначають як множину чисел, замкнену відносно чотирьох арифметичних дій – додавання, віднімання, множення та ділення (крім ділення на 0). Доведіть, що це означення рівносильне нашому означенню 2.

1.3. Не використовуючи тригонометричну форму числа, доведіть, що з кожного ненульового комплексного числа існує рівно два корені степеня 2.

1.4.° Доведіть, що коли числа m і n – взаємно прості і $z^m=z^n=1$, то $z=1$.

1.5. Доведіть, що $\mathbb{C}_n\cap\mathbb{C}_m=\mathbb{C}_d$, де d – це найбільший спільний дільник чисел m і n.

1.6. Доведіть, що коли числа m і n – взаємно прості, то кожен корінь ε степеня mn з 1 однозначно розкладається в добуток $\varepsilon=\mu\cdot\nu$ коренів з 1 степенів m і n відповідно.

[4] Символом * позначено задачі підвищеного рівня складності. Символом ° – ті, що вимагають додаткових знань.

1.7. Нехай числа m і n – взаємно прості. Доведіть, що ε буде первісним коренем степеня mn з 1 тоді й лише тоді, коли ε розкладається в добуток $\varepsilon = \mu \cdot \nu$ первісного кореня степеня m і первісного кореня степеня n.

1.8. Чи може сума двох первісних коренів степеня n з 1 також бути первісним коренем степеня n з 1?

1.9.* Доведіть, що рівність $(2+i)^n = (2-i)^n$ не виконується для жодного натурального числа n.

1.10. Доведіть, що функція Жуковського $u = \dfrac{1}{2}\left(z + \dfrac{1}{z}\right)$ відображає:

а) коло $|z| = 1$ на відрізок $[-1, 1]$ дійсної осі;

б)° коло $|z| = r$, $r \neq 1$, на еліпс із фокусами $-1, 1$;

в)° промінь $\arg z = \varphi$ на гілку гіперболи із фокусами $-1, 1$.

1.11. *Подвійним відношенням* $[z_1, z_2, z_3, z_4]$ чотирьох комплексних чисел z_1, z_2, z_3, z_4, $z_1 \neq z_4$, $z_2 \neq z_3$, називається число

$$[z_1, z_2, z_3, z_4] = \frac{z_1 - z_2}{z_1 - z_4} : \frac{z_3 - z_2}{z_3 - z_4}.$$

Доведіть, що

а) $[z_2, z_3, z_4, z_1] = [z_1, z_2, z_3, z_4]^{-1}$;

б) при зсуві $T_a : z \mapsto z + a$, де число a — фіксоване, подвійне відношення $[z_1, z_2, z_3, z_4]$ не змінюється.

1.12.* Доведіть, що, коли точки z_1, z_2, z_3, z_4 не лежать на одній прямій, то вони лежать на одному колі тоді й лише тоді, коли їх подвійне відношення $\dfrac{z_1 - z_2}{z_1 - z_4} : \dfrac{z_3 - z_2}{z_3 - z_4}$ є дійсним числом.

1.13.** Доведіть, що для довільних двох наборів $z_1, \ldots, z_n$ і $u_1, \ldots, u_n$ комплексних чисел виконується нерівність

$$\left| \sum_{k=1}^{n} z_k u_k \right|^2 \leq \sum_{k=1}^{n} |z_k|^2 \cdot \sum_{k=1}^{n} |u_k|^2.$$

1.14.* Знайдіть вигляд загального члена послідовності $(a_n)_{n \geq 0}$, якщо $a_0 = a_1 = 1$ і $a_{n+1} = 2a_n - 2a_{n-1}$ для всіх $n \geq 1$.

1.15.* а) На площині лежать 4 механічні годинники (тобто зі стрілками). Діаметри й орієнтація годинників можуть бути довільними, але відомо, що всі вони йдуть правильно, їх центри утворюють квадрат і в певний момент кінці хвилинних стрілок також утворювали квадрат. Доведіть, що кінці хвилинних стрілок завжди будуть утворювати квадрат.

б) Узагальніть попереднє твердження на n годинників.

1.16.°* Бієктивне перетворення $\varphi : \mathbb{C} \to \mathbb{C}$ називається *автоморфізмом* поля $\mathbb{C}$, якщо для довільних z_1 і z_2 виконуються рівності $\varphi(z_1 + z_1) = \varphi(z_1) + \varphi(z_2)$ і $\varphi(z_1 \cdot z_1) = \varphi(z_1) \cdot \varphi(z_2)$. Доведіть, що єдиним нетривіальним (тобто відмінним від тотожного перетворення) неперервним автоморфізмом поля $\mathbb{C}$ є спряження.

1.17. Сформулюйте й доведіть аналог рівності 1.19 для чотирьох квадратів.

2. Системи лінійних рівнянь

2.1. Типи систем лінійних рівнянь. Алгоритм Гаусса

У загальному випадку *система лінійних рівнянь* (СЛР) має вигляд

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & = & b_1\,, \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & = & b_2\,, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & = & b_m\,, \end{array} \tag{2.1}$$

де $x_1, x_2, \dots, x_n$ – це невідомі, а символи a_{ij} позначають коефіцієнти при невідомих[5]. Використання для позначення коефіцієнтів двох індексів є дуже зручним: перший індекс i вказує на номер рівняння, а другий індекс j – на номер невідомої. Зауважимо, що число n невідомих може відрізнятися від числа m рівнянь.

Використовуючи символ Σ, систему (2.1) можна записати компактніше

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \quad (i = 1, \dots, n)\,. \tag{2.2}$$

Розв'язування систем лінійних рівнянь є центральною задачею лінійної алгебри. Необхідність у розв'язуванні таких систем виникає як у багатьох розділах математики (із деякими прикладами ми зустрінемося уже незабаром: інтерполяція функцій многочленами, розклад раціональних функцій у суму найпростіших дробів, зображення симетричних многочленів у вигляді многочленів від елементарних симетричних многочленів тощо), так і в найрізноманітніших її застосуваннях.

Для ілюстрації останнього твердження розглянемо так звану *задачу про міжгалузевий баланс*. Є n галузей виробництва, кожна з яких випускає власну продукцію. Кількість продукції, що випускається i-ю галуззю, позначимо x_i. При виробництві i-ї продукції може використовуватися продукція інших галузей. Нехай при виробництві одиниці i-ї продукції використовується a_{ij} одиниць продукції продукції j-ї галузі. Тоді чистий випуск i-ї продукції становитиме $x_i - \sum\limits_{j=1}^{n} a_{ij}x_j$ одиниць. Скільки продукції повинна випустити кожна з галузей, якщо остаточно споживачі повинні

[5] Символ a_{23} читається "a два-три", а не "a двадцять три". У тих випадках, коли виникає неоднозначність, між індексами i та j ставлять кому, наприклад, $a_{1,23}$ або $a_{12,3}$.

отримати b_i $(i = 1, 2, \ldots, n)$ одиниць i-ї продукції? Зрозуміло, що задача зводиться до розв'язання системи лінійних рівнянь

$$x_i - \sum_{j=1}^{n} a_{ij} x_j \quad (i = 1, \ldots, n).$$

Ще в кінці XIX ст. теорія систем лінійних рівнянь стала взірцем для створення теорії інтегральних рівнянь, яка відіграє величезну роль у фізиці та механіці. Розроблені для дослідження систем лінійних рівнянь методи стали однією з основ сучасної математики. Наприклад, завдяки проникненню методів лінійної алгебри у класичний математичний аналіз в середині XX ст. виникла нова потужна область математики – функціональний аналіз. Розв'язування за допомогою комп'ютерів величезної кількості практичних задач також стає можливим лише завдяки зведенню цих задач до систем лінійних рівнянь.

Коефіцієнт b_i системи (2.1) називається *вільним членом* (i-го рівняння). Якщо всі вільні члени системи дорівнюють нулю, то така СЛР називається *однорідною* (коротко ОСЛР). У противному разі СЛР називається *неоднорідною*.

Інколи буває корисно паралельно із СЛР (2.2) розглядати так звану *пов'язану* (або *асоційовану*) із нею однорідну СЛР. Це ОСЛР

$$\sum_{j=1}^{n} a_{ij} x_j = 0 \quad (i = 1, \ldots, n), \tag{2.3}$$

яка має такі самі коефіцієнти при невідомих.

Можна досягти значної економії часу і зусиль, якщо в записі СЛР повністю відмовитися від виписування невідомих, а писати лише коефіцієнти при них. Щоб уникнути плутанини, коефіцієнти повинні виписуватися у певному порядку. Зручно їх виписувати у вигляді прямокутної таблиці

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} \end{pmatrix}, \tag{2.4}$$

яка називається *матрицею коефіцієнтів* (коротко: *матрицею* або *основною матрицею*) СЛР (2.1)[6].

Кажуть, що матриця (2.4) має розміри $m \times n$. Коротко цю матрицю позначають $(a_{ij})_{m\times n}$ або просто (a_{ij}). Поруч із круглими дужками для запису матриць можуть уживатися подвійні прямі $||a_{ij}||$ і прямокутні $[a_{ij}]$ дужки.

Матрицю розміру $n \times n$ часто називають *квадратною* матрицею *порядку* n. Набір $(a_{i1}, a_{i2}, \ldots, a_{in})$ називають i-м *рядком*, а набір

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \ldots \\ a_{mj} \end{pmatrix}$$

– j-м *стовпцем* матриці (2.1). Таким чином, індекси i та j елемента a_{ij} вказують номери рядка і стовпця, на перетині яких стоїть цей елемент.

Сукупність елементів a_{11}, a_{22}, a_{33}, ... з однаковими індексами утворює так звану *головну діагональ* матриці. У випадку квадратної матриці ці елементи справді лежать на діагоналі квадрата. У квадратній матриці порядку n виділяють також *побічну діагональ* $a_{1n}, a_{2,n-1}, \ldots, a_{n1}$.

Виділимо кілька спеціальних типів матриць, які часто зустрічатимуться в подальшому.

Квадратна матриця називається *верхньою* (відповідно *нижньою*) *трикутною*, якщо для всіх $i > j$ (відповідно для всіх $i < j$) виконується рівність $a_{ij} = 0$. Верхня трикутна матриця є частковим випадком так званої *трапецієподібної* матриці, яка вже не обов'язково квадратна і має вигляд

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1k} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2k} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_{kk} & \ldots & a_{kn} \\ 0 & 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}.$$

[6] Матриці (і дії над ними, які ми будемо розглядати трохи пізніше) увів видатний англійський математик А. Келі (1821–1895).

Трапецієподібна матриця вигляду

$$\begin{pmatrix} 1 & 0 & \dots & 0 & a_{1,k+1} & \dots & a_{1n} \\ 0 & 1 & \dots & 0 & a_{2,k+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & a_{k,k+1} & \dots & a_{kn} \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

називається *спеціальною трапецієподібною*.

Квадратна матриця, в якій всі елементи поза головною діагоналлю дорівнюють нулю, називається *діагональною*. Діагональну матрицю порядку n часто записують у вигляді $\operatorname{diag}(a_{11}, a_{22}, \dots, a_{nn})$. Діагональна матриця називається *скалярною*, якщо всі її діагональні елементи однакові. Скалярна матриця, в якої на діагоналі стоять одиниці, називається *одиничною* і позначається символом E (або E_n, якщо хочуть вказати її порядок).

Матриця, усі елементи якої дорівнюють нулю, називається *нульовою*. Її позначають символом $\mathbf{0}_{m\times n}$, або $\mathbf{0}_n$ (для квадратної матриці порядку n), або просто $\mathbf{0}$.

Прямокутні матриці зустрічаються в математиці настільки часто, що в середині XIX ст. виникла, а із часом розвинулась у велику самостійну область математики, *теорію матриць*. У XX ст. теорія матриць стала складовою частиною лінійної алгебри і донині зберігає своє значення дуже потужного інструменту, однаково придатного і для розв'язання різноманітних задач, що виникають із потреб практики, і для дослідження абстрактних конструкцій сучасної математики.

Поруч із матрицею (2.4) для системи (2.1) розглядають і *розширену матрицю*

$$\left(\begin{array}{ccccc|c} a_{11} & a_{12} & a_{13} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} & b_m \end{array}\right), \tag{2.5}$$

яка одержується із (2.4) приєднанням стовпця вільних членів (щоб не сплутати вільні члени з коефіцієнтами при невідомих, стовпець вільних членів відділяють вертикальною рискою).

Коротко основну і розширену матриці системи (2.1) позначають (a_{ij}) і $(a_{ij}|b_i)$ відповідно.

За формою основної матриці СЛР (2.1) називається *прямокутною* (якщо $m \neq n$) або *квадратною* (якщо $m = n$). У випадку трикутної основної матриці СЛР також називають *трикутною*.

Надалі будемо вважати, що всі коефіцієнти СЛР (2.1) є елементами деякого поля P. *Розв'язком* цієї системи у полі P називається такий набір $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ із n елементів $a_1, a_2, \ldots, a_n$ поля P, що після підстановки в систему (2.1) цих елементів відповідно замість невідомих $x_1, x_2, \ldots, x_n$ отримаємо правильні рівності. Елементи $a_1, a_2, \ldots, a_n$ називаються *компонентами* або *координатами* розв'язку $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$[7].

Підкреслюємо, що розв'язком системи є саме набір $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$, а не його компоненти $a_1, a_2, \ldots, a_n$.

Якщо СЛР (2.1) має хоча б один розв'язок, вона називається *сумісною*. У протилежному разі СЛР називається *несумісною*. Сумісна СЛР, яка має рівно один розв'язок, називається *визначеною*. Якщо ж сумісна СЛР має більше одного розв'язку, то вона називається *невизначеною*. Таким чином, СЛР поділяються на три типи залежно від кількості розв'язків.

Зауважимо, що однорідна СЛР завжди є сумісною, бо завжди має так званий *тривіальний* або *нульовий* розв'язок $\mathbf{0} = (0, 0, \ldots, 0)$.

Проблему розв'язання СЛР можна розбити на дві частини: *якісну* – визначення типу СЛР, і *кількісну* – знаходження множини розв'язків сумісної СЛР . Довкола цих двох проблем в основному йтиме подальший виклад.

Дві СЛР з одними і тими ж невідомими називаються *рівносильними* або *еквівалентними*, якщо вони мають однакові множини розв'язків. Зокрема, рівносильними будуть будь-які дві несумісні системи з однаковими невідомими.

Вправа 6. *Доведіть, що на множині всіх СЛР відношення рівносильності є відношенням еквівалентності.*

Елементарними перетвореннями СЛР називаються такі її перетворення:

1) перестановку двох рівнянь системи;

2) множення одного з рівнянь системи на число $\lambda \neq 0$;

3) додавання до одного з рівнянь системи іншого її рівняння, помноженого на деяке число λ.

Зауважимо, що елементарні перетворення є оборотними: якщо при елементарному перетворенні СЛР S_1 переходить в S_2, то за допомогою

[7] Інколи розглядають загальнішу ситуацію, коли всі коефіцієнти СЛР(2.1) належать деякому кільцю (наприклад, кільцю цілих чисел $\mathbb{Z}$), і вимагають, щоб компоненти розв'язку також належали цьому кільцю.

елементарного перетворення СЛР S_2 можна повернутися назад до S_1. Справді, якщо S_2 одержана з S_1 перестановкою двох рівнянь, то, переставивши ці рівняння ще раз, повернемося до S_1. Якщо S_2 одержується із S_1 множенням якогось рівняння на $\lambda \neq 0$, то, помноживши отримане рівняння на λ^{-1}, повертаємося до S_1. Нарешті, якщо S_2 одержується із S_1 додаванням до i-го рівняння її j-го рівняння, помноженого на λ, то для повернення назад досить до i-го рівняння системи S_2 додати її j-те рівняння, помножене на $-\lambda$.

Теорема 6. *Якщо від однієї СРЛ до іншої можна перейти за допомогою скінченної кількості елементарних перетворень, то такі дві СЛР є рівносильними.*

Доведення. Досить показати, що при одному елементарному перетворенні СЛР переходить у рівносильну. Більше того, оскільки елементарні перетворення є оборотними, то досить показати, що при елементарному перетворенні СЛР множина її розв'язків не зменшується.

Для елементарних перетворень перших двох типів це очевидно. Розглянемо перетворення третього типу. Нехай $\boldsymbol{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ — розв'язок системи (2.1) і нехай до її i-го рівняння додали j-те рівняння, помножене на число λ. Тоді

$$a_{i1}\alpha_1 + a_{i2}\alpha_2 + \ldots + a_{in}\alpha_n = b_i \quad \text{і} \quad a_{j1}\alpha_1 + a_{j2}\alpha_2 + \ldots + a_{jn}\alpha_n = b_j.$$

Нова система відрізняється від (2.1) лише i-м рівнянням, яке має вигляд

$$(a_{i1} + \lambda a_{j1})x_1 + (a_{i2} + \lambda a_{j2})x_2 + \ldots + (a_{in} + \lambda a_{jn})x_n = b_i + \lambda b_j.$$

Легко перевіряється, що $\boldsymbol{a}$ є розв'язком і цього рівняння. Справді,

$$(a_{i1} + \lambda a_{j1})\alpha_1 + (a_{i2} + \lambda a_{j2})\alpha_2 + \ldots + (a_{in} + \lambda a_{jn})\alpha_n =$$
$$= (a_{i1}\alpha_1 + a_{i2}\alpha_2 + \ldots + a_{in}\alpha_n) + \lambda(a_{j1}\alpha_1 + a_{j2}\alpha_2 + \ldots + a_{jn}\alpha_n) = b_i + \lambda b_j.$$

Отже, усі розв'язки системи (2.1) є розв'язками нової системи. □

Очевидно, що перетворенням рівнянь СЛР відповідають перетворення рядків її матриці. *Елементарними перетвореннями* рядків (стовпців) матриці (2.4) називаються такі її перетворення:

1) перестановка двох рядків (стовпців) матриці;

2) множення одного з рядків (стовців) матриці на число $\lambda \neq 0$;

3) додавання до одного з рядків (стовців) матриці іншого її рядка (стовпця), помноженого на деяке число λ.

Якщо матриця B отримана з матриці A за допомогою скінченного ланцюга елементарних перетворень рядків, то такі матриці називатимемо *еквівалентними* і записуватимемо як $A \sim B$.

Зауважимо, що елементарним перетворенням рівнянь СЛР відповідають такі ж елементарні перетворення відповідних рядків розширеної матриці цієї СЛР і навпаки. Тому маємо таке твердження.

Твердження 8. *Якщо розширені матриці двох СЛР еквівалентні, то відповідні СЛР будуть рівносильними.*

Теорема 7 (алгоритм Гаусса)**.** *Елементарними перетвореннями рядків та перестановками стовпців довільну ненульову матрицю A розміру $m \times n$ можна звести до спеціального трапецієподібного вигляду*

$$\begin{pmatrix} 1 & 0 & \dots & 0 & f_{1,r+1} & \dots & f_{1n} \\ 0 & 1 & \dots & 0 & f_{2,r+1} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & f_{r,r+1} & \dots & f_{rn} \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}, \tag{2.6}$$

де $0 < r \leq \min(m, n)$.

Доведення. Опишемо алгоритм зведення довільної ненульової матриці $A = (a_{ij})$ розміру $m \times n$ до вигляду (2.6).

Оскільки $A \neq \mathbf{0}$, то перестановкою стовпців і рядків з матриці A можна отримати матрицю $\tilde{A} = (\tilde{a}_{ij})$, в якій $\tilde{a}_{11} \neq 0$. Поділимо перший рядок матриці $\tilde{A}$ на $\tilde{a}_{11}$, а потім для кожного $l = 2, 3, \dots, m$ від l-го рядка віднімемо утворений перший рядок, помножений на $\tilde{a}_{l1}$. Одержимо матрицю

$$B = \begin{pmatrix} 1 & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix}. \tag{2.7}$$

Якщо матриця B містить ненульові елементи лише в першому рядку, то вона вже є спеціальною трапецієподібною. У противному разі серед елементів b_{ij}, де $i, j \geq 2$, є ненульовий. Перестановкою стовпців (відмінних від першого) і рядків (відмінних від першого) із матриці B можна

отримати матрицю

$$\tilde{B} = \begin{pmatrix} 1 & \tilde{b}_{12} & \dots & \tilde{b}_{1n} \\ 0 & \tilde{b}_{22} & \dots & \tilde{b}_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \tilde{b}_{m2} & \dots & \tilde{b}_{mn} \end{pmatrix},$$

в якій $\tilde{b}_{22} \neq 0$. Поділимо тепер уже другий рядок матриці $\tilde{B}$ на $\tilde{b}_{22}$, а потім для кожного $l = 3, \dots, m$ від l-го рядка віднімемо утворений другий рядок, помножений на $\tilde{b}_{l2}$. Одержимо матрицю

$$C = \begin{pmatrix} 1 & c_{12} & c_{13} & \dots & c_{1n} \\ 0 & 1 & c_{23} & \dots & c_{2n} \\ 0 & 0 & c_{33} & \dots & c_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & c_{3m} & \dots & c_{mn} \end{pmatrix}. \tag{2.8}$$

Якщо серед елементів c_{ij}, де $i, j \geq 3$, є ненульові, то продовжуємо аналогічні перетворення далі (тільки вже працюємо з рядками і стовпцями з номерами ≥ 3). І так далі. Зрештою, прийдемо до матриці вигляду

$$D = \begin{pmatrix} 1 & d_{12} & \dots & d_{1,r-1} & d_{1r} & d_{1,r+1} & \dots & d_{1n} \\ 0 & 1 & \dots & d_{2,r-1} & d_{2r} & d_{2,r+1} & \dots & d_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & d_{r-1,r} & d_{r-1,r+1} & \dots & d_{r-1,n} \\ 0 & 0 & \dots & 0 & 1 & d_{r,r+1} & \dots & d_{rn} \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}. \tag{2.9}$$

Тепер починаємо робити нулі над діагоналлю. Спочатку робимо нулі в r-му стовпці. Для цього для кожного $l = 1, \dots, r-1$ від l-го рядка матриці D віднімемо її r-й рядок, помножений на число d_{lr}. Отримуємо матрицю

$$D' = \begin{pmatrix} 1 & d_{12} & \dots & d_{1,r-1} & 0 & d'_{1,r+1} & \dots & d'_{1n} \\ 0 & 1 & \dots & d_{2,r-1} & 0 & d'_{2,r+1} & \dots & d'_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & d'_{r-1,r+1} & \dots & d'_{r-1,n} \\ 0 & 0 & \dots & 0 & 1 & d_{r,r+1} & \dots & d_{rn} \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Далі робимо нулі над діагоналлю в $(r-1)$-му стовпці. Для цього для кожного $l = 1, \ldots, r-2$ від l-го рядка матриці D' віднімаємо її $(r-1)$-й рядок, помножений на $d_{l,r-1}$. І так далі. Зрештою, отримаємо матрицю

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & f_{1,r+1} & \ldots & f_{1n} \\ 0 & 1 & \ldots & 0 & 0 & f_{2,r+1} & \ldots & f_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & f_{r-1,r+1} & \ldots & f_{r-1,n} \\ 0 & 0 & \ldots & 0 & 1 & f_{r,r+1} & \ldots & f_{rn} \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}, \tag{2.10}$$

яка вже має спеціальний трапецієподібний вигляд. □

Описана в доведенні теореми 7 послідовність дій при переході від початкової матриці A до матриці (2.9) називається *прямим ходом алгоритму Гаусса*, а послідовність дій при переході від (2.9) до (2.10) — *зворотним ходом алгоритму Гаусса*. Процес зведення матриці A до спеціального трапецієподібного вигляду називається *алгоритмом Гаусса*.

Зауважимо, що в цьому алгоритмі над коефіцієнтами матриці виконуються лише раціональні операції – додавання, віднімання, множення, ділення. Тому його можна застосовувати до матриць із коефіцієнтами з довільного поля. При цьому в процесі обчислень ми завжди лишатимемося у тому полі, якому належать коефіцієнти системи.

2.2. Метод Гаусса розв'язування СЛР

Дві системи S_1 і S_2 лінійних рівнянь називатимемо *квазірівносильними*, якщо в одній із них можна перейменувати змінні так, щоб отримати рівносильні СЛР. Зокрема, якщо система S_2 одержується із S_1 перенумерацією змінних, то основна матриця системи S_2 одержується з відповідної матриці для S_1 перестановкою стовпців.

Уже зі шкільного досвіду відомо, що основним шляхом розв'язування рівнянь і систем рівнянь є їх зведення за допомогою певних перетворень (бажано, рівносильних) до такого вигляду, коли відсутність чи наявність розв'язків, а також самі розв'язки (якщо вони є) видно безпосередньо. У випадку систем лінійних рівнянь послідовність таких перетворень відбувається за єдиною схемою, яка називається *методом Гаусса*.

Змістовно цей метод полягає в послідовному виключенні із системи невідомих, тобто в послідовному переході до систем із меншою кількістю

невідомих. Звідси друга його назва – *метод послідвного виключення невідомих*[8].

Ідею цього методу легко зрозуміти з наступних прикладів. Нагадаємо, що елементарним перетворенням рівнянь (при яких система переходить у рівносильну) відповідають елементарні перетворення рядків її матриці.

Приклад 1. Розглянемо систему

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & 3x_3 & = & 6, \\ 4x_1 & + & 5x_2 & + & 6x_3 & = & 15, \\ 7x_1 & + & 8x_2 & + & 9x_3 & = & 25 \end{array} \tag{2.11}$$

з основною матрицею

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 4 & 5 & 6 & 15 \\ 7 & 8 & 9 & 25 \end{array}\right). \tag{2.12}$$

Спочатку віднімемо від другого і третього рядків перший, помножений відповідно на 4 і 7. Отримаємо

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 0 & -3 & -6 & -9 \\ 0 & -6 & -12 & -17 \end{array}\right).$$

Тепер від третього рядка віднімемо подвоєний другий. Отримаємо

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 0 & -3 & -6 & -9 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Таким чином, третє рівняння системи набуло вигляду $0\cdot x_1 + 0\cdot x_2 + 0\cdot tx_3 = 1$. Оскільки воно не має розв'язків, то дана СЛР є несумісною.

Приклад 2. Розглянемо тепер систему

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & 3x_3 & = & 6, \\ 4x_1 & + & 5x_2 & + & 6x_3 & = & 15, \\ 7x_1 & + & 8x_2 & + & 10x_3 & = & 25 \end{array} \tag{2.13}$$

[8] Гаусс є одним із найбільших математичних геніїв, однак зовсім не тому, що він придумав метод виключення. До речі, цей метод був відомий і до нього. Гаусс лише надав йому чіткішої форми. Та за іронією долі серед усіх пов'язаних з іменем Гаусса ідей найчастіше згадується саме метод виключення.

з основною матрицею

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 4 & 5 & 6 & 15 \\ 7 & 8 & 10 & 25 \end{array}\right). \tag{2.14}$$

Якщо із цією матрицею виконати такі ж перетворення, як у попередньому прикладі, то отримаємо матрицю

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 0 & -3 & -6 & -9 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Продовжимо перетворення рядків далі. Спочатку поділимо другий рядок на -3, а потім віднімемо від першого і другого рядків третій, помножений відповідно на 3 і 2. Отримаємо

$$\left(\begin{array}{ccc|c} 1 & 2 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Нарешті віднімемо від першого рядка подвоєний другий:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Таким чином, система набула вигляду

$$\begin{aligned} x_1 &= 1, \\ x_2 &= 1, \\ x_3 &= 1. \end{aligned}$$

Отже, дана СЛР є визначеною, а її єдиним розв'язком є набір $(1, 1, 1)$.

Приклад 3. Розглянемо ще систему

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 6, \\ 4x_1 + 5x_2 + 6x_3 &= 15, \\ 7x_1 + 8x_2 + 9x_3 &= 24 \end{aligned} \tag{2.15}$$

з основною матрицею

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 4 & 5 & 6 & 15 \\ 7 & 8 & 9 & 24 \end{array}\right). \tag{2.16}$$

Якщо із цією матрицею виконати такі ж перетворення, як у першому прикладі, то отримаємо матрицю

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 0 & -3 & -6 & -9 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Перетворення рядків можна продовжити далі: поділимо другий рядок на -3, а потім віднімемо від першого рядка подвоєний другий. Отримаємо

$$\left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Таким чином, система набула вигляду

$$\begin{array}{rcrcl} x_1 & - & x_3 & = & 0, \\ x_2 & + & 2x_3 & = & 3, \\ & & 0 & = & 0. \end{array}$$

Виключимо останнє рівняння, яке є тотожно істинним, і перенесемо члени з x_3 у праву частину:

$$\begin{array}{rcl} x_1 & = & x_3, \\ x_2 & = & 3 - 2x_3. \end{array}$$

Таким чином, невідомій x_3 можна надавати довільного значення t, після чого x_1 і x_2 визначаються однозначно: $x_1 = t$, $x_2 = 3 - t$. Отже, дана СЛР є невизначеною, а множина її розв'язків має вигляд $\{(t, 3-2t, t) \mid t \in \mathbb{R}\}$.

Із цих прикладів видно, що в основі методу послідовного виключення невідомих лежить описаний в теоремі 7 алгоритм Гаусса зведення матриці до спеціального трапецієподібного вигляду.

Розглянемо детальніше, що означає цей алгоритм для СЛР. Якщо всі коефіцієнти a_{ij} основної матриці СЛР (2.1) є нулями, то кожне з рівнянь системи має вигляд $0 = b_i$. Якщо серед вільних членів b_i є хоча б один ненульовий, то СЛР є, очевидно, несумісною. Якщо ж усі b_i дорівнюють нулю, то будь-який вектор $x = (x_1, x_2, \ldots, x_n)$ буде розв'язком і СЛР є невизначеною. Тому далі вважаємо, що серед коефіцієнтів основної матриці є ненульові. Перейменувавши, за потреби, змінні й переставивши рівняння, можна вважати, що саме $a_{11} \neq 0$. Поділимо перше рівняння на a_{11}, а потім для кожного k $(k = 2, 3, \ldots, m)$ від k-го рівняння віднімемо

перше, помножене на a_{k1}. У результаті ми з усіх рівнянь системи, крім першого, виключимо x_1 і одержимо СЛР

$$\begin{array}{rcccccccc} x_1 & + & b_{12}x_2 & + & \dots & + & b_{1n}x_n & = & b'_1, \\ & & b_{22}x_2 & + & \dots & + & b_{2n}x_n & = & b'_2, \\ & & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & b_{m2}x_2 & + & \dots & + & b_{mn}x_n & = & b'_m, \end{array} \tag{2.17}$$

яка рівносильна (квазірівносильна, якщо змінні перейменовувалися) початковій системі. Зауважимо, що основною матрицею цієї системи є матриця (2.7).

Останні $m-1$ рівнянь цієї системи утворюють СЛР , яка містить уже на одну невідому менше – лише $x_2, x_3, \dots, x_n$. Із цих рівнянь, використовуючи аналогічні перетворення, можна виключити ще одну невідому. І так далі. На кожному кроці методу Гаусса ми будемо виключати чергову невідому (у разі потреби перенумерувавши невідомі). Тому на k-му кроці із системи виключається x_k.

Як довго можна виключати невідомі? Наступний крок не можна виконати тільки в двох випадках: або вже не залишилось рівнянь, або в рівняннях, що залишились, усі коефіцієнти при невідомих дорівнюють 0. Якщо таке трапилося після r кроків, то одержана система буде мати вигляд

$$\begin{array}{rcccccccccc} x_1 & + & d_{12}x_2 & + \dots + & d_{1r}x_r & + & d_{1,r+1}x_{r+1} & + \dots + & d_{1n}x_n & = & b''_1, \\ & & x_2 & + \dots + & d_{2r}x_r & + & d_{2,r+1}x_{r+1} & + \dots + & d_{2n}x_n & = & b''_2, \\ & & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & & x_r & + & d_{r,r+1}x_{r+1} & + \dots + & d_{rn}x_n & = & b''_r, \\ & & & & & & & & 0 & = & b''_{r+1}, \\ & & & & & & & & \dots & \dots & \dots \\ & & & & & & & & 0 & = & b''_m, \end{array} \tag{2.18}$$

а її основна матриця збігатиметься з матрицею (2.9).

Перехід від системи (2.1) до системи (2.18) називається *прямим ходом* методу Гаусса.

Якщо $r < m$, то система (2.18) містить рівняння вигляду $0 = b''_t$, $t = r+1, \dots, m$. Якщо серед вільних членів $b''_{r+1}, \dots, b''_m$ є хоча б один ненульовий, то система (2.18) (а тим самим і квазірівносильна їй початкова СЛР) є несумісною. Тому на цьому процес її розв'язання завершується.

Якщо ж $r = m$ або всі коефіцієнти $b''_{r+1}, \dots, b''_m$ дорівнюють 0, то перетворення системи можна продовжити далі, перейшовши до *зворотного ходу* методу Гаусса. Виконуючи такі самі перетворення, як у зворотному

ході алгоритму Гаусса, систему (2.18) можна звести до такої:

$$\begin{array}{rrrrrrrrrrrr}
x_1 & & & + f_{1,r+1}x_{r+1} & + \ldots + & f_{1n}x_n & = & h_1, \\
 & x_2 & & + f_{2,r+1}x_{r+1} & + \ldots + & f_{2n}x_n & = & h_2, \\
 & & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & \\
 & & x_r & + f_{r,r+1}x_{r+1} & + \ldots + & f_{rn}x_n & = & h_r, \\
 & & & & & 0 & = & 0, \\
 & & & & & \ldots\ldots & & \\
 & & & & & 0 & = & 0.
\end{array} \tag{2.19}$$

Основною матрицею цієї СЛР буде матриця (2.10).

Далі розглянемо два випадки (рівняння вигляду $0 = 0$ можна відкинути):

I. $r = n$. У цьому випадку система (2.19) має вигляд

$$\begin{array}{rcl}
x_1 & = & h_1, \\
x_2 & = & h_2, \\
\ldots\ldots & & \\
x_n & = & h_n.
\end{array} \tag{2.20}$$

Очевидно, що ця СЛР є сумісною, а її єдиним розв'язком буде набір $(h_1, \ldots, h_n)$. Тобто СЛР є визначеною.

II. $r < n$. У цьому випадку систему (2.19) можна переписати як

$$\begin{array}{rcrrrrr}
x_1 & = & h_1 & - f_{1,r+1}x_{r+1} & - \ldots - & f_{1n}x_n\,, \\
x_2 & = & h_2 & - f_{2,r+1}x_{r+1} & - \ldots - & f_{2n}x_n\,, \\
\ldots\ldots & & & & & & \\
x_r & = & h_r & - f_{r,r+1}x_{r+1} & - \ldots - & f_{rn}x_n\,.
\end{array} \tag{2.21}$$

Якщо СЛР зводиться до вигляду (2.21), то невідомі $x_{r+1}, \ldots, x_n$ називаються *вільними*. Таким невідомим можна надавати довільних значень: $x_{r+1} = t_1, \ldots, x_n = t_{n-r}$. Якщо значення вільних невідомих вибрані, то *головні* невідомі вже визначаються однозначно:

$$\begin{array}{rcrrrrrrr}
x_1 & = & h_1 & - f_{1,r+1}t_1 & - f_{1,r+2}t_2 & - \ldots - & f_{1n}t_{n-r}\,, \\
x_2 & = & h_2 & - f_{2,r+1}t_1 & - f_{2,r+2}t_2 & - \ldots - & f_{2n}t_{n-r}\,, \\
\ldots\ldots & & & & & & & \\
x_r & = & h_r & - f_{r,r+1}t_1 & - f_{r,r+1}t_2 & - \ldots - & f_{rn}t_{n-r}\,.
\end{array} \tag{2.22}$$

Таким чином, розв'язком буде кожен набір вигляду

$$(h_1 - f_{1,r+1}t_1 - \ldots - f_{1n}t_{n-r}, \ldots, h_r - f_{r,r+1}t_1 - \ldots - f_{rn}t_{n-r}, t_1, \ldots, t_{n-r}), \tag{2.23}$$

де замість параметрів $t_1, \ldots, t_{n-r}$ можна підставляти довільні значення. Оскільки у кожному розв'язкові невідомі $x_{r+1}, \ldots, x_n$ повинні набувати якихось значень, то наборами вигляду (2.23) вичерпуються всі розв'язки СЛР (2.19). Зокрема, у цьому випадку наша СЛР є невизначеною.

Підсумки наших міркувань можна сформулювати у вигляді теореми 8.

Теорема 8 (теорема Гаусса)**.** *а) СЛР* (2.1) *буде сумісною тоді й лише тоді, коли після прямого ходу методу Гаусса вона зводиться до вигляду* (2.18)*, причому* $b''_{r+1} = \ldots = b''_m = 0$.

б) Якщо СЛР (2.1) *сумісна, то зворотним ходом методу Гаусса її можна звести до квазірівносильної їй СЛР вигляду* (2.19). *Якщо* $r = n$*, то СЛР буде визначеною, а якщо* $r < n$ *– то невизначеною. Розв'язками СЛР* (2.19) *будуть усі набори вигляду* (2.23) *і тільки вони.*

При застосуванні методу Гаусса на практиці, звичайно, замість елементарних перетворень рівнянь системи виконують відповідні перетворення рядків її розширеної матриці.

Розв'язок невизначеної СЛР , записаний у вигляді сукупності рівностей (2.22) або набору (2.23) із довільними параметрами $t_1, \ldots, t_{n-r}$, часто називають *загальним розв'язком* СЛР . Зауважимо, що оскільки СЛР до вигляду (2.18) можна зводити по-різному, то вибір вільних невідомих, узагалі кажучи, є неоднозначним. Але кількість вільних невідомих, як ми пізніше побачимо, від способу зведення вже не залежить.

Із теореми Гаусса одразу випливає такий наслідок.

Наслідок 5. *Над нескінченним полем кожна невизначена СЛР має безліч розв'язків.*

Доведення. Якщо СЛР невизначена, то її розв'язками є набори вигляду (2.23), причому $r < n$. Значенням параметра t_1 може бути довільний елемент поля. Оскільки поле нескінченне, а різним значенням параметра t_1 відповідають різні розв'язки, то розв'язків буде нескінченно багато. □

Із цього наслідку випливає, що над нескінченним полем СЛР може мати або один розв'язок, або нескінченно багато розв'язків, або не мати жодного розв'язку.

Приклад 4. Дослідимо на сумісність і знайдемо загальний розв'язок системи лінійних рівнянь

$$\begin{aligned} 7x_1 - 5x_2 - 2x_3 &= 8, \\ -3x_1 + 2x_2 + x_3 &= -3, \\ 2x_1 - x_2 - x_3 &= 1, \\ - x_2 + x_3 &= 3 \end{aligned}$$

із дійсними коефіцієнтами.

Елементарними перетвореннями рядків зведемо розширену матрицю нашої системи до спеціального трапецієподібного вигляду:

$$\left(\begin{array}{ccc|c} 7 & -5 & -2 & 8 \\ -3 & 2 & 1 & -3 \\ 2 & -1 & -1 & 1 \\ 0 & -1 & 1 & 3 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -1 & 0 & 2 \\ 0 & -1 & 1 & 3 \\ 0 & 1 & -1 & -3 \\ 0 & -1 & 1 & 3 \end{array}\right) \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{ccc|c} 1 & -1 & 0 & 2 \\ 0 & 1 & -1 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

(тут ми спочатку до першого рядка додали подвоєний другий; потім до другого та третього рядків додали перший, помножений на 3 і -2 відповідно; далі до третього та четвертого додали другий, помножений на 1 і -1 відповідно; насамкінець помножили другий рядок на -1 і отриманий рядок додали до першого). Остання матриця відповідає СЛР

$$\begin{aligned} x_1 - x_3 &= -1, \\ x_2 - x_3 &= -3, \end{aligned}$$

яка за теоремою Гаусса є невизначеною. Невідома x_3 є вільною, а загальний розв'язок нашої системи має вигляд $(-1+t, -3+t, t)$, де параметр t є довільним дійсним числом.

Із теореми Гаусса випливає, що тип СЛР вже повністю визначається після прямого ходу методу Гаусса, тобто після її зведення до вигляду (2.18). Зокрема, маємо таке.

Наслідок 6. *Сумісна СЛР буде визначеною тоді й лише тоді, коли після прямого ходу методу Гаусса її основна матриця має трикутний вигляд.*

Звідси, у свою чергу, одержимо ще один важливий наслідок.

Наслідок 7 (теорема про невизначеність однорідних СЛР)**.** *Якщо в однорідній СЛР кількість невідомих перевищує кількість рівнянь, то ця СЛР є невизначеною.*

Доведення. Однорідна СЛР завжди є сумісною, оскільки нульовий набір $(0, 0, \ldots, 0)$ є її розв'язком. Але, якщо невідомих більше, ніж рівнянь, то до трикутного вигляду її звести не можна. Тому, за наслідком 6, така СЛР буде невизначеною. □

Твердження 9. *У кожному полі, яке містить коефіцієнти даної СЛР, її тип буде одним і тим самим.*

Доведення. Тип СЛР повністю визначається після прямого ходу методу Гаусса, тобто після її зведення до вигляду (2.18). При цьому зведенні ми використовуємо лише арифметичні операції над коефіцієнтами системи – додавання, віднімання, множення, ділення, – які не виводять за межі найменшого поля, що містить ці коефіцієнти. □

Зауважимо, що аналогічне твердження для нелінійних систем (уже навіть для рівнянь другого степеня) є хибним: сумісність чи несумісність рівняння $x^2 = 2$ (або $x^2 = -1$) залежить від поля, над яким полем ми його розглядаємо – $\mathbb{Q}$, $\mathbb{R}$ чи $\mathbb{C}$.

2.3. Оцінювання ефективності методу Гаусса

Більшість математичних моделей, які використовують на практиці (від локальних – розрахунок міцності конкретної деталі, до глобальних – прогноз погоди на планеті), є наближеними. Тому часто доводиться робити вибір між точністю моделі, пов'язаною з кількістю змінних, і необхідним об'ємом обчислень. Друга важлива проблема, яка тут виникає, пов'язана із чутливістю моделі до похибок: зазвичай як параметри моделі, так і обчислення на комп'ютерах є наближеними.

Задача 1. *Геометрична прогресія*

$$a_0 = 1,\ a_1 = \frac{1-\sqrt{5}}{2},\ a_2 = \left(\frac{1-\sqrt{5}}{2}\right)^2,\ \ldots$$

задовольняє як рекурентне співвідношення $a_{n+1} = a_n \cdot \frac{1-\sqrt{5}}{2}$*, так і рекурентне співвідношення* $a_{n+1} = a_n + a_{n-1}$*. Кожне із цих співвідношень можна використовувати для обчислення членів даної прогресії. Обчисліть на*

калькуляторі двома способами 50-й член прогресії і порівняйте отримані результати. Який із способів дає точніший результат? Яка причина розбіжності результатів?

СЛР , які виникають на практиці, містять сотні, а то й тисячі невідомих і рівнянь, коефіцієнти яких часто відомі лише з певною точністю. Теоретично кожну таку СЛР можна розв'язати методом Гаусса. Але з погляду практики виникає два важливі питання. По-перше, наскільки цей метод ефективний із погляду об'єму обчислень? СЛР якого порядку реально можуть бути розв'язані за допомогою сучасних обчислювальних засобів? І по-друге, наскільки метод Гаусса чутливий до похибок початкових даних і результатів обчислень і як можна контролювати цю чутливість? Відповідь на друге питання виходить далеко за межі нашого курсу, а на перше вже зараз можна дати досить вичерпну відповідь.

При застосуванні методу Гаусса інколи доводиться робити перестановку рівнянь чи перенумерацію невідомих. Однак ці операції зводяться до перестановок рядків і стовпців матриці СЛР і виконуються дуже швидко. Тому часом на виконання цих операцій нехтуємо. Крім того в методі Гаусса кількість додавань-віднімань приблизно дорівнює кількості множень-ділень, а останні у випадку багатоцифрових чисел вимагають значно більших зусиль. Тому для оцінювання ефективності методу Гаусса досить підрахувати лише кількість множень-ділень.

Лема 3. *У загальному випадку при розв'язуванні визначеної квадратної СЛР порядку n прямий хід методу Гаусса вимагає не більше ніж $n(n+1)(2n+1)/6$ операцій множення-ділення.*

Доведення. На першому кроці прямого ходу методу Гаусса потрібно зробити нулі під діагоналлю у першому стовпці розширеної матриці. Для цього перший рядок ділимо на a_{11}. Це вимагає n операцій ділення (коефіцієнт при x_1 дорівнюватиме 1, тому потрібно обчислити коефіцієнти при решті невідомих і вільний член). Далі в кожному з решти рядків робимо 0 на першому місці, віднімаючи для цього від кожного з рядків відповідне кратне першого рядка. Це вимагає $(n-1)n$ операцій множення. Таким чином, перший крок прямого ходу вимагає загалом $n + (n-1)n = n^2$ операцій множення-ділення.

На другому кроці прямого ходу ми фактично працюємо із СЛР порядку $n-1$. Тому другий крок вимагатиме $(n-1)^2$ операцій множення-ділення. Аналогічно третій крок вимагатиме $(n-2)^2$ операцій і т. д. У випадку визначеної СЛР прямий хід методу Гаусса завершиться зведенням основної матриці СЛР до трикутного вигляду з одиницями на

головній діагоналі. Тому загальна кількість операцій множення-ділення, яку доведеться виконати, така:

$$n^2 + (n-1)^2 + (n-2)^2 + \ldots + 2^2 + 1^2 = \frac{n(n+1)(2n+1)}{6}. \qquad \square$$

Лема 4. *У загальному випадку при розв'язуванні визначеної квадратної СЛР порядку n зворотний хід методу Гаусса вимагає не більше ніж $(n^2 - n)/2$ операцій множення.*

Доведення. У випадку визначеної квадратної СЛР прямий хід методу Гаусса закінчується зведенням основної матриці СЛР до трикутного вигляду з одиницями на головній діагоналі. На першому кроці зворотного ходу робляться нулі над діагоналлю в останньому стовпці основної матриці. Для цього з кожного рядка, крім останнього, віднімається відповідне кратне останнього рядка. Оскільки у цих рядках потрібно обчислювати лише вільні члени, то це вимагає не більше ніж $n-1$ операцій множення (операцій множення може бути менше, ніж $n-1$, бо деякі елементи останнього стовпця могли стати нульовими вже після прямого ходу). Зауважимо, що операції ділення при цьому не виконуються.

На другому кроці зворотного ходу робляться нулі над діагоналлю в передостанньому стовпці основної матриці. Міркуючи аналогічно попередньому, бачимо, що це вимагає не більше ніж $n-2$ операцій множення, і т. д. Тому загальна кількість операцій множення при зворотному ході методу Гаусса не більша, ніж

$$(n-1) + (n-2) + \ldots + 2 + 1 = \frac{n^2 - n}{2}. \qquad \square$$

Таким чином, при розв'язуванні СЛР порядку n метод Гаусса вимагає не більше, ніж

$$\frac{n(n+1)(2n+1)}{6} + \frac{n^2 - n}{2} = \frac{n^3 + 3n^2 - n}{3}$$

(тобто при великих n приблизно $n^3/3$) операцій множення-ділення. Довгий час вважалося, що швидших методів розв'язування СЛР не існує. (Звичайно, для деяких класів СЛР спеціального вигляду – наприклад, трикутних або стрічкових – можуть існувати і швидші методи, які істотно враховують специфіку таких СЛР.) Однак кілька десятків років тому Штрассен придумав новий метод, в якому кількість операцій множення-ділення обмежена згори числом $Cn^{\log_2 7}$, де C – деяка

константа. Для великих n цей метод потенційно є кращим за метод Гаусса. Однак розв'язувати методом Штрассена СЛР не дуже великих порядків непрактично, бо цей метод вимагає більшої кількості операцій додавання-віднімання, а константа C є великою. До того ж метод Штрассена має досить складну логічну структуру.

Переваги методу Штрассена стають відчутними лише для дуже великих n. Настільки великих, що за сучасного стану обчислювальної техніки розв'язування СЛР таких порядків навіть методом Штрассена все одно вимагає нереального часу.

Є гіпотеза, що існують методи розв'язування СЛР, кількість операцій множення-ділення в яких обмежена згори числом $Cn^2 \log n$. Однак константа C може виявитися настільки великою, що практичного значення ці методи все одно не матимуть.

2.4. Задачі

2.1. Розв'яжіть СЛР

$$\begin{array}{rcrcrcl} x & + & y & + & z & = & a, \\ x & + & \varepsilon y & + & \varepsilon^2 z & = & b, \\ x & + & \varepsilon^2 y & + & \varepsilon z & = & c, \end{array}$$

де ε – первісний корінь степеня 3 з одиниці.

2.2*. Нехай $Ax = b$ – квадратна невироджена СЛР і нехай сума модулів елементів кожного рядка матриці $E + A$ менша за 1. Для довільного стовпця X_0 матриці A рекурентно визначимо послідовність стовпців: $X_{k+1} = (A + E)X_k - b$. Доведіть, що ця послідовність збігається до розв'язку СЛР $Ax = b$.

2.3*. Доведіть, що довільну квадратну матрицю із цілими коефіцієнтами можна звести до діагонального вигляду за допомогою лише цілочислових перетворень.

3. Арифметичні векторні простори

3.1. Лінійна залежність

З огляду на СЛР у нас з'являлися впорядковані набори чисел, які залежно від контексту означали різні речі: розв'язки СЛР, стовпці вільних членів, рядки (стовпці) матриці СЛР. При розв'язуванні СЛР (точніше,

при зведенні її матриці до простішого вигляду) ми такі набори покомпонентно додавали і множили на числа. Виявляється, аналогічні операції мають зміст і в багатьох інших випадках. Наприклад, є справедливим таке твердження.

Твердження 10. *Покомпонентна сума двох розв'язків і довільне кратне розв'язку однорідної СЛР знову будуть розв'язками цієї СЛР.*

Доведення. Нехай $(a_1, a_2, \ldots, a_n)$ та $(b_1, b_2, \ldots, b_n)$ – два довільні розв'язки однорідної СЛР

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & 0, \\ a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n & = & 0, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n & = & 0. \end{array} \tag{3.1}$$

Це означає, що для кожного i $(1 \le i \le m)$ виконуються рівності

$$a_{i1}a_1 + a_{i2}a_2 + \ldots + a_{in}a_n = 0, \qquad a_{i1}b_1 + a_{i2}b_2 + \ldots + a_{in}b_n = 0.$$

Але тоді для кожного i $(1 \le i \le m)$ та довільного k будуть справедливі й рівності

$$\begin{gathered} a_{i1}(a_1 + b_1) + a_{i2}(a_2 + b_2) + \ldots + a_{in}(a_n + b_n) = \\ = a_{i1}a_1 + a_{i1}b_1 + a_{i2}a_2 + a_{i2}b_2 + \ldots + a_{in}a_n + a_{in}b_n = \\ = (a_{i1}a_1 + a_{i2}a_2 + \ldots + a_{in}a_n) + (a_{i1}b_1 + a_{i2}b_2 + \ldots + a_{in}b_n) = 0 + 0 = 0 \end{gathered}$$

та

$$a_{i1}(ka_1) + a_{i2}(ka_2) + \ldots + a_{in}(ka_n) = k(a_{i1}a_1 + a_{i2}a_2 + \ldots + a_{in}a_n) = 0.$$

Отже, набори $(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ і $(ka_1, ka_2, \ldots, ka_n)$ також будуть розв'язками системи (4.4). □

Вправа 7. *Переконайтеся на прикладі системи*

$$\begin{array}{ccccc} x_1 & + & x_2 & = & 1, \\ 2x_1 & + & 2x_2 & = & 2, \end{array}$$

що для неоднорідних СЛР твердження 10 не виконується.

Стан, коли один і той же об'єкт (у цьому разі – впорядковані набори чисел із покомпонентним додаванням і множенням на числа) зустрічається під різними масками (рядки матриць, розв'язки однорідних

СЛР тощо), є типовим для математики, особливо для алгебри. У таких випадках доречно зняти маски і вивчити об'єкт у "голому" вигляді. Знайденими властивостями пізніше можна буде користуватися кожного разу, коли ми знову зустрінемо цей об'єкт під тією чи іншою маскою.

У випадку з упорядкованими наборами чисел такий підхід приводить до поняття арифметичного векторного простору.

Означення 5. *Нехай P – деяке поле*[9]. ***Арифметичним векторним простором*** *розмірності n над полем P називається множина*

$$P^n := \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in P\}$$

(*елементи якої будемо називати* ***векторами***) *разом із операціями* ***додавання*** *векторів і* ***множення*** *векторів на елементи поля P, визначеними таким чином*:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

$$\alpha \cdot (a_1, a_2, \ldots, a_n) := (\alpha a_1, \alpha a_2, \ldots, \alpha a_n).$$

Елементи поля P часто називають *скалярами*.

Теорема 9. *Арифметичний векторний простір має такі властивості*:

(1) *додавання векторів* ***асоціативне***: *для довільних векторів $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ із P^n виконується рівність $(\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c} = \boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c})$*;

(2) *додавання векторів* ***комутативне***: *для довільних векторів $\boldsymbol{a}, \boldsymbol{b}$ із P^n виконується рівність $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{b} + \boldsymbol{a}$*;

(3) *для додавання векторів існує* ***нейтральний елемент***: *існує такий вектор $\mathbf{0}$, що для довільного вектора $\boldsymbol{a} \in P^n$ виконується рівність $\boldsymbol{a} + \mathbf{0} = \boldsymbol{a}$*;

(4) *для додавання векторів існують* ***протилежні елементи***: *для кожного вектора $\boldsymbol{a} \in P^n$ існує такий вектор $\boldsymbol{b} \in P^n$, що $\boldsymbol{a} + \boldsymbol{b} = \mathbf{0}$*;

(5) ***унітарність***: *для кожного вектора $\boldsymbol{a} \in P^n$ виконується рівність $1\boldsymbol{a} = \boldsymbol{a}$*;

(6) *для довільних скалярів $\alpha, \beta \in P$ та вектора $\boldsymbol{a} \in P^n$ виконується рівність $(\alpha\beta)\boldsymbol{a} = \alpha(\beta\boldsymbol{a})$*;

[9] Поки що можна вважати, що P є одним із полів $\mathbb{Q}$, $\mathbb{R}$ або $\mathbb{C}$. Пізніше список полів значно розшириться.

(7) ***дистрибутивність*** *відносно додавання скалярів*: *для довільних скалярів* $\alpha, \beta \in P$ *та вектора* $\boldsymbol{a} \in P^n$ *виконується рівність* $(\alpha + \beta)\boldsymbol{a} = \alpha\boldsymbol{a} + \beta\boldsymbol{a}$;

(8) ***дистрибутивність*** *відносно додавання векторів*: *для довільних скаляра* $\alpha \in P$ *та векторів* $\boldsymbol{a}, \boldsymbol{b} \in P^n$ *виконується рівність* $\alpha(\boldsymbol{a} + \boldsymbol{b}) = \alpha\boldsymbol{a} + \alpha\boldsymbol{b}$.

Доведення. Усі властивості легко перевіряються безпосередньо. Зауважимо тільки, що нейтральним вектором для додавання є *нульовий вектор* $\mathbf{0} = (0, 0, \ldots, 0)$, а протилежним до вектора $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ є вектор $-\boldsymbol{a} = (-a_1, -a_2, \ldots, -a_n)$. □

Властивості (1)-(8) із теореми 9 називають *аксіомами векторного простору*. Подібний список властивостей буде з'являтись у нас ще багато разів і згодом ляже в основу більш загального поняття векторного простору.

Можна домовитися записувати елементи арифметичного векторного простору P^n як вектори-рядки, а можна – як вектори-стовпці. Різниця між цими формами запису є чисто умовною, і вибирати одну з них зручно залежно від ситуації (ми вже стикалися із цим, коли говорили про вектори-рядки і вектори-стовпці матриці).

Упорядковані набори $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ векторів часто називають *системами векторів*. Від множини векторів це поняття відрізняється як наявністю порядку (який інколи може бути дуже важливим), так і тим, що серед векторів системи можуть бути однакові.

Означення 6. ***Лінійною комбінацією*** *векторів* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ *з коефіцієнтами* $k_1, k_2, \ldots, k_m$ *з поля* P *називається вектор*

$$\boldsymbol{u} = k_1\boldsymbol{v}_1 + k_2\boldsymbol{v}_2 + \ldots + k_m\boldsymbol{v}_m \,.$$

Якщо вектор $\boldsymbol{u}$ *є лінійною комбінацією векторів* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$, *то кажуть також, що* ***u лінійно виражається*** *через ці вектори.*

Означення 7. *Множину всіх векторів, що лінійно виражаються через вектори* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$, *називають* ***лінійною оболонкою*** *, натягнутою на систему* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ *(або породженою системою* $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$*), і позначають* $\langle \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m \rangle$ *або* $\mathcal{L}(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m)$.

Означення 8. *Лінійна комбінація*

$$k_1\boldsymbol{v}_1 + k_2\boldsymbol{v}_2 + \ldots + k_n\boldsymbol{v}_m$$

називається ***нетривіальною****, якщо серед коефіцієнтів* k_1, k_2, …, k_m *є принаймні один ненульовий. У противному разі лінійна комбінація називається* ***тривіальною****.*

Означення 9. *Система векторів* $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, …, $\boldsymbol{v}_m$ *називається* ***лінійно залежною****, якщо принаймні одна нетривіальна лінійна комбінація цих векторів дорівнює нульовому вектору. У противному разі система векторів називається* ***лінійно незалежною****.*

Таким чином, лінійна незалежність системи векторів $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m$ означає, що рівність

$$k_1\boldsymbol{v}_1 + k_2\boldsymbol{v}_2 + \ldots + k_m\boldsymbol{v}_m = \boldsymbol{0}$$

можлива тоді й лише тоді, коли $k_1 = k_2 = \ldots = k_m = 0$.

Приклад 5. 1. Система векторів $\boldsymbol{e}_1 = (1, 0, \ldots, 0)$, $\boldsymbol{e}_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $\boldsymbol{e}_n(0, \ldots, 0, 1)$ є лінійно незалежною. Справді, лінійна комбінація

$$k_1\boldsymbol{e}_1 + k_2\boldsymbol{e}_2 + \ldots + k_n\boldsymbol{e}_n = (k_1, k_2, \ldots, k_n)$$

цих векторів дорівнює $\boldsymbol{0}$ лише тоді, коли $k_1 = k_2 = \ldots = k_n = 0$.

2. Система векторів $\boldsymbol{u}_1 = (1, 0, \ldots, 0)$, $\boldsymbol{u}_2 = (1, 1, 0, \ldots, 0)$, $\ldots$, $\boldsymbol{u}_n = (1, 1, \ldots, 1)$ також є лінійно незалежною. Справді, лінійна комбінація цих векторів із коефіцієнтами k_1, k_2, …, k_n має вигляд

$$k_1\boldsymbol{u}_1 + k_2\boldsymbol{u}_2 + \ldots + k_n\boldsymbol{n}_n =$$
$$= (k_1 + k_2 + \ldots + k_n, k_2 + \ldots + k_n, \ldots, k_{n-1} + k_n, k_n).$$

Очевидно, що вона дорівнює $\boldsymbol{0}$ лише тоді, коли $k_1 = k_2 = \ldots = k_n = 0$.

3. Система векторів $\boldsymbol{v}_1 = (1, -1, 0, \ldots, 0)$, $\boldsymbol{v}_2 = (0, 1, -1, 0, \ldots, 0)$, $\ldots$, $\boldsymbol{v}_n = (-1, 0, \ldots, 0, 1)$ є лінійно залежною, оскільки

$$1 \cdot \boldsymbol{e}_1 + 1 \cdot \boldsymbol{e}_2 + \ldots + 1 \cdot \boldsymbol{e}_n = (0, 0, \ldots, 0).$$

Зауваження. **1.** Із комутативності додавання векторів випливає, що властивість системи векторів бути лінійно (не)залежною не залежить від конкретного впорядкування векторів цієї системи.

2. Лінійна залежність або незалежність – це властивості *систем векторів*. Однак стало звичним застосовувати ці вирази і до самих векторів: замість говорити про "лінійно (не)залежну систему векторів" часто говорять про "лінійно (не)залежні вектори" або навіть про множину "лінійно (не)залежних векторів".

З означення 9 випливає, що *порожня система векторів є лінійно незалежною*. Це виглядає трохи парадоксально, але це повністю узгоджується з подальшою теорією і є дуже зручним, бо позбавляє від непотрібних обмежень і розгляду вироджених випадків. Тут повна аналогія з тим, що суму нульової кількості доданків зручно вважати рівною 0, а добуток нульової кількості множників – рівним 1. Зокрема, звідси випливає, що нульовий вектор треба вважати лінійною комбінацією порожньої множини векторів (навіть більше – він є єдиним вектором із такою властивістю).

Вправа 8. *Доведіть, що*

а) *система з одного вектора буде лінійно залежною тоді й лише тоді, коли цей вектор нульовий*;

б) *система із двох векторів буде лінійно залежною тоді й лише тоді, коли ці вектори пропорційні.*

Використовуючи дії над векторами, можна дати іншу інтерпретацію системам лінійних рівнянь. Справді, СЛР (2.1) можна записати у вигляді

$$x_1\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + x_2\begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \ldots + x_n\begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}, \tag{3.2}$$

або, позначивши через

$$\boldsymbol{a}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \quad \boldsymbol{a}_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix}, \quad \ldots, \quad \boldsymbol{a}_n = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

відповідно стовпці основної матриці і стовпець вільних членів цієї системи, у вигляді

$$x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_n\boldsymbol{a}_n = \boldsymbol{b}. \tag{3.3}$$

Рівність (3.3) (або її розгорнутий варіант (3.2)) називається *векторним способом запису* СЛР (2.1).

На векторній мові зручно формулювати багато властивостей СЛР. Наприклад, сумісність СЛР (2.1) рівносильна тому, що стовпець $\boldsymbol{b}$ вільних членів лінійно виражається через стовпці $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ основної матриці, а визначеність СЛР означає, що стовпець вільних членів можна подати у вигляді лінійної комбінації стовпців основної матриці єдиним способом.

Теорема 10. *Властивості лінійно (не)залежних систем векторів*:

а) надсистема лінійно залежної системи лінійно залежна;

б) підсистема лінійно незалежної системи лінійно незалежна;

в) (***транзитивність властивості "лінійно виражатися"***) *якщо вектори* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ *лінійно виражаються через вектори* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$, *а кожен з векторів* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$ *у свою чергу лінійно виражається через вектори* $\boldsymbol{c}_1 \ldots, \boldsymbol{c}_m$, *то вектори* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ *лінійно виражатимуться через вектори* $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m$;

г) якщо система векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ *лінійно незалежна, а система* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{u}$ *– лінійно залежна, то вектор* $\boldsymbol{u}$ *є лінійною комбінацією векторів* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$, *причому коефіцієнти* $\lambda_1, \ldots, \lambda_k$ *лінійної комбінації* $\boldsymbol{u} = \lambda_1\boldsymbol{a}_1 + \ldots + \lambda_k\boldsymbol{a}_k$ *визначені однозначно.*

Доведення. Твердження а) і б) випливають безпосередньо із означення лінійно (не)залежних систем векторів.

в) Нехай

$$\boldsymbol{a}_i = \sum_{j=1}^{l} \beta_{ij}\boldsymbol{b}_j,\ 1 \le i \le k, \qquad \boldsymbol{b}_j = \sum_{t=1}^{m} \gamma_{jt}\boldsymbol{c}_t,\ 1 \le j \le l.$$

Тоді

$$\boldsymbol{a}_i = \sum_{j=1}^{l} \beta_{ij} \sum_{t=1}^{m} \gamma_{jt}\boldsymbol{c}_t = \sum_{t=1}^{m} \left(\sum_{j=1}^{l} \beta_{ij}\gamma_{jt} \right) \boldsymbol{c}_t.$$

г) Із лінійної залежності системи векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{u}$ випливає, що знайдуться такі скаляри $\alpha_1, \ldots, \alpha_k, \alpha$, які не всі дорівнюють нулю і задовольняють рівність

$$\alpha_1\boldsymbol{a}_1 + \ldots + \alpha_k\boldsymbol{a}_k + \alpha\boldsymbol{u} = \boldsymbol{0}.$$

Зауважимо, що $\alpha \neq 0$, бо інакше остання рівність означала б, що нетривіальна лінійна комбінація векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ дорівнює нульовому вектору. А це суперечить лінійній незалежності цих векторів. Тому

$$\boldsymbol{u} = -\frac{\alpha_1}{\alpha}\boldsymbol{a}_1 - \ldots - \frac{\alpha_k}{\alpha}\boldsymbol{a}_k. \tag{3.4}$$

Припустимо тепер, що ми маємо два зображення вектора $\boldsymbol{u}$ у вигляді лінійної комбінації векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$:

$$\boldsymbol{u} = \lambda_1\boldsymbol{a}_1 + \ldots + \lambda_k\boldsymbol{a}_k \quad \text{і} \quad \boldsymbol{u} = \lambda'_1\boldsymbol{a}_1 + \ldots + \lambda'_k\boldsymbol{a}_k.$$

Віднімаючи від першої рівності другу, одержуємо $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$:

$$\boldsymbol{0} = (\lambda_1 - \lambda'_1)\boldsymbol{a}_1 + \ldots + (\lambda_k - \lambda'_k)\boldsymbol{a}_k.$$

Оскільки вектори $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ лінійно незалежні, то

$$\lambda_1 - \lambda'_1 = \ldots = \lambda_k - \lambda'_k = 0.$$

Отже, $\lambda_1 = \lambda'_1, \ \ldots, \ \lambda_k = \lambda'_k$, що й доводить єдиність зображення (3.4). □

Із пункту а) цієї теореми і вправи 8 одразу випливає, що кожна система, яка містить нульовий вектор або два пропорційні вектори, є лінійно залежною.

Теорема 11 (критерій лінійної залежності)**.** *Система векторів* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ $(k > 1)$ *буде лінійно залежною тоді й лише тоді, коли хоча б один із векторів цієї системи лінійно виражається через інші вектори системи.*

Ми доведемо навіть трохи сильніше твердження:

Теорема 12. *Система векторів* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ $(k > 1)$ *буде лінійно залежною тоді й лише тоді, коли хоча б один із векторів цієї системи лінійно виражається через попередні вектори.*

Доведення. Достатність. Нехай вектор $\boldsymbol{a}_i$ лінійно виражається через попередні вектори: $\boldsymbol{a}_i = \lambda_1\boldsymbol{a}_1 + \ldots + \lambda_k\boldsymbol{a}_{i-1}$. Тоді маємо нетривіальну лінійну комбінацію векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$, яка дорівнює нулю:

$$\lambda_1\boldsymbol{a}_1 + \ldots + \lambda_{i-1}\boldsymbol{a}_{i-1} + (-1)\cdot\boldsymbol{a}_i + 0\cdot\boldsymbol{a}_{i+1} + \ldots + 0\cdot\boldsymbol{a}_k = \boldsymbol{0}.$$

Отже, вектори $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ є лінійно залежними.

Необхідність. Нехай вектори $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ лінійно залежні і

$$\lambda_1\boldsymbol{a}_1 + \ldots + \lambda_{i-1}\boldsymbol{a}_{i-1} + \lambda_i\boldsymbol{a}_i + \lambda_{i+1}\boldsymbol{a}_{i+1} + \ldots + \lambda_k\boldsymbol{a}_k = \boldsymbol{0}$$

– відповідна нетривіальна лінійна комбінація, яка дорівнює нулю. Нехай λ_i – останній ненульовий коефіцієнт у цій рівності. Тоді

$$\lambda_1\boldsymbol{a}_1 + \ldots + \lambda_{i-1}\boldsymbol{a}_{i-1} + \lambda_i\boldsymbol{a}_i = \boldsymbol{0},$$

звідки

$$\boldsymbol{a}_i = -\frac{\lambda_1}{\lambda_i}\boldsymbol{a}_1 - \ldots - \frac{\lambda_{i-1}}{\lambda_i}\boldsymbol{a}_{i-1}.$$ □

Теорема 13 (теорема про лінійну залежність)**.** *Якщо кожний вектор системи* $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ *лінійно виражається через вектори* $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_l$ *і* $k > l$*, то система векторів* $\boldsymbol{a}_1, \boldsymbol{a}_2 \ldots, \boldsymbol{a}_k$ *є лінійно залежною.*

Доведення. Нехай

$$\begin{gathered}\boldsymbol{a}_1 = \lambda_{11}\boldsymbol{b}_1 + \lambda_{21}\boldsymbol{b}_2 + \ldots + \lambda_{l1}\boldsymbol{b}_l,\\ \boldsymbol{a}_2 = \lambda_{12}\boldsymbol{b}_1 + \lambda_{22}\boldsymbol{b}_2 + \ldots + \lambda_{l2}\boldsymbol{b}_l,\\ \ldots\ldots\ldots\ldots\\ \boldsymbol{a}_k = \lambda_{1k}\boldsymbol{b}_1 + \lambda_{2k}\boldsymbol{b}_2 + \ldots + \lambda_{lk}\boldsymbol{b}_l.\end{gathered}$$

Нам потрібно довести існування нетривіальної лінійної комбінації векторів $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$, яка дорівнює нулю. Запишемо її з невизначеними коефіцієнтами:

$$x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_k\boldsymbol{a}_k = \boldsymbol{0}, \tag{3.5}$$

і підставимо у (3.5) зображення векторів $\boldsymbol{a}_i$ через вектори $\boldsymbol{b}_j$. Одержимо

$$\begin{gathered}x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_k\boldsymbol{a}_k = x_1(\lambda_{11}\boldsymbol{b}_1 + \lambda_{21}\boldsymbol{b}_2 + \ldots + \lambda_{l1}\boldsymbol{b}_l) +\\ +x_2(\lambda_{12}\boldsymbol{b}_1 + \lambda_{22}\boldsymbol{b}_2 + \ldots + \lambda_{l2}\boldsymbol{b}_l) + \ldots + x_k(\lambda_{1k}\boldsymbol{b}_1 + \lambda_{2k}\boldsymbol{b}_2 + \ldots + \lambda_{lk}\boldsymbol{b}_l) =\\ = (x_1\lambda_{11} + x_2\lambda_{12} + \ldots + x_k\lambda_{1k})\boldsymbol{b}_1 +\\ +(x_1\lambda_{21} + x_2\lambda_{22} + \ldots + x_k\lambda_{2k})\boldsymbol{b}_2 +\\ \ldots\ldots\ldots\ldots\\ +(x_1\lambda_{l1} + x_2\lambda_{l2} + \ldots + x_k\lambda_{lk})\boldsymbol{b}_l.\end{gathered}$$

Рівність (3.5) очевидно справджується, коли всі коефіцієнти при $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_l$ дорівнюють нулю, тобто коли

$$\begin{array}{ccccccccc} x_1\lambda_{11} & + & x_2\lambda_{12} & + & \ldots & + & x_k\lambda_{1k} & = & 0\,,\\ x_1\lambda_{21} & + & x_2\lambda_{22} & + & \ldots & + & x_k\lambda_{2k} & = & 0\,,\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\ x_1\lambda_{l1} & + & x_2\lambda_{l1} & + & \ldots & + & x_k\lambda_{lk} & = & 0\,. \end{array} \tag{3.6}$$

Система (3.6) є однорідною СЛР, в якій кількість рівнянь l менша за кількість невідомих k. За теоремою про невизначеність однорідних СЛР (наслідок 7) ця система є невизначеною, отже, має ненульовий розв'язок $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Тому

$$\alpha_1\boldsymbol{a}_1 + \alpha_2\boldsymbol{a}_2 + \ldots + \alpha_k\boldsymbol{a}_k = \boldsymbol{0},$$

де не всі $\alpha_1, \alpha_2, \ldots, \alpha_k$ дорівнюють нулю. Отже, вектори $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ є лінійно залежними. □

З теореми про лінійну залежність одразу випливає такий наслідок.

Наслідок 8. *Якщо кожний вектор системи $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ лінійно виражається через вектори $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$ і система $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ лінійно незалежна, то $k \leq l$.*

Наслідок 9. *В арифметичному векторному просторі P^n будь-які $n+1$ векторів є лінійно залежними.*

Доведення випливає з теореми 13 і того, що у просторі P^n кожний вектор лінійно виражається через вектори $\boldsymbol{e}_1 = (1, 0, \ldots, 0)$, $\boldsymbol{e}_2 = (0, 1, \ldots, 0)$, $\ldots$, $\boldsymbol{e}_n = (0, \ldots, 0, 1)$. □

3.2. Ранг системи векторів

За наслідком 9 будь-які $n+1$ векторів арифметичного векторного простору P^n є лінійно залежними, а тому кожна лінійно незалежна система із P^n містить не більше ніж n векторів. Звідси випливає, що для кожної – скінченної чи нескінченної – системи $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k, \ldots$ векторів з P^n серед її лінійно незалежних підсистем є *максимальні*, тобто такі, які не містяться в жодній більшій лінійно незалежній підсистемі. Максимальні лінійно незалежні підсистеми коротко будемо називати *МЛНЗ-підсистемами*.

Твердження 11. *Довільний вектор системи векторів лінійно виражається через вектори її МЛНЗ-підсистеми.*

Доведення. Випливає з означення МЛНЗ-підсистеми та теореми 10.г). □

Наслідок 10. *Кожна МЛНЗ-підсистема системи векторів $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ буде також МЛНЗ-підсистемою її лінійної оболонки $\mathcal{L}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$.*

Доведення. Нехай $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$ – МЛНЗ-підсистема системи векторів $\boldsymbol{u}_1$, $\ldots$, $\boldsymbol{u}_k$, $U = \mathcal{L}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$. За твердженням 11 кожен вектор системи $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ лінійно виражається через вектори системи $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$, а за означенням лінійної оболонки кожен вектор $\boldsymbol{u} \in U$ лінійно виражається через вектори системи $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$. Тому за теоремою 10.в) про транзитивність властивості “лінійно виражатись” кожен вектор $\boldsymbol{u} \in U$ буде лінійно виражатись через вектори системи $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$. Але тоді для кожного $\boldsymbol{u} \in U$ система $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m, \boldsymbol{u}$ буде лінійно залежною. Отже, $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$ є МЛНЗ-підсистемою лінійної оболонки U. □

Системи векторів $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ та $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ називаються *еквівалентними*, якщо збігаються натягнуті на ці системи лінійні оболонки, тобто якщо $\mathcal{L}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = \mathcal{L}(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l)$.

Теорема 14 (про МЛНЗ-підсистеми еквівалентних систем)**.** *Будь-які МЛНЗ-підсистеми еквівалентних систем векторів складаються з однакової кількості векторів.*

Доведення. Нехай $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ та $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ – еквівалентні системи векторів, а U – їх спільна лінійна оболонка. Не обмежуючи загальності, можна вважати, що їх МЛНЗ-підсистемами будуть відповідно $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ ($r \leq k$) та $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ ($s \leq l$). За наслідком 10 вони одночасно будуть і МЛНЗ-підсистемами лінійної оболонки U. Оскільки $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ – МЛНЗ-підсистема U, то за твердженням 11 кожен вектор системи $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ буде лінійно виражатись через вектори $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$. Із лінійної незалежності векторів $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ і наслідку 8 теореми 13 випливає, що $r \leq s$.

Нерівність $s \leq r$ доводиться аналогічно. Тому $r = s$. □

Із цієї теореми одразу маємо.

Наслідок 11. *Будь-які дві максимальні лінійно незалежні підсистеми даної системи векторів складаються з однакової кількості векторів.*

Кількість векторів у МЛНЗ-підсистемі даної системи векторів S називається *рангом* цієї системи векторів і позначається $\operatorname{rank}(S)$ або $r(S)$. Якщо система S є скінченною і складається з векторів $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$, то використовують також позначення $\operatorname{rank}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ або $r(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$.

Безпосередньо з означення рангу системи векторів випливають такі його властивості.

Твердження 12. *а) Система векторів лінійно незалежна тоді й лише тоді, коли її ранг дорівнює кількості векторів у ній.*

б) $r(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k) \leq r(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{a}_{k+1}, \ldots, \boldsymbol{a}_{k+m})$.

в) Якщо до системи векторів долучити лінійну комбінацію векторів із цієї системи, то ранг системи не зміниться.

г) Якщо $r(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{b}) = r(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k)$*, то* $\boldsymbol{b}$ *є лінійною комбінацією векторів* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$.

Твердження 13. *Якщо кожен із векторів* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ *лінійно виражається через вектори* $\boldsymbol{w}_1 \ldots, \boldsymbol{w}_m$*, то* $r(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) \leq r(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m)$.

Доведення. Нехай $\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_p}$ – максимальна лінійно незалежна підсистема системи векторів $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, а $\boldsymbol{w}_{j_1}, \ldots, \boldsymbol{w}_{j_q}$ – аналогічна підсистема системи $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$. Тоді $r(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = p$, $r(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m) = q$. За твердженням 11 кожен вектор системи $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ лінійно виражається через вектори $\boldsymbol{w}_{j_1}, \ldots, \boldsymbol{w}_{j_q}$, а за умовою кожен вектор системи $\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_p}$ лінійно виражається через вектори $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$. Тому, за транзитивністю властивості "лінійно виражатись" (теорема 10.в), кожен вектор $\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_p}$ лінійно виражається через вектори $\boldsymbol{w}_{j_1}, \ldots, \boldsymbol{w}_{j_q}$. Із наслідку 8 теореми 13 про лінійну залежність тепер маємо, що $p \leq q$. □

Із теореми 14 про МЛНЗ-підсистеми еквівалентних систем та наслідку 11 випливає таке твердження.

Твердження 14. *Еквівалентні системи векторів мають однакові ранги.*

За аналогією з елементарними перетвореннями рівнянь СЛР чи рядків і стовпців матриці визначимо *елементарні перетворення* системи векторів. Такими перетвореннями є:

1) перестановка двох векторів системи;

2) множення одного з векторів системи на число $\lambda \neq 0$;

3) додавання до одного з векторів системи іншого її вектора, помноженого на деяке число λ.

Твердження 15. *Ранг системи векторів не змінюється при елементарних перетвореннях векторів цієї системи.*

Доведення. Нехай система векторів S_1 одержана елементарним перетворенням системи S. Оскільки кожен вектор із S_1 лінійно виражається через вектори з S, то за твердженням 13 $r(S_1) \leq r(S)$. З іншого боку, S можна одержати з S_1 оберненим елементарним перетворенням. Тому $r(S) \leq r(S_1)$. Отже, $r(S_1) \leq r(S)$. □

Якщо для векторів $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ можна підібрати такі скаляри $\lambda_1, \lambda_2, \ldots, \lambda_k$, що виконується рівність

$$\lambda_1 \boldsymbol{a}_1 + \lambda_2 \boldsymbol{a}_2 + \ldots + \lambda_k \boldsymbol{a}_k = \boldsymbol{0}, \tag{3.7}$$

то ми будемо казати, що для векторів $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ виконується *лінійне співвідношення* 3.7 (або що вектори $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ задовольняють лінійне співвідношення 3.7).

Лема 5. *При елементарних перетвореннях рядків матриці зберігаються всі лінійні співвідношення між стовпцями матриці.*

Доведення. Нехай для стовпців $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ матриці A виконується лінійне співвідношення

$$\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \ldots + \lambda_k\boldsymbol{a}_k = \boldsymbol{0}.$$

Це означає, що набір $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ є розв'язком записаної у векторній формі СЛР

$$x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_k\boldsymbol{a}_k = \boldsymbol{0}. \tag{3.8}$$

При елементарному перетворенні рядків матриці стовпці $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ перейдуть у стовпці $\boldsymbol{a}'_1, \boldsymbol{a}'_2, \ldots, \boldsymbol{a}'_k$, а СЛР 3.8 – у СЛР

$$x_1\boldsymbol{a}'_1 + x_2\boldsymbol{a}'_2 + \ldots + x_k\boldsymbol{a}'_k = \boldsymbol{0}. \tag{3.9}$$

Однак нова СЛР є рівносильною попередній, а тому набір $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ залишається її розв'язком. Отже, стовпці $\boldsymbol{a}'_1, \boldsymbol{a}'_2, \ldots, \boldsymbol{a}'_k$ задовольняють лінійне співвідношення

$$\lambda_1\boldsymbol{a}_1 + \lambda_2\boldsymbol{a}_2 + \ldots + \lambda_k\boldsymbol{a}_k = \boldsymbol{0}$$

із тими самими коефіцієнтами $\lambda_1, \lambda_2, \ldots, \lambda_k$. □

Лема 5 лежить в основі методу, який не тільки дозволяє знайти максимальну лінійно незалежну підсистему даної системи векторів, а й виразити через цю МЛНЗ-підсистему решту векторів системи. Нехай $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ деяка система векторів простору P^m. Розглянемо матрицю A, стовпцями якої є вектори $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$. Елементарними перетвореннями рядків (і, можливо, перестановками стовпців, що впливають лише на порядок векторів системи) цю матрицю можна звести до вигляду

$$\begin{pmatrix} 1 & \ldots & 0 & \gamma_{1,k+1} & \ldots & \gamma_{1n} \\ & \ddots & & \ldots & & \\ 0 & \ldots & 1 & \gamma_{k,k+1} & \ldots & \gamma_{kn} \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}. \tag{3.10}$$

Далі для зручності будемо вважати, що перестановки стовпців не виконувалися. Позначимо стовпці матриці (3.10) $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$. Очевидно, що перші k стовпців матриці A є лінійно незалежними. Крім того, із вигляду

матриці A безпосередньо видно, що кожен із наступних стовпців лінійно виражається через перші k стовпців:

$$\begin{gathered} \boldsymbol{b}_{k+1} = \gamma_{1,k+1}\boldsymbol{b}_1 + \ldots + \gamma_{k,k+1}\boldsymbol{b}_k\,, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \boldsymbol{b}_n = \gamma_{1n}\boldsymbol{b}_1 + \ldots + \gamma_{kn}\boldsymbol{b}_k\,. \end{gathered} \tag{3.11}$$

Тому долучення до $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ будь-якого нового стовпця робить систему векторів лінійно залежною. Це означає, що вектори $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ утворюють МЛНЗ-підсистему.

За лемою 5 при елементарних перетвореннях рядків усі лінійні співвідношення між стовпцями зберігаються. Тому висновки, які ми зробили про стовпці матриці (3.10), будуть правильними і для стовпців початкової матриці A, тобто для векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$: *вектори* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ *утворюють МЛНЗ-підсистему, а кожен із решти векторів виражається через ці вектори так*:

$$\begin{gathered} \boldsymbol{a}_{k+1} = \gamma_{1,k+1}\boldsymbol{a}_1 + \ldots + \gamma_{k,k+1}\boldsymbol{a}_k\,, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \boldsymbol{a}_n = \gamma_{1n}\boldsymbol{a}_1 + \ldots + \gamma_{kn}\boldsymbol{a}_k\,. \end{gathered}$$

Приклад 6. Для системи векторів $\mathbf{a}_1 = (1, 0, 3, 3)$, $\mathbf{a}_2 = (-2, -3, -5, -4)$, $\mathbf{a}_3 = (2, 2, 5, 4)$, $\mathbf{a}_4 = (0, -1, 0, 0)$, $\mathbf{a}_5 = (1, -4, 4, 5)$ знайти МЛНЗ-підсистему і виразити через цю МЛНЗ-підсистему інші вектори системи.

Виписуємо матрицю, стовпцями якої є вектори $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4, \boldsymbol{a}_5$, і зводимо її елементарними перетвореннями рядків до вигляду (3.10):

$$\begin{pmatrix} 1 & -2 & 2 & 0 & 1 \\ 0 & -3 & 2 & -1 & -4 \\ 3 & -5 & 5 & 0 & 4 \\ 3 & -4 & 4 & 0 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -2 & 2 & 0 & 1 \\ 0 & -3 & 2 & -1 & -4 \\ 0 & 1 & -1 & 0 & 1 \\ 0 & 2 & -2 & 0 & 2 \end{pmatrix} \rightsquigarrow$$

$$\rightsquigarrow \begin{pmatrix} 1 & -2 & 2 & 0 & 1 \\ 0 & 1 & -1 & 0 & 1 \\ 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Таким чином, вектори $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ і $\boldsymbol{a}_3$ утворюють МЛНЗ-підсистему і

$$\boldsymbol{a}_4 = \boldsymbol{a}_2 + \boldsymbol{a}_3, \qquad \boldsymbol{a}_5 = 3\boldsymbol{a}_1 + 2\boldsymbol{a}_2 + \boldsymbol{a}_3.$$

Зауважимо, що два останні співвідношення легко перевірити безпосередньо.

3.3. Ранг матриці

Із кожною матрицею

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}, \tag{3.12}$$

пов'язуються дві системи векторів: система

$$\boldsymbol{a}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \quad \boldsymbol{a}_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix}, \quad \dots, \quad \boldsymbol{a}_n = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} \tag{3.13}$$

її стовпців і система

$$\boldsymbol{b}_1 = (a_{11}, a_{12}, \dots, a_{1n}), \quad \dots, \quad \boldsymbol{b}_m = (a_{m1}, a_{m2}, \dots, a_{mn}) \tag{3.14}$$

її рядків. Ранг системи вектор-стовпців називається *стовпцевим* рангом матриці A і позначається $r_{\text{ст}}(A)$, а ранг системи вектор-рядків називається *рядковим* рангом матриці A і позначається $r_{\text{ряд}}(A)$.

Лема 6. *Обидва ранги матриці не змінюються при елементарних перетвореннях рядків цієї матриці.*

Доведення. Те, що не змінюється рядковий ранг, випливає із твердження 15, а те, що не змінюється стовпцевий ранг, одержуємо з леми 5. □

Транспонованою до матриці (3.12) називається матриця

$$A^\top = \begin{pmatrix} a_{11} & a_{21} & a_{31} & \dots & a_{m1} \\ a_{12} & a_{22} & a_{32} & \dots & a_{m2} \\ \dots & \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & a_{3n} & \dots & a_{nm} \end{pmatrix}. \tag{3.15}$$

Таким чином, при транспонуванні матриці A її рядки стають стовпцями транспонованої матриці $A^\top$, а стовпці A – рядками матриці $A^\top$. Зокрема,

$$r_{\text{ряд}}(A^\top) = r_{\text{ст}}(A), \qquad r_{\text{ст}}(A^\top) = r_{\text{ряд}}(A). \tag{3.16}$$

За лемою 6 при елементарних перетвореннях рядків матриці $A^\top$ обидва її ранги не змінюються. Але елементарні перетворення рядків матриці $A^\top$ – це фактично елементарні перетворення стовпців матриці A. Тому з леми 6 одразу випливає наслідок.

Наслідок 12. *Обидва ранги матриці не змінюються при елементарних перетвореннях стовпців цієї матриці.*

Теорема 15 (про ранг матриці)**.** *Рядковий $r_{ряд}(A)$ і стовпцевий $r_{ст}(A)$ ранги матриці A збігаються.*

Доведення. Нехай A – це матриця (3.12). Ми вже доводили, що елементарними перетвореннями рядків (і, можливо, перестановками стовпців) матрицю A можна звести до вигляду

$$\begin{pmatrix} 1 & \dots & 0 & \gamma_{1,k+1} & \dots & \gamma_{1n} \\ & \ddots & & \dots & & \\ 0 & \dots & 1 & \gamma_{k,k+1} & \dots & \gamma_{kn} \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}. \tag{3.17}$$

Далі ми можемо зробити нулі в першому рядку, віднімаючи від стовпців із номерами від $k+1$ до n відповідні кратні першого стовпця. Потім, аналогічно, нулі у другому рядку і т. д. Зрештою отримаємо матрицю

$$B = \begin{pmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ & \ddots & & \dots & & \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}, \tag{3.18}$$

в якої на діагоналі стоїть k одиниць, а решта елементів – нулі. Оскільки перші k рядків матриці B лінійно незалежні, а решта рядків – нульові, то перші k рядків матриці B утворюють МЛНЗ-підсистему системи векторів-рядків матриці B. Аналогічно перші k стовпців утворюють МЛНЗ-підсистему системи векторів-стовпців матриці B. Тому $r_{\text{ряд}}(B) = r_{\text{ст}}(B) = k$.

Але ми перейшли від A до B за допомогою елементарних перетворень рядків і стовпців, які не змінюють жодного з рангів матриці. Тому $r_{\text{ряд}}(A) = r_{\text{ст}}(A) = k$. □

Означення 10. *Спільне значення рядкового та стовпцевого рангів матриці A називається* ***рангом матриці*** *A і позначається $r(A)$ (або* $\operatorname{rank}(A)$*).*

Квадратна матриця порядку n називається *виродженою* (або *особливою*), якщо її ранг менший за n. У противному разі така матриця називається *невиродженою* (*неособливою*).

Зауваження. Із доведення теореми про ранг матриці випливає метод обчислення рангу матриці. Для цього початкову матрицю A елементарними перетвореннями рядків і стовпців (порядок виконання перетворень подібний до того, який в алгоритмі Гаусса) зводимо до вигляду (3.18). Кількість отриманих одиниць на діагоналі і буде дорівнювати рангові матриці.

Приклад 7. Обчислимо ранг матриці

$$A = \begin{pmatrix} 2 & -1 & 5 & 7 \\ 4 & -2 & 7 & 5 \\ 2 & -1 & 1 & -5 \end{pmatrix}.$$

Виконуючи елементарні перетворення рядків, робимо нулі під діагоналлю:

$$\begin{pmatrix} 2 & -1 & 5 & 7 \\ 4 & -2 & 7 & 5 \\ 2 & -1 & 1 & -5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & -1 & 1 & -5 \\ 0 & 0 & 5 & 15 \\ 0 & 0 & 4 & 12 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & -1 & 1 & -5 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

На цьому обчислення можна закінчити – зводити далі матрицю до вигляду (3.18) не потрібно. Справді, в останній матриці перші два рядки лінійно незалежні, а третій – нульовий. Тому її рядковий ранг дорівнює 2. Але тоді і $\operatorname{rank}(A) = 2$.

3.4. Підпростір, база і розмірність

Означення 11. ***Підпростором*** *простору P^n будемо називати довільну непорожню підмножину $V \subseteq P^n$, яка замкнена відносно додавання векторів і множення векторів на скаляри, тобто підмножину V, яка задовольняє такі дві умови*:

1) *для довільних $\boldsymbol{a}$, $\boldsymbol{b} \in V$ виконується $\boldsymbol{a} + \boldsymbol{b} \in V$*;

2) *для довільних $\boldsymbol{a} \in V$ та $\alpha \in P$ виконується $\alpha \cdot \boldsymbol{a} \in V$.*

З означення одразу випливає, що весь простір P^n і підмножина, яка складається лише з нульового вектора, будуть підпросторами. Ці два підпростори називаються *тривіальними*. Набагато ширший набір підпросторів дає наступна теорема, яка випливає з твердження 10:

Теорема 16. *Множина розв'язків однорідної СЛР із коефіцієнтами з поля P утворює підпростір простору P^n, де n – кількість невідомих.*

Ще одна серія прикладів підпросторів пов'язана з поняттям лінійної оболонки. Означення 7 лінійної оболонки узагальнюється на довільні підмножини простору P^n. А саме, *лінійною оболонкою* $\mathcal{L}(S)$ (або $\langle S\rangle$) множини $S \subseteq P^n$ називається множина усіх лінійних комбінацій усіх скінченних наборів векторів із S.

Твердження 16. *Для кожної непорожньої підмножини $S \subseteq P^n$ її лінійна оболонка $\mathcal{L}(S)$ є підпростором простору P^n.*

Доведення. Нехай $\boldsymbol{u}$ і $\boldsymbol{v}$ – два довільні вектори з $\mathcal{L}(S)$. Можна вважати, що вони є лінійними комбінаціями однієї й тієї ж скінченної підсистеми з S (завжди до лінійної комбінації можна дописати потрібні доданки з нульовими коефіцієнтами):

$$\boldsymbol{u} = a_1\boldsymbol{w}_1 + a_2\boldsymbol{w}_2 + \ldots + a_k\boldsymbol{w}_k, \qquad \boldsymbol{v} = b_1\boldsymbol{w}_1 + b_2\boldsymbol{w}_2 + \ldots + b_k\boldsymbol{w}_k\,.$$

Тоді

$$c\boldsymbol{u} = (ca_1)\boldsymbol{w}_1 + (ca_2)\boldsymbol{w}_2 + \ldots + (ca_k)\boldsymbol{w}_k \in \mathcal{L}(S)$$

і

$$\boldsymbol{u} + \boldsymbol{v} = (a_1 + b_1)\boldsymbol{w}_1 + (a_2 + b_2)\boldsymbol{w}_2 + \ldots + (a_k + b_k)\boldsymbol{w}_k \in \mathcal{L}(S)\,.$$

Отже, множина $\mathcal{L}(S)$ замкнена відносно додавання і множення на скаляри, а тому є підпростором. □

Означення 12. *Якщо S – така система векторів підпростору $V \subseteq P^n$, що $\mathcal{L}(S) = V$, то S називається* ***системою твірних*** *підпростору V.*

Означення 13. *Лінійно незалежна система твірних векторного підпростору називається його* ***базою*** *(або* ***базисом****).*

Зауважимо, що база є саме системою твірних, а не множиною. Далі ми побачимо, що в багатьох випадках порядок векторів бази є істотним. Зручно також вважати, що базою нульового підпростору є пуста множина.

Вправа 9. *Доведіть, що кожна із систем векторів*

$$а)\ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}; \quad б)\ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}; \quad в)\ \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix}$$

є базою простору $\mathbb{R}^2$.

Оскільки кожна надмножина системи твірних також буде системою твірних, то із вправи 9 випливає, що система твірних (і навіть база) векторного підпростору визначені, взагалі кажучи, неоднозначно.

Теорема 17. *а) Кожен вектор підпростору $V \subseteq P^n$ лінійно виражається через вектори бази підпростору V, причому тільки одним способом.*

б) Кожна максимальна лінійно незалежна система векторів підпростору $V \subseteq P^n$ є його базою. Навпаки, кожна база підпростору V є його максимальною лінійно незалежною підсистемою.

в) Будь-які дві бази підпростору $V \subseteq P^n$ складаються з однакової кількості векторів.

Доведення. а) Це випливає з теореми 10.г. Справді, база $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ є лінійно незалежною системою векторів. Враховуючи, що кожен вектор $\boldsymbol{v} \in V$ лінійно виражається через вектори бази, то система векторів $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{v}$ є лінійно залежною. Тому вектор $\boldsymbol{v}$ лінійно виражається через вектори $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$, причому тільки одним способом.

б) Нехай $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ – максимальна лінійно незалежна система векторів підпростору V, а $\boldsymbol{u}$ – довільний вектор із V. Оскільки система $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n, \boldsymbol{u}$ – лінійно залежна, то за теоремою 10.г вектор $\boldsymbol{u}$ має лінійно виражатися через вектори $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. Із довільності вектора $\boldsymbol{u}$ випливає, що $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ є системою твірних простору V, отже, є базою.

Нехай тепер $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ – база простору V. За означенням бази вона лінійно незалежна. З іншого боку, кожен вектор $\boldsymbol{u} \in V$ лінійно виражається через вектори $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, а тому система $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n, \boldsymbol{u}$ – лінійно залежна. Отже, система $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ є максимальною лінійно незалежною.

в) Це випливає з пункту а) та наслідку 11. □

Із теореми 17 та наслідку 9 із теореми 13 про лінійну залежність маємо такий наслідок.

Наслідок 13. *Будь-яку лінійно незалежну систему векторів підпростору $V \subseteq P^n$ можна доповнити до бази підпростору V.*

Означення 14. *Кількість векторів у базі підпростору $V \subseteq P^n$ називається* ***розмірністю*** *підпростору V і позначається* $\dim V$. *Підпростір розмірності k називають також k-**вимірним**.*

Із теореми 17 та наслідку 10 випливає таке.

Наслідок 14. *Ранг системи векторів збігається з розмірністю лінійної оболонки цієї системи*: $\operatorname{rank}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k) = \dim \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k)$.

Теорема 18 (про бази арифметичного векторного простору)**.**

а) Бази в арифметичному векторному просторі P^n існують.

б) Кожна база простору P^n містить n векторів.

в) Кожна система з n лінійно незалежних векторів є базою простору P^n.

г) Кожна система твірних простору P^n містить підсистему, яка є базою P^n.

д) Кожну лінійно незалежну підсистему простору P^n можна доповнити до бази простору P^n.

Доведення. а) Як показано в прикладі 5.1, система векторів $\boldsymbol{e}_1 = (1, 0, \ldots, 0)$, $\boldsymbol{e}_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $\boldsymbol{e}_n = (0, \ldots, 0, 1)$ є лінійно незалежною. З іншого боку, довільний вектор $\boldsymbol{b} = (\beta_1, \beta_2, \ldots, \beta_n) \in P^n$ лінійно виражається через $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$:

$$\boldsymbol{b} = \beta_1\boldsymbol{e}_1 + \beta_2\boldsymbol{e}_2 + \ldots + \beta_n\boldsymbol{e}_n.$$

Тому вектори $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ утворюють базу простору P^n.

б) Це випливає з пункту а) і теореми 17.б.

в) За наслідком 9 з теореми 13 про лінійну залежність будь-які $n + 1$ векторів у просторі P^n є лінійно залежними. Тому n лінійно незалежних векторів утворюють МЛНЗ-підсистему і, за теоремою 17.а, є базою.

г) Нехай S – система твірних простору P^n, а $\boldsymbol{b}_1, \ldots,$ вектори $\boldsymbol{b}_k$ – її МЛНЗ-підсистема. За твердженням 11 довільний вектор із S лінійно виражається через вектори $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$, а за означенням системи твірних довільний вектор із P^n лінійно виражається через вектори із S. За теоремою 10.в про транзитивність властивості “лінійно виражатися” кожен вектор із P^n буде лінійно виражатися через вектори $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$. Отже, вектори $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ утворюють лінійно незалежну систему твірних, тобто базу.

д) Нехай вектори $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l$ – лінійно незалежні. Якщо ці вектори не утворюють базу, то знайдеться вектор $\boldsymbol{c}_{l+1} \in P^n$, який через них лінійно не виражається. Тоді вектори $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l, \boldsymbol{c}_{l+1}$ також будуть лінійно незалежними. Якщо вони знову не утворюють базу, то розширимо нашу систему ще раз. І так далі. Цей процес не може тривати нескінченно довго, бо будь-які $n + 1$ у просторі P^n є лінійно залежними. Тому на якомусь кроці отримаємо систему лінійно незалежних векторів, через які буде виражатися довільний вектор із P^n, тобто базу. □

Отже, для довільного підпростору $V \subseteq P^n$ маємо $0 \leq \dim V \leq n$, причому $\dim V = 0$ лише тоді, коли $V = \{\boldsymbol{0}\}$, а $\dim V = n$ лише тоді, коли $V = P^n$.

3.5. Застосування до СЛР

Ми ще не раз переконаємося, що поняття вектора, векторного простору, лінійної залежності та похідні від них є дуже корисними. Зокрема, при дослідженні СЛР. Ми вже бачили, що СЛР можна переписати у векторній формі. Переваги такого запису не є зразу очевидними. Але виявляється, що перехід до векторів, по-перше, дає змогу зручно і просто формулювати властивості СЛР та їх розв'язків геометричною мовою, а по-друге, дозволяє спиратися на геометричну інтуїцію.

Розглянемо спочатку *однорідні системи лінійних рівнянь*. За теоремою 16 множина розв'язків однорідної СЛР із коефіцієнтами з поля P утворює векторний підпростір простору P^n, де n – кількість невідомих. База цього підпростору називається *фундаментальною системою розв'язків* (або коротко – ФСР) цієї однорідної СЛР.

Теорема 19 (про будову множини розв'язків однорідної СЛР)**.** *Кожен розв'язок однорідної СЛР записується у вигляді лінійної комбінації розв'язків із ФСР, причому таке зображення однозначне.*

Доведення. Це випливає з означення ФСР і властивостей бази підпростору. □

Якщо однорідна СЛР є невизначеною, то, узагалі кажучи, вона має багато різних ФСР. Ефективний метод знаходження ФСР дає наступна теорема.

Теорема 20 (про хвости)**.** *Якщо $x_{r+1}, x_{r+2}, \ldots, x_n$ – список усіх вільних невідомих однорідної СЛР, то ця система має ФСР вигляду*

$$\begin{array}{rcccccccc} f_1 & = & (c_{11}, & \ldots, & c_{1r}, & 1, & 0, & \ldots, & 0), \\ f_2 & = & (c_{21}, & \ldots, & c_{2r}, & 0, & 1, & \ldots, & 0), \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ f_{n-r} & = & (c_{n-r,1}, & \ldots, & c_{n-r,r}, & 0, & 0, & \ldots, & 1) \end{array} \tag{3.19}$$

(*у розв'язку f_i одиниця в хвості стоїть на $(r+i)$-му місці*).

Доведення. Якщо $x_{r+1}, x_{r+2}, \ldots, x_n$ – список усіх вільних невідомих однорідної СЛР, то з теореми Гаусса (теорема 8) випливає, що елементарними перетвореннями рядків матрицю системи можна звести до трапецієподібного вигляду

$$\left(\begin{array}{cccccc|c} 1 & \dots & 0 & b_{1,r+1} & \dots & b_{1n} & 0 \\ & \ddots & & \dots & & & \dots \\ 0 & \dots & 1 & b_{r,r+1} & \dots & b_{rn} & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{array}\right). \qquad (3.20)$$

Тому загальний розв'язок системи має вигляд

$$(-b_{1,r+1}t_{r+1} - \dots - b_{1n}t_n, \dots, -b_{r,r+1}t_{r+1} - \dots - b_{rn}t_n, t_{r+1}, \dots, t_n). \quad (3.21)$$

Очевидно, що серед цих розв'язків можна вибрати розв'язки $\boldsymbol{f}_1, \dots, \boldsymbol{f}_{n-r}$ потрібного нам вигляду. Якщо лінійна комбінація

$$\alpha_1\boldsymbol{f}_1 + \dots + \alpha_{n-r}\boldsymbol{f}_{n-r} = (d_1, \dots, d_r, \alpha_1, \dots, \alpha_{n-r})$$

цих розв'язків дорівнює $\mathbf{0}$, то $\alpha_1 = \dots = \alpha_{n-r} = 0$. Отже, ці розв'язки лінійно незалежні.

Розглянемо тепер довільний розв'язок $\boldsymbol{f} = (g_1, \dots, g_r, \beta_1, \dots, \beta_{n-r})$ даної системи. Лінійна комбінація

$$\boldsymbol{f}' = \beta_1\boldsymbol{f}_1 + \dots + \beta_{n-r}\boldsymbol{f}_{n-r} = (g'_1, \dots, g'_r, \beta_1, \dots, \beta_{n-r})$$

розв'язків $\boldsymbol{f}_1, \dots, \boldsymbol{f}_{n-r}$ також є розв'язком системи, як і різниця

$$\boldsymbol{f} - \boldsymbol{f}' = (g_1 - g'_1, \dots, g_r - g'_r, 0, \dots, 0).$$

Але з вигляду загального розв'язку (3.21) зрозуміло, що коли всі вільні невідомі набувають значення 0, то $x_1, \dots, x_r$ також дорівнюють 0. Отже, $\boldsymbol{f} - \boldsymbol{f}' = \mathbf{0}$ і $\boldsymbol{f}' = \beta_1\boldsymbol{f}_1 + \dots + \beta_{n-r}\boldsymbol{f}_{n-r}$.

Таким чином, розв'язки $\boldsymbol{f}_1, \dots, \boldsymbol{f}_{n-r}$ утворюють лінійно незалежну систему твірних простору розв'язків даної однорідної СЛР , тобто її ФСР. □

Оскільки ненульові рядки матриці (3.20) лінійно незалежні, то її ранг дорівнює r. Звідси одразу випливає такий наслідок.

Наслідок 15. *Розмірність підпростору розв'язків* (тобто кількість розв'язків у ФСР) *однорідної СЛР дорівнює $n - r$, де n – кількість невідомих, а r – ранг матриці системи. Зокрема, однорідна СЛР буде визначеною тоді й лише тоді, коли $n = r$, тобто, коли стовпці її основної матриці лінійно незалежні.*

Наслідок 16. *Кількість вільних невідомих не залежить від способу зведення СЛР до трапецієподібного вигляду.*

Нехай $\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_{n-r}$ – ФСР однорідної СЛР. Оскільки ФСР є базою підпростору розв'язків, то кожен розв'язок $\boldsymbol{u}$ цієї ОСЛР можна зобразити у вигляді лінійної комбінації розв'язків $\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots, \boldsymbol{f}_{n-r}$:

$$\boldsymbol{u} = t_1\boldsymbol{f}_1 + t_2\boldsymbol{f}_2 + \ldots + t_{n-r}\boldsymbol{f}_{n-r}. \tag{3.22}$$

Зображення розв'язку ОСЛР у вигляді рівності (3.22) із невизначеними коефіцієнтами $t_1, t_2, \ldots, t_{n-r}$ також будемо називати *загальним розв'язком* цієї ОСЛР .

Розглянемо на прикладі метод знаходження ФСР , описаний в доведенні теореми про хвости.

Приклад 8. Знайдемо ФСР та загальний розв'язок ОСЛР

$$\begin{array}{rcrcrcrcrcl} x_1 & + & 3x_2 & + & 2x_3 & + & 3x_4 & & & = & 0, \\ 2x_1 & + & 6x_2 & + & 5x_3 & + & 8x_4 & - & x_5 & = & 0, \\ 3x_1 & + & 9x_2 & + & 5x_3 & + & 7x_4 & & & = & 0, \\ x_1 & + & 3x_2 & + & 5x_3 & + & 9x_4 & - & 3x_5 & = & 0. \end{array} \tag{3.23}$$

Елементарними перетвореннями рядків зводимо матрицю нашої системи до спеціальної трапецієподібної форми:

$$\left(\begin{array}{ccccc|c} 1 & 3 & 2 & 3 & 0 & 0 \\ 2 & 6 & 5 & 8 & -1 & 0 \\ 3 & 9 & 5 & 7 & 1 & 0 \\ 1 & 3 & 5 & 9 & -3 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccccc|c} 1 & 3 & 2 & 3 & 0 & 0 \\ 0 & 0 & 1 & 2 & -1 & 0 \\ 0 & 0 & -1 & -2 & 1 & 0 \\ 0 & 0 & 3 & 6 & -3 & 0 \end{array}\right) \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{ccccc|c} 1 & 3 & 2 & 3 & 0 & 0 \\ 0 & 0 & 1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccccc|c} 1 & 3 & 0 & -1 & 2 & 0 \\ 0 & 0 & 1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Із вигляду останньої матриці випливає, що вільними невідомими є x_2, x_4, x_5 і

$$x_1 = -3x_2 + x_4 - 2x_5, \qquad x_3 = -2x_4 + x_5. \tag{3.24}$$

ФСР зручно виписувати у вигляді таблиці, стовпці якої нумеруються невідомими. Спочатку по черзі надаємо одній із вільних невідомих

значення 1, а решті вільних невідомих – значення 0:

x_1	x_2	x_3	x_4	x_5
	1		0	0
	0		1	0
	0		0	1

.

Потім із рівностей (3.24) обчислюємо значення решти невідомих:

x_1	x_2	x_3	x_4	x_5
-3	1	0	0	0
1	0	-2	1	0
-2	0	1	0	1

.

Розв'язкам із фундаментальної системи відповідають рядки таблиці: $\boldsymbol{f}_1 = (-3, 1, 0, 0, 0), \boldsymbol{f}_2 = (1, 0, -2, 1, 0), \boldsymbol{f}_3 = (-2, 0, 1, 0, 1)$. Тому загальний розв'язок має вигляд $t_1\boldsymbol{f}_1 + t_2\boldsymbol{f}_2 + t_3\boldsymbol{f}_3$, де t_1, t_2, t_3 – довільні.

Справедлива і теорема 21, обернена до теореми 16:

Теорема 21 (про вигляд підпросторів простору P^n)**.** *Довільний підпростір V арифметичного векторного простору P^n є множиною розв'язків деякої однорідної системи лінійних рівнянь.*

Доведення. Нехай базою підпростору V слугує система векторів $\boldsymbol{u}_1 = (\alpha_{11}, \ldots, \alpha_{1n}), \ldots, \boldsymbol{u}_k = (\alpha_{k1}, \ldots, \alpha_{kn})$, де $k = \dim V$. Розглянемо таку ОСЛР:

$$\begin{array}{ccccccc} \alpha_{11}x_1 & + & \ldots & + & \alpha_{1n}x_n & = & 0, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{k1}x_1 & + & \ldots & + & \alpha_{kn}x_n & = & 0. \end{array} \tag{3.25}$$

Вектор-рядки $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ матриці системи (3.25) є лінійно незалежними, бо утворюють базу підпростору V. Тому ранг матриці цієї системи дорівнює k, а ФСР буде складатися із $r = n - k$ розв'язків.

Нехай $\boldsymbol{f}_1 = (\beta_{11}, \ldots, \beta_{1n}), \ldots, \boldsymbol{f}_r = (\beta_{r1}, \ldots, \beta_{rn})$ – ФСР системи (3.25). Це, зокрема, означає, що для довільних i $(1 \le i \le k)$ та j $(1 \le j \le r)$ виконується рівність

$$\alpha_{i1}\beta_{j1} + \alpha_{i2}\beta_{j2} + \ldots + \alpha_{in}\beta_{jn} = 0. \tag{3.26}$$

Розглянемо тепер ОСЛР

$$\begin{array}{ccccccc} \beta_{11}x_1 & + & \ldots & + & \beta_{1n}x_n & = & 0, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_{r1}x_1 & + & \ldots & + & \beta_{rn}x_n & = & 0. \end{array} \tag{3.27}$$

Її ранг дорівнює r, а тому її ФСР буде складатися з $n - r = k$ розв'язків. Тому підпростір W розв'язків системи (3.27) має розмірність k. Із рівностей (3.26) випливає, що кожен із векторів $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ є розв'язком системи (3.27), отже, належить підпростору W. Позаяк їх кількість дорівнює розмірності підпростору W і вони лінійно незалежні, то вони утворюють базу W. Тому $W = \mathcal{L}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = V$. □

Розглянемо тепер *неоднорідні системи лінійних рівнянь*.

Теорема 22 (про загальний розв'язок неоднорідної СЛР)**.** *Різниця довільних двох розв'язків неоднорідної СЛР S є розв'язком відповідної однорідної системи. Навпаки, сума фіксованого розв'язку системи S і довільного розв'язку відповідної однорідної системи буде розв'язком системи S, причому кожен розв'язок системи S можна одержати саме таким чином.*

Доведення. Запишемо неоднорідну систему S у векторній формі:

$$x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_n\boldsymbol{a}_n = \boldsymbol{b}. \tag{3.28}$$

Тоді відповідна їй однорідна СЛР має вигляд

$$x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + \ldots + x_n\boldsymbol{a}_n = \boldsymbol{0}. \tag{3.29}$$

Нехай $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ і $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ – два розв'язки системи (3.28). Тоді

$$u_1\boldsymbol{a}_1 + u_2\boldsymbol{a}_2 + \ldots + u_n\boldsymbol{a}_n = \boldsymbol{b},$$
$$v_1\boldsymbol{a}_1 + v_2\boldsymbol{a}_2 + \ldots + v_n\boldsymbol{a}_n = \boldsymbol{b}.$$

Віднімаючи від першої рівності другу, одержуємо

$$(u_1 - v_1)\boldsymbol{a}_1 + (u_2 - v_2)\boldsymbol{a}_2 + \ldots + (u_n - v_n)\boldsymbol{a}_n = \boldsymbol{0}.$$

Отже, різниця $\boldsymbol{u} - \boldsymbol{v}$ є розв'язком однорідної системи (3.29).

Нехай тепер $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ – фіксований розв'язок неоднорідної системи (3.28), а $\boldsymbol{w} = (w_1, w_2, \ldots, w_n)$ – розв'язок відповідної однорідної системи (3.29). Тоді

$$w_1\boldsymbol{a}_1 + w_2\boldsymbol{a}_2 + \ldots + w_n\boldsymbol{a}_n = \boldsymbol{0},$$

звідки

$$(u_1 + w_1)\boldsymbol{a}_1 + (u_2 + w_2)\boldsymbol{a}_2 + \ldots + (u_n + w_n)\boldsymbol{a}_n =$$
$$= (u_1\boldsymbol{a}_1 + u_2\boldsymbol{a}_2 + \ldots + u_n\boldsymbol{a}_n) + (w_1\boldsymbol{a}_1 + w_2\boldsymbol{a}_2 + \ldots + w_n\boldsymbol{a}_n) = \boldsymbol{b} + \boldsymbol{0} = \boldsymbol{b}.$$

Отже, сума $\boldsymbol{u} + \boldsymbol{w}$ є розв'язком неоднорідної системи (3.28).

Нарешті, довільний розв'язок $\boldsymbol{u}'$ системи (3.28) можна записати у вигляді $\boldsymbol{u}' = \boldsymbol{u} + (\boldsymbol{u}' - \boldsymbol{u})$, де другий доданок $\boldsymbol{u}' - \boldsymbol{u}$, як доведено вище, є розв'язком однорідної системи (3.29). □

Зауважимо, що теорему 22 ще називають *теоремою про зв'язок між розв'язками неоднорідної СЛР і відповідної однорідної СЛР*.

Хоча множини розв'язків неоднорідних систем лінійних рівнянь підпросторів не утворюють, вони також мають природну геометричну інтерпретацію. Нам знадобиться поняття лінійного многовиду.

Означення 15. ***Лінійним многовидом*** *із представником* $\boldsymbol{v} \in P^n$ *і напрямним підпростором* $U \subseteq P^n$ *називається множина*

$$\boldsymbol{v} + U := \{\boldsymbol{v} + \boldsymbol{u} \mid \boldsymbol{u} \in U\}.$$

Твердження 17. *Два лінійні многовиди* $\boldsymbol{v}_1 + U_1$ *і* $\boldsymbol{v}_2 + U_2$ *простору* P^n *збігаються тоді й лише тоді, коли* $U_1 = U_2$ *і* $\boldsymbol{v}_2 - \boldsymbol{v}_1 \in U_1$.

Доведення. Необхідність. Нехай $\boldsymbol{v}_1 + U_1 = \boldsymbol{v}_2 + U_2$. Тоді знайдуться такі $\boldsymbol{u}_1' \in U_1$, $\boldsymbol{u}_2' \in U_2$, що

$$\boldsymbol{v}_1 + \boldsymbol{0} = \boldsymbol{v}_1 = \boldsymbol{v}_2 + \boldsymbol{u}_2', \quad \boldsymbol{v}_2 + \boldsymbol{0} = \boldsymbol{v}_2 = \boldsymbol{v}_1 + \boldsymbol{u}_1'.$$

Тому $\boldsymbol{v}_2 - \boldsymbol{v}_1 = \boldsymbol{u}_1' = -\boldsymbol{u}_2' \in U_1 \cap U_2$.

Розглянемо тепер довільний вектор $\boldsymbol{u}_1 \in U_1$. Із рівності многовидів $\boldsymbol{v}_1 + U_1$ і $\boldsymbol{v}_2 + U_2$ випливає, що знайдеться такий $\boldsymbol{u}_2 \in U_2$, що $\boldsymbol{v}_1 + \boldsymbol{u}_1 = \boldsymbol{v}_2 + \boldsymbol{u}_2$. Але тоді $\boldsymbol{u}_1 = (\boldsymbol{v}_2 - \boldsymbol{v}_1) + \boldsymbol{u}_2 \in U_2$ як сума двох векторів із U_2. Тому $U_1 \subseteq U_2$. Аналогічно доводиться включення $U_2 \subseteq U_1$. Отже, $U_1 = U_2$.

Достатність. Нехай $U_1 = U_2$ і $\boldsymbol{v}_2 - \boldsymbol{v}_1 = \boldsymbol{u} \in U_1 = U_2$. Тоді для довільного $\boldsymbol{u}_1 \in U_1$ матимемо

$$\boldsymbol{v}_1 + \boldsymbol{u}_1 = \boldsymbol{v}_2 + (\boldsymbol{u}_1 - \boldsymbol{v}_2 + \boldsymbol{v}_1) = \boldsymbol{v}_2 + (\boldsymbol{u}_1 - \boldsymbol{u}) \in \boldsymbol{v}_2 + U_2,$$

бо $\boldsymbol{u}_1 - \boldsymbol{u} \in U_2$. Отже, $\boldsymbol{v}_1 + U_1 \subseteq \boldsymbol{v}_2 + U_2$. Аналогічно доводиться зворотне включення. Тому $\boldsymbol{v}_1 + U_1 = \boldsymbol{v}_2 + U_2$. □

Зауваження. 1. Із теореми 17 випливає, що напрямний підпростір U лінійного многовиду $\boldsymbol{v} + U$ визначається однозначно, а за представника многовиду можна брати довільний вектор з нього.

2. Оскільки напрямний підпростір U визначається однозначно, то можна говорити про *розмірність* многовиду, яка визначається як розмірність підпростору U.

3. Многовиди розмірності один часто називають *прямими*, а розмірності два – *площинами*.

Приклади лінійних многовидів.

1. Прямі на координатній площині $\mathbb{R}^2$.

2. Прямі та площини у просторі $\mathbb{R}^3$.

3. Частковим випадком лінійних многовидів є підпростори: напрямним підпростором треба брати сам підпростір, а представником – нульовий вектор.

4. Із теореми 22 випливає, що лінійний многовид утворюватиме множина розв'язків неоднорідної СЛР: представником цього многовиду буде довільний фіксований розв'язок цієї СЛР, а напрямним підпростором – підпростір розв'язків відповідної ОСЛР.

Справедлива і теорема, обернена до останнього прикладу.

Теорема 23 (про вигляд лінійних многовидів простору P^n)**.** *Довільний лінійний многовид арифметичного векторного простору P^n є множиною розв'язків деякої системи лінійних рівнянь з n невідомими.*

Доведення. Нехай $\boldsymbol{c} + U$ – лінійний многовид, де $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in P^n$, $U \subseteq P^n$. Тоді за теоремою 21 U є множиною розв'язків деякої однорідної системи лінійних рівнянь

$$\boldsymbol{a}_1 x_1 + \ldots + \boldsymbol{a}_n x_n = \boldsymbol{0}. \tag{3.30}$$

Розглянемо тепер СЛР

$$\boldsymbol{a}_1 x_1 + \ldots + \boldsymbol{a}_n x_n = \boldsymbol{b}, \tag{3.31}$$

де $\boldsymbol{b} = \boldsymbol{a}_1 c_1 + \boldsymbol{a}_2 c_2 \ldots + \boldsymbol{a}_n c_n$. Тоді вектор $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ є розв'язком СЛР 3.31, а U – підпростором розв'язків відповідної однорідної СЛР (3.30). □

Приклад 9. Знайдемо множину розв'язків СЛР

$$\begin{array}{rcrcrcl} x_1 & + & 2x_2 & + & x_3 & = & 1, \\ x_1 & + & x_2 & - & x_3 & = & 0. \end{array} \tag{3.32}$$

Можна помітити, що частковим розв'язком системи (3.32) є, наприклад, вектор $(2, -1, 1)$. Знайдемо підпростір розв'язків відповідної однорідної СЛР:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 1 & 1 & -1 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & -1 & -2 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & -3 & 0 \\ 0 & 1 & 2 & 0 \end{array}\right).$$

Вільною невідомою є x_3, тому ФСР складатиметься з одного розв'язку, наприклад, $(3, -2, 1)$. Множиною розв'язків однорідної СЛР буде породжений цим вектором підпростір $U = \mathcal{L}((3, -2, 1))$, а множиною розв'язків початкової неоднорідної СЛР – лінійний многовид

$$(2, -1, 1) + \mathcal{L}((3, -2, 1)).$$

У теоретичних міркуваннях часто буває достатньо знати лише тип СЛР , тобто чи є вона сумісною, а якщо є, то чи буде визначеною. Для цього бажано мати такі критерії сумісності і визначеності, які б не вимагали зведення системи до трапецієподібного вигляду, а тим більше повного її розв'язання. Такі критерії можна дати в термінах рангів матриць системи.

Теорема 24 (перша теорема Кронекера – Капеллі – критерій сумісності СЛР)**.** *СЛР сумісна тоді і тільки тоді, коли ранг основної матриці системи дорівнює рангові розширеної матриці.*

Доведення. Необхідність. Нехай система (2.1) – сумісна і $(x_1^\circ, x_2^\circ, \ldots, x_n^\circ)$ – якийсь її розв'язок. Тоді $\boldsymbol{a}_1 x_1^\circ + \boldsymbol{a}_2 x_2^\circ + \ldots + \boldsymbol{a}_n x_n^\circ = \boldsymbol{b}$, отже, стовпець $\boldsymbol{b}$ вільних членів є лінійною комбінацією стовпців $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$. Тому $\boldsymbol{b} \in \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$, звідки $\mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b})$ і $\dim \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \dim \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b})$. Оскільки ранг системи векторів збігається з розмірністю лінійної оболонки цієї системи, то

$$\operatorname{rank} \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \operatorname{rank} \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b})\,.$$

Але число зліва є рангом основної матриці СЛР (2.1), а число справа – рангом розширеної матриці.

Достатність. Навпаки, якщо ранг основної матриці СЛР (2.1) збігається з рангом розширеної матриці, то

$$\operatorname{rank} \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \operatorname{rank} \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b})$$

і

$$\dim \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \dim \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b}).$$

Оскільки $\mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) \subseteq \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b})$, то з рівності розмірностей випливає, що $\mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n, \boldsymbol{b})$. Але тоді $\boldsymbol{b} \in \mathcal{L}(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$, тобто існують такі коефіцієнти $x_1^\circ, x_2^\circ, \ldots, x_n^\circ$, що $\boldsymbol{a}_1 x_1^\circ + \boldsymbol{a}_2 x_2^\circ + \ldots + \boldsymbol{a}_n x_n^\circ = \boldsymbol{b}$. Останнє означає, що набір $(x_1^\circ, x_2^\circ, \ldots, x_n^\circ)$ є розв'язком СЛР (2.1), а тому вона сумісна. □

Теорема 25 (друга теорема Кронекера – Капеллі – критерій визначеності СЛР)**.** *СЛР визначена тоді і тільки тоді, коли ранг основної матриці системи дорівнює рангові розширеної матриці і дорівнює кількості невідомих.*

Доведення. Враховуючи попередню теорему і те, що визначена система є сумісною, досить довести, що сумісна СЛР є визначеною тоді і тільки тоді, коли ранг основної матриці системи дорівнює кількості невідомих. За теоремою про будову загального розв'язку СЛР (теорема 22) кількість розв'язків сумісної СЛР збігається з кількістю розв'язків відповідної однорідної СЛР . А за теоремою 19 розв'язки останньої утворюють векторний підпростір розмірності $n - r$, де n – кількість невідомих, а r – ранг основної матриці системи. Тому відповідна ОСЛР матиме єдиний розв'язок тоді й лише тоді, коли $n - r = 0$, тобто, коли $n = r$. Отже, і початкова сумісна СЛР буде визначеною тоді й лише тоді, коли $n = r$. □

3.6. Задачі

3.1. а) Доведіть, що система векторів буде лінійно незалежною тоді й лише тоді, коли кожний вектор, що лінійно виражається через цю систему, виражається через неї єдиним чином.

б) Чи можна в умові задачі слово "кожний" замінити на "хоча б один"?

3.2. Нехай A – невироджена $(0, 1)$-матриця порядку n. Чи залишиться вона невиродженою, якщо всі одиниці замінити довільними додатними числами?

3.3. Нехай A – матриця порядку $m \times n$. Доведіть, що СЛР із основною матрицею A

а) буде сумісною для довільного стовпця вільних членів $\boldsymbol{b}$ тоді й лише тоді, коли $\operatorname{rank} A = m$;

б) матиме не більше одного розв'язку для кожного стовпця вільних членів $\boldsymbol{b}$ тоді й лише тоді, коли $\operatorname{rank} A = n$;

в) не буде визначеною для жодного не більше одного розв'язку $\boldsymbol{b}$ тоді й лише тоді, коли $\operatorname{rank} A < n$;

г) буде визначеною для кожного не більше одного розв'язку $\boldsymbol{b}$ тоді й лише тоді, коли $\operatorname{rank} A = n = m$.

3.4. Доведіть, що для квадратної СЛР завжди виконується *альтернатива Фредгольма*: або ця СЛР сумісна при довільному стовпцеві вільних членів, або відповідна однорідна СЛР має ненульовий розв'язок.

3.5. Знайдіть необхідну й достатню умову, щоб три прямі $a_1x+b_1y=c_1$, $a_2x+b_2y=c_2$, $a_3x+b_3y=c_3$ проходили через одну точку.

3.6.* Те, що крива другого порядку

$$a_{11}x^2+2a_{12}xy+a_{22}y^2+2a_{13}x+2a_{23}y+a_{33}=0$$

проходить через точку $M_0(x_0,y_0)$, означає виконання рівності

$$a_{11}x_0^2+2a_{12}x_0y_0+a_{22}y_0^2+2a_{13}x_0+2a_{23}y_0+a_{33}=0\,,$$

на яку можна дивитися як на лінійне однорідне рівняння відносно невідомих a_{11}, a_{12}, a_{22}, a_{13}, a_{23}, a_{33}. Візьмемо тепер 5 точок M_1, M_2, M_3, M_4, M_5 і для кожної випишемо відповідне рівняння. Доведіть, що отримані рівняння будуть лінійно незалежні тоді й лише тоді, коли жодні 4 із цих точок не лежать на одній прямій.

4. Алгебра матриць

4.1. Лінійні відображення

Прямокутні матриці зустрічаються в математиці настільки часто, що виник самостійний розділ математики – теорія матриць. Ми вже трішки зачепили цю теорію, коли говорили про ранг матриці. Для глибшого вивчення як властивостей самих матриць, так і їх застосувань, дуже зручною є геометрична мова, до викладу якої ми й переходимо.

Нехай P^n і P^m – два арифметичні векторні простори над полем P розмірностей n і m відповідно. Відображення $\varphi : P^n \to P^m$ називається *лінійним*, якщо воно задовольняє такі дві умови:

1) $\varphi(\boldsymbol{\nu}_1 + \boldsymbol{\nu}_2) = \varphi(\boldsymbol{\nu}_1) + \varphi(\boldsymbol{\nu}_2)$ для довільних векторів $\boldsymbol{\nu}_1, \boldsymbol{\nu}_2 \in P^n$;
2) $\varphi(\lambda\boldsymbol{\nu}) = \lambda\varphi(\boldsymbol{\nu})$ для довільних вектора $\boldsymbol{\nu} \in P^n$ і скаляра $\lambda \in P$.

Лінійне відображення $\varphi : P^n \to P^n$ простору P^n у себе називають ще *лінійним перетворенням* простору P^n або *лінійним оператором* у просторі P^n.

Приклад 10. 1. Нехай $n \geq m$. Легко перевіряється, що відображення

$$P^n \to P^m, \quad (a_1, a_2, \ldots, a_n) \mapsto (a_1, a_2, \ldots, a_m)$$

є лінійним. Воно називається *проектуванням* простору P^n на перші m координат.

2. Із рівностей

$$\alpha(\boldsymbol{\nu}_1 + \boldsymbol{\nu}_2) = \alpha\boldsymbol{\nu}_1 + \alpha\boldsymbol{\nu}_2, \quad \alpha(\lambda\boldsymbol{\nu}) = \lambda(\alpha\boldsymbol{\nu})$$

випливає, що для довільного фіксованого скаляра α перетворення

$$P^n \to P^n, \quad \boldsymbol{\nu} \mapsto \alpha\boldsymbol{\nu},$$

є лінійним. Це перетворення називається *гомотетією* простору P^n із коефіцієнтом α.

3. Якщо ототожнити простір $\mathbb{R}^2$ із площиною з фіксованою на ній прямокутною системою координат, то поворот площини навколо центра координат на даний кут φ є лінійним перетворенням простору $\mathbb{R}^2$. Справді, при такому повороті довільне кратне кожного вектора також повертається на кут φ, і якщо кожен із доданків повернути на кут φ, то їх сума також повернеться на кут φ.

Вправа 10. *Перевірте, що для довільних дійсних чисел a, b, c, d перетворення $(x, y) \mapsto (ax + by, cx + dy)$ простору $\mathbb{R}^2$ буде лінійним.*

Із кожним лінійним відображенням $\varphi : P^n \to P^m$ пов'язуються дві множини: *ядро*

$$\operatorname{Ker}\varphi := \{\boldsymbol{v} \in P^n \mid \varphi(\boldsymbol{v}) = \mathbf{0}\}$$

відображенням φ та *образ*

$$\operatorname{Im}\varphi := \{\boldsymbol{w} \in P^m \mid \text{існує такий } \boldsymbol{v} \in P^n, \text{ що } \varphi(\boldsymbol{v}) = \boldsymbol{w}\}$$

відображення φ.

Оскільки для кожного лінійного відображення $\varphi : P^n \to P^m$ маємо

$$\varphi(\mathbf{0}) = \varphi(0 \cdot \mathbf{0}) = 0 \cdot \varphi(\mathbf{0}) = \mathbf{0},$$

то нульовий вектор простору P^n належить ядру $\operatorname{Ker}\varphi$, а нульовий вектор простору P^m – образу $\operatorname{Im}\varphi$. Зокрема, кожна із множин $\operatorname{Ker}\varphi$ і $\operatorname{Im}\varphi$ не є пустою.

Твердження 18. *Ядро* $\operatorname{Ker}\varphi$ *лінійного відображення* $\varphi : P^n \to P^m$ *є підпростором простору* P^n*, а образ* $\operatorname{Im}\varphi$ *– підпростором простору* P^m.

Доведення. 1) Нехай $\boldsymbol{v}_1$ і $\boldsymbol{v}_2$ – довільні вектори з $\operatorname{Ker}\varphi$, а $\alpha \in P$ – довільний скаляр. Тоді

$$\varphi(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \varphi(\boldsymbol{v}_1) + \varphi(\boldsymbol{v}_2) = \mathbf{0} + \mathbf{0} = \mathbf{0} \quad \text{і} \quad \varphi(\alpha\boldsymbol{v}_1) = \alpha\varphi(\boldsymbol{v}_1) = \alpha \cdot \mathbf{0} = \mathbf{0}.$$

Тому $\boldsymbol{v}_1 + \boldsymbol{v}_2 \in \operatorname{Ker}\varphi$ і $\alpha\boldsymbol{v}_1 \in \operatorname{Ker}\varphi$. Отже, множина $\operatorname{Ker}\varphi$ є замкненою відносно додавання векторів і множення на скаляри, а тому є підпростором простору P^n.

2) Нехай $\boldsymbol{w}_1$ і $\boldsymbol{w}_2$ – довільні вектори з $\operatorname{Im}\varphi$. Тоді існують такі вектори $\boldsymbol{v}_1, \boldsymbol{v}_2 \in P^n$, що $\varphi(\boldsymbol{v}_1) = \boldsymbol{w}_1$, $\varphi(\boldsymbol{v}_2) = \boldsymbol{w}_2$. Тому

$$\varphi(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \varphi(\boldsymbol{v}_1) + \varphi(\boldsymbol{v}_2) = \boldsymbol{w}_1 + \boldsymbol{w}_2.$$

Отже, $\boldsymbol{w}_1 + \boldsymbol{w}_2 \in \operatorname{Im}\varphi$, а тому множина $\operatorname{Im}\varphi$ є замкненою відносно додавання векторів. Крім того, для довільного скаляра $\alpha \in P$ маємо

$$\varphi(\alpha\boldsymbol{v}_1) = \alpha\varphi(\boldsymbol{v}_1) = \alpha\boldsymbol{w}_1,$$

що доводить замкненість $\operatorname{Im}\varphi$ відносно множення на скаляри. Тому $\operatorname{Im}\varphi$ є підпростором простору P^m. □

Вимога лінійності накладає дуже сильні обмеження на відображення $\varphi : P^n \to P^m$:

Твердження 19. *Лінійне відображення* $\varphi : P^n \to P^m$ *повністю визначається своїми значеннями на векторах бази* $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ *простору* P^n.

Доведення. Довільний вектор $\boldsymbol{v} = (x_1, x_2, \ldots, x_n)$ простору P^n ми можемо записати у вигляді лінійної комбінації бази $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ простору P^n:

$$\boldsymbol{v} = x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \ldots + x_n\boldsymbol{e}_n.$$

Це дозволяє знайти образ вектора $\boldsymbol{v}$:

$$\varphi(\boldsymbol{v}) = \varphi(x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \ldots + x_n\boldsymbol{e}_n) = \varphi(x_1\boldsymbol{e}_1) + \varphi(x_2\boldsymbol{e}_2) + \ldots + \varphi(x_n\boldsymbol{e}_n) = \\ = x_1\varphi(\boldsymbol{e}_1) + x_2\varphi(\boldsymbol{e}_2) + \ldots + x_n\varphi(\boldsymbol{e}_n). \qquad \square$$

Твердження 19 дає дуже зручний спосіб задання лінійних відображень матрицями. Справді, якщо

$$\varphi(\boldsymbol{e}_1) = (a_{11}, a_{21}, \ldots, a_{m1}), \quad \varphi(\boldsymbol{e}_2) = (a_{12}, a_{22}, \ldots, a_{m2}), \quad \ldots \\ \ldots, \quad \varphi(\boldsymbol{e}_n) = (a_{1n}, a_{2n}, \ldots, a_{mn}),$$

то ми можемо розглянути матрицю

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}, \tag{4.1}$$

стовпцями якої є образи базових векторів при відображенні φ. Матриця (4.1) називається *матрицею лінійного відображення* $\varphi : P^n \to P^m$ і позначається A_φ або $[\varphi]$.

Твердження 20. *Існує взаємно однозначна відповідність між лінійними відображеннями* $\varphi : P^n \to P^m$ *та матрицями розміром* $m \times n$ *із коефіцієнтами з поля* P.

Доведення. Кожному лінійному відображенню $\varphi : P^n \to P^m$ поставимо у відповідність його матрицю $[\varphi]$. Рівність $[\varphi_1] = [\varphi_2]$ означає, що для кожного базового вектора $\boldsymbol{e}_i$ простору P^n виконується рівність $\varphi_1(\boldsymbol{e}_i) = \varphi_2(\boldsymbol{e}_i)$. Але тоді із твердження 19 випливає, що $\varphi_1 = \varphi_2$. Отже, відображення $\varphi \mapsto [\varphi]$ є ін'єктивним.

Розглянемо тепер довільну матрицю A вигляду (4.1) і покладемо

$$\varphi(\boldsymbol{e}_1) = (a_{11}, a_{21}, \ldots, a_{m1}), \quad \varphi(\boldsymbol{e}_2) = (a_{12}, a_{22}, \ldots, a_{m2}), \quad \ldots$$
$$\ldots, \quad \varphi(\boldsymbol{e}_n) = (a_{1n}, a_{2n}, \ldots, a_{mn}).$$

Далі для довільного вектора $\boldsymbol{v} = (x_1, x_2, \ldots, x_n)$ покладемо

$$\varphi(\boldsymbol{v}) = x_1\varphi(\boldsymbol{e}_1) + x_2\varphi(\boldsymbol{e}_2) + \ldots + x_n\varphi(\boldsymbol{e}_n).$$

Легко перевірити, що визначене таким чином відображення $\varphi : P^n \to P^m$ є лінійним, а з його побудови одразу випливає, що $[\varphi] = A$. Отже, відображення $\varphi \mapsto [\varphi]$ є сюр'єктивним.

Таким чином, відображення $\varphi \mapsto [\varphi]$ є бієкцією між множиною всіх лінійних відображень $\varphi : P^n \to P^m$ та множиною всіх матриць розміром $m \times n$ із коефіцієнтами з поля P. □

Над лінійними відображеннями можна визначити такі природні дії:

а) *додавання* відображень $\varphi : P^n \to P^m$ і $\psi : P^n \to P^m$:

$$(\varphi + \psi)(\boldsymbol{v}) := \varphi(\boldsymbol{v}) + \psi(\boldsymbol{v})$$

(результат – відображення $(\varphi + \psi) : P^n \to P^m$ – називається *сумою* відображень φ і ψ);

б) *множення відображення* φ *на скаляр* c:

$$(c\varphi)(\boldsymbol{v}) := c\varphi(\boldsymbol{v})$$

(результат – відображення $(c\varphi) : P^n \to P^m$ – називається *кратним* відображення φ);

в) *множення* відображень $\mu : P^m \to P^k$ і $\varphi : P^n \to P^m$:

$$(\mu \circ \varphi)(\boldsymbol{v}) := \mu(\varphi(\boldsymbol{v}))$$

(результат – відображення $(\mu \circ \varphi) : P^n \to P^k$ – називається *добутком* відображень μ і φ). Множення відображень ще називають *композицією* або *суперпозицією* відображень[10].

Зауважимо, що додавати можна не довільні лінійні відображення, а лише ті, які визначені на тому самому просторі і набувають значень у тому самому просторі. Аналогічно при множенні лінійних відображень

[10] Для добутку відображень μ і φ поруч із позначенням $\mu \circ \varphi$ часто вживають позначення $\varphi\mu$. Звертаємо увагу на важливу деталь: при записі добутку як $\mu \circ \varphi$ першим виконується правий множник, а при записі $\varphi\mu$ – лівий множник.

другий множник повинен бути визначеним на тому самому просторі, в якому набуває значень перший множник. Але, якщо розглядаються лінійні перетворення фіксованого простору, то жодних обмежень на дії нема.

Твердження 21. *Сума, кратне і добуток лінійних відображень знову є лінійними відображеннями.*

Доведення. Доведемо тільки лінійність добутку лінійних відображень (лінійність суми і кратного доводиться аналогічно). Отже, нехай $\mu : P^m \to P^k$ і $\varphi : P^n \to P^m$ – два лінійні відображення. Тоді

$$(\mu \circ \varphi)(\boldsymbol{\nu}_1 + \boldsymbol{\nu}_2) = \mu(\varphi(\boldsymbol{\nu}_1 + \boldsymbol{\nu}_2)) = \mu(\varphi(\boldsymbol{\nu}_1) + \varphi(\boldsymbol{\nu}_2)) =$$
$$= \mu(\varphi(\boldsymbol{\nu}_1)) + \mu(\varphi(\boldsymbol{\nu}_2)) = (\mu \circ \varphi)(\boldsymbol{\nu}_1) + (\mu \circ \varphi)(\boldsymbol{\nu}_2).$$

Аналогічно

$$(\mu \circ \varphi)(\lambda\boldsymbol{\nu}) = \mu(\varphi(\lambda\boldsymbol{\nu})) = \mu(\lambda\varphi(\boldsymbol{\nu})) = \lambda\mu(\varphi(\boldsymbol{\nu})) = \lambda(\mu \circ \varphi)(\boldsymbol{\nu}).$$

Отже, обидві умови лінійності відображення виконані. □

Твердження 22. *Для довільних лінійних відображень* φ, ψ *і* μ *та скаляра* c *виконуються такі рівності*:

а) $c(\varphi \circ \psi) = (c\varphi) \circ \psi = \varphi \circ (c\psi)$;

б) $\varphi \circ (\psi + \mu) = \varphi \circ \psi + \varphi \circ \mu$, $(\varphi + \psi) \circ \mu = \varphi \circ \mu + \psi \circ \mu$.

Доведення. а) Для довільного вектора $\boldsymbol{\nu}$ маємо

$$\big(c(\varphi \circ \psi)\big)(\boldsymbol{\nu}) = c(\varphi \circ \psi)(\boldsymbol{\nu}) = c\psi(\varphi(\boldsymbol{\nu}));$$
$$\big((c\varphi) \circ \psi)\big)(\boldsymbol{\nu}) = \psi((c\varphi)(\boldsymbol{\nu})) = \psi(c\varphi(\boldsymbol{\nu})) = c\psi(\varphi(\boldsymbol{\nu})).$$

Отже, $\big(c(\varphi \circ \psi)\big)(\boldsymbol{\nu}) = \big((c\varphi) \circ \psi)\big)(\boldsymbol{\nu})$. Оскільки вектор $\boldsymbol{\nu}$ – довільний, то $c(\varphi \circ \psi) = (c\varphi) \circ \psi$. Друга рівність доводиться аналогічно.

b) Для довільного вектора $\boldsymbol{\nu}$ маємо

$$\big(\varphi \circ (\psi + \mu)\big)(\boldsymbol{\nu}) = (\psi + \mu)(\varphi(\boldsymbol{\nu})) = \psi(\varphi(\boldsymbol{\nu})) + \mu(\varphi(\boldsymbol{\nu}));$$
$$\big(\varphi \circ \psi + \varphi \circ \mu\big)(\boldsymbol{\nu}) = (\varphi \circ \psi)(\boldsymbol{\nu}) + (\varphi \circ \mu)(\boldsymbol{\nu}) = \psi(\varphi(\boldsymbol{\nu})) + \mu(\varphi(\boldsymbol{\nu})).$$

Отже, $\big(\varphi \circ (\psi + \mu)\big)(\boldsymbol{\nu}) = \big(\varphi \circ \psi + \varphi \circ \mu\big)(\boldsymbol{\nu})$. Оскільки вектор $\boldsymbol{\nu}$ – довільний, то $\varphi \circ (\psi + \mu) = \varphi \circ \psi + \varphi \circ \mu$. Друга рівність доводиться аналогічно. □

4.2. Дії з матрицями

Враховуючи те, що згідно із твердженням 20, між лінійними відображеннями та їх матрицями є взаємно однозначна відповідність, то діям із лінійними відображеннями повинні відповідати аналогічні дії з матрицями.

Нехай P^n, P^m, P^k – арифметичні векторні простори, $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ і $\boldsymbol{e}'_1, \boldsymbol{e}'_2, \ldots, \boldsymbol{e}'_m$ – бази просторів P^n і P^m відповідно, $\varphi : P^n \to P^m$, $\psi : P^n \to P^m$, $\mu : P^m \to P^k$ – лінійні відображення, $[\varphi] = (a_{ij})$, $[\psi] = (b_{ij})$, $[\mu] = (c_{ij})$ – їх матриці. Розглянемо також відображення

$$\varphi + \psi : P^n \to P^m, \quad c \cdot \varphi : P^n \to P^m, \quad \mu \circ \varphi : P^n \to P^k$$

та їх матриці $[\varphi + \psi] = (p_{ij})$, $[c \cdot \varphi] = (q_{ij})$, $[\mu \circ \varphi] = (r_{ij})$.

а) Оскільки для кожного базового вектора $\boldsymbol{e}_j$

$$(\varphi + \psi)(\boldsymbol{e}_j) = \varphi(\boldsymbol{e}_j) + \psi(\boldsymbol{e}_j) = (a_{1j}, a_{2j}, \ldots, a_{mj}) + (b_{1j}, b_{2j}, \ldots, b_{mj}) =$$
$$= (a_{1j} + b_{1j}, a_{2j} + b_{2j}, \ldots, a_{mj} + b_{mj}) = (p_{1j}, p_{2j}, \ldots, p_{mj}),$$

то для всіх індексів i, j виконується рівність $p_{ij} = a_{ij} + b_{ij}$.

Матрицю $[\varphi + \psi]$ перетворення $\varphi + \psi$ природно назвати *сумою* матриць $A = [\varphi]$ і $B = [\psi]$. Тобто ми хочемо, щоб для додавання матриць виконувалася рівність $[\varphi + \psi] = [\varphi] + [\psi]$. Тому правило додавання матриць виглядає так:

якщо $A = (a_{ij})$ і $B = (b_{ij})$ – матриці однакового розміру, то їх сумою $A + B$ є матриця $(a_{ij} + b_{ij})$.

Наголошуємо, що додавати можна лише матриці однакового розміру, причому сума буде матрицею такого ж розміру.

б) Для кожного базового вектора $\boldsymbol{e}_j$ маємо

$$(c \cdot \varphi)(\boldsymbol{e}_j) = c \cdot \varphi(\boldsymbol{e}_j) = c \cdot (a_{1j}, a_{2j}, \ldots, a_{mj}) =$$
$$= (ca_{1j}, ca_{2j}, \ldots, ca_{mj}) = (q_{1j}, q_{2j}, \ldots, q_{mj}),$$

тоді для всіх індексів i, j виконується рівність $q_{ij} = ca_{ij}$.

Матрицю $[c \cdot \varphi]$ перетворення $c \cdot \varphi$ природно назвати *добутком скаляра c на матрицю $A = [\varphi]$*. Тобто для множення матриць на скаляри

має виконуватися рівність $[c \cdot \varphi] = c \cdot [\varphi]$. Тому *множення матриці на скаляр* визначається таким правилом:

$$якщо \;\; A = (a_{ij}), \;\; то \;\; c \cdot A = (c \cdot a_{ij}) .$$

в) Для композиції $\mu \circ \varphi$ відображень μ і φ маємо

$$(\mu \circ \varphi)(\boldsymbol{e}_j) = \mu(\varphi(\boldsymbol{e}_j)) = \mu\big(a_{1j}, a_{2j}, \ldots, a_{mj})\big) =$$
$$= \mu(a_{1j}\boldsymbol{e}'_1 + a_{2j}\boldsymbol{e}'_2 + \ldots + a_{mj}\boldsymbol{e}'_m) = a_{1j}\mu(\boldsymbol{e}'_1) + a_{2j}\mu(\boldsymbol{e}'_2) + \ldots + a_{mj}\mu(\boldsymbol{e}'_m) =$$
$$= a_{1j}(c_{11}, c_{21}, \ldots, c_{k1}) + a_{2j}(c_{12}, c_{22}, \ldots, c_{k2}) + \ldots + a_{mj}(c_{1m}, c_{2m}, \ldots, c_{km}) =$$
$$= (c_{11}a_{1j} + \ldots + c_{1m}a_{mj}, c_{21}a_{1j} + \ldots + c_{2m}a_{mj}, \ldots, c_{k1}a_{1j} + \ldots + c_{km}a_{mj}) =$$
$$= (r_{1j}, r_{2j}, \ldots, r_{kj}) .$$

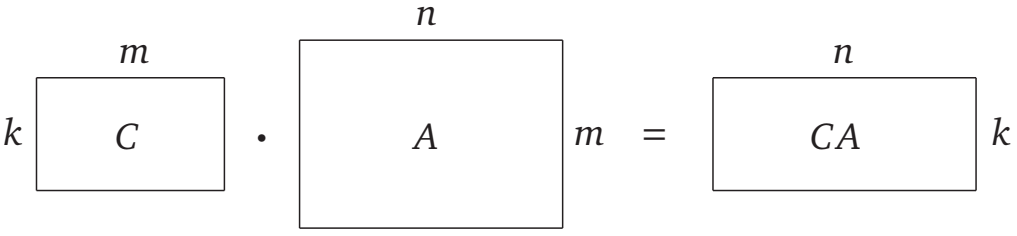
Отже, для всіх індексів i, j маємо рівність

$$r_{ij} = c_{i1}a_{1j} + c_{i2}a_{2j} + \ldots + c_{im}a_{mj}.$$

Якщо ми тепер хочемо визначити *множення матриць* таким чином, щоб виконувалася рівність $[\mu \circ \varphi] = [\mu] \cdot [\varphi]$, то правило множення матриць повинне бути таким:

якщо $C = (c_{ij})$ *і* $A = (a_{ij})$ *– матриці розмірів* $k \times m$ *і* $m \times n$ *відповідно,*
то їх добутком є матриця $CA = (r_{ij})$ *розміру* $k \times n$,
де $r_{ij} = c_{i1}a_{1j} + c_{i2}a_{2j} + \ldots + c_{im}a_{mj}$.

Не зовсім строго правило множення матриць можна сформулювати так: *елемент, що стоїть на перетині і-го рядка і j-го стовпця добутку двох матриць, є скалярним добутком і-го рядка першого множника на j-й стовпець другого множника*. Звертаємо увагу, що дві матриці можна перемножити тоді й лише тоді, коли кількість стовпців першого множника дорівнює кількості рядків другого. Умови, коли дві матриці можна перемножити, і зв'язок розмірів добутку із розмірами множників зручно подати таким рисунком:



Вправа 11. *Нехай C і A – матриці розмірів $k \times m$ і $m \times n$ відповідно. Підрахуйте, скільки разів треба виконати множення коефіцієнта матриці C на коефіцієнт матриці A, щоб обчислити добуток CA.*

Далі для довільної матриці $A = (a_{ij})$ замість $(-1) \cdot A$ будемо писати просто $-A$. Очевидно, що $-A = (-a_{ij})$.

Легко встановити бієкцію між множиною матриць $M_{m\times n}(P)$ і векторним арифметичним простором P^{mn} – наприклад, послідовно виписуючи в рядок спочатку перший, потім другий, і так аж до останнього, рядки матриці. Оскільки матриці додаються і множаться на скаляри поелементно, то додаванню матриць і множенню матриць на скаляри відповідають такі ж дії над відповідними векторами. Тому всі властивості додавання векторів і множення векторів на скаляри автоматично переносяться на відповідні дії над матрицями.

Твердження 23 (властивості додавання матриць і множення матриць на скаляри)**.** *Для довільних матриць A, B, C із $M_{m\times n}(P)$ та довільних скалярів $a, b \in P$ виконуються такі співвідношення*:
1) $(A + B) + C = A + (B + C)$ (***асоціативність*** *додавання матриць*)*;*
2) $A + B = B + A$ (***комутативність*** *додавання матриць*)*;*
3) *для нульової матриці* $0 \quad A + 0 = 0 + A = A$;
4) $A + (-A) = (-A) + A = 0$ (*існування* ***протилежної*** *матриці*)*;*
5) $1 \cdot A = A$ (***унітарність*** *множення на скаляри*)*;*
6) $a(bA) = (ab)A$*;*
7) $(a+b)A = aA+bA$ (***дистрибутивність*** *множення на скаляри відносно додавання скалярів*)*;*
8) $a(A+B) = aA+aB$ (***дистрибутивність*** *множення на скаляри відносно додавання матриць*).

У наступних міркуваннях нам буде зручно записувати вектори як стовпці. Нехай $\varphi : P^n \to P^m$ – лінійне відображення, $A_\varphi = (a_{ij})$ – його матриця, $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = x_1\boldsymbol{e}_1 + \dots + x_n\boldsymbol{e}_n$ – довільний вектор із P^n. Тоді

$$\varphi(\boldsymbol{x}) = \varphi(x_1\boldsymbol{e}_1 + \dots + x_n\boldsymbol{e}_n) = x_1\varphi(\boldsymbol{e}_1) + \dots + x_n\varphi(\boldsymbol{e}_n) =$$
$$= x_1 \begin{pmatrix} a_{11} \\ \dots \\ a_{m1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1n} \\ \dots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \dots\dots\dots\dots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix}.$$

З іншого боку,

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n) \end{pmatrix}. \tag{4.2}$$

Отже,

$$[\varphi(\boldsymbol{x})] = [\varphi] \cdot [\boldsymbol{x}]\,. \tag{4.3}$$

Рівність (4.2) дозволяє, використовуючи матричні позначення і множення матриць, переписати систему лінійних рівнянь

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1\,, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array} \tag{4.4}$$

у дуже компактному вигляді

$$A\boldsymbol{x} = \boldsymbol{b}, \tag{4.5}$$

де $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ – основна матриця системи, $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$ – стовпець невідомих, а $\boldsymbol{b} = \begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix}$ – стовпець вільних членів. Запис системи лінійних рівнянь у вигляді (4.5) будемо називати *матричною формою запису* цієї системи.

Вправа 12. *Чи правильно, що з рівності* $A\boldsymbol{x} = A\boldsymbol{y}$ *випливає рівність* $\boldsymbol{x} = \boldsymbol{y}$*?*

Порівняння співвідношень (4.3) і (4.5) дозволяє дати дуже корисну геометричну інтерпретацію системі лінійних рівнянь (4.4) у термінах лінійних відображень:

множина розв'язків системи (4.4) *– це повний прообраз вектора* $\boldsymbol{b}$ *вільних членів при лінійному відображенні* $P^n \longrightarrow P^m$ *із матрицею* $A = (a_{ij})$*, що є основною матрицею системи* (4.4).

Зокрема, множина розв'язків однорідної системи лінійних рівнянь збігається з ядром відповідного лінійного відображення, а множина тих стовпців $\boldsymbol{b}$ вільних членів, при яких система (4.4) є сумісною, – із образом цього відображення.

У випадку матриць ми вперше (але не востаннє) зустрічаємося із множенням, яке не є комутативним. Справді, нехай A – матриця порядку $m \times n$, а B – матриця порядку $p \times q$. Добуток AB визначений тоді й лише тоді, коли $n = p$, а добуток BA – тоді й лише тоді, коли $q = m$. Оскільки рівності $n = p$ і $q = m$ є незалежними, то можливість самого множення двох матриць залежить від порядку множників: з існування добутку AB зовсім не випливає існування добутку BA.

Якщо обидва добутки – AB і BA – існують, то вони можуть виявитися різними, навіть матрицями різного розміру. Наприклад, нехай $A = \begin{pmatrix}1 & 2\end{pmatrix}$, а $B = \begin{pmatrix}1\\2\end{pmatrix}$. Тоді

$$AB = \begin{pmatrix}1 & 2\end{pmatrix} \cdot \begin{pmatrix}1\\2\end{pmatrix} = (5) \quad \text{і} \quad BA = \begin{pmatrix}1\\2\end{pmatrix} \cdot \begin{pmatrix}1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2\\2 & 4\end{pmatrix}.$$

Результат множення матриць може залежати від порядку множників навіть тоді, коли множники є квадратними матрицями однакового порядку. Наприклад:

$$\begin{pmatrix}1 & 0\\0 & 2\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\0 & 2\end{pmatrix}, \quad \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 2\end{pmatrix} = \begin{pmatrix}1 & 2\\0 & 2\end{pmatrix}.$$

Наведені приклади не слід розуміти в тому сенсі, що нерівність $AB \neq BA$ виконується завжди. Наприклад, множення квадратних матриць першого порядку є комутативним (перевірте!). Рівність $AB = BA$ виконується і в багатьох інших випадках. Якщо $AB = BA$, то кажуть, що матриці A і B є *переставними* або що A і B *комутують*.

Матричні рівності у твердженні 24 і далі завжди будуть розумітися в тому сенсі, що або обидві частини рівності не визначені, або обидві частини визначені і збігаються.

Твердження 24 (властивості множення матриць)**.** *Для довільних матриць A, B, C з коефіцієнтами з поля P і скаляра $c \in P$ виконуються такі рівності*:

а) *для нульової матриці* 0 *маємо* $0 \cdot A = 0$ *і* $A \cdot 0 = 0$;

б) *для одиничної матриці* E *маємо* $E \cdot A = A$ *і* $A \cdot E = A$;

в) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$;

г) $c(A \cdot B) = (cA) \cdot B = A \cdot (cB)$;

д) $A \cdot (B + C) = A \cdot B + A \cdot C, \quad (A + B) \cdot C = A \cdot C + B \cdot C.$

Доведення. а) Очевидно.

б) Якщо $A = (a_{ij})_{m\times n}$ і добуток $E \cdot A$ визначений, то матриці $E \cdot A$ і A мають однакові розміри. Обчислимо елемент, що стоїть на перетині i-го рядка і j-го стовпця матриці $E \cdot A$, він буде таким:

$$0 \cdot a_{1j} + \ldots + 0 \cdot a_{i-1,j} + 1 \cdot a_{ij} + 0 \cdot a_{i+1,j} + \ldots + 0 \cdot a_{mj} = a_{ij}.$$

Тому $E \cdot A = A$. Рівність $A \cdot E = A$ доводиться аналогічно.

в) Матриці A, B і C можна розглядати як матриці певних лінійних відображень φ, ψ і μ. Відомо, що множення довільних відображень є асоціативним, тоді $\varphi \circ (\psi \circ \mu) = (\varphi \circ \psi) \circ \mu$. Тому

$$A \cdot (B \cdot C) = [\varphi \circ (\psi \circ \mu)] = [(\varphi \circ \psi) \circ \mu] = (A \cdot B) \cdot C.$$

г) Це випливає із твердження 22.а (міркування аналогічні міркуванням із попередньому пункту).

д) Це випливає із твердження 22.б (міркування аналогічні міркуванням із пункту в). □

Зокрема, якщо A – квадратна матриця того ж порядку, що і E, то $AE = EA = A$. Тому E відіграє для множення матриць таку саму роль, як і число 1 для множення чисел. Цим і пояснюється назва матриці E.

Якщо матриця A має вигляд

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix},$$

то матриця

$$A^\top = \begin{pmatrix} a_{11} & a_{21} & \ldots & a_{m1} \\ a_{12} & a_{22} & \ldots & a_{mn} \\ \ldots & \ldots & \ldots & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{mn} \end{pmatrix}$$

називається *транспонованою* до матриці A. Таким чином, рядками матриці $A^\top$ є стовпці матриці A, а стовпцями – рядки матриці A.

Квадратна матриця $A = (a_{ij})$ називається *симетричною*, якщо $A^\top = A$ (тобто, якщо для довільних i, j виконується рівність $a_{ij} = a_{ji}$), і *кососиметричною*, якщо $A^\top = -A$ (тобто, якщо для довільних i, j справджується $a_{ij} = -a_{ji}$).

Твердження 25 (властивості транспонування)**.**
а) $(A^\top)^\top = A$; *б*) $(A+B)^\top = A^\top + B^\top$;
в) $(cA)^\top = cA^\top$; *г*) $(AB)^\top = B^\top A^\top$.

Доведення. Властивості а), б), в) – очевидні.

г) Нехай $A = (a_{ij})$ і $B = (b_{ij})$ – матриці розмірів $m \times n$ і $n \times k$ відповідно. Тоді матриці $AB = (c_{ij})$, $A^\top$, $B^\top$, $(AB)^\top$ і $B^\top A^\top = (d_{ij})$ мають відповідно розміри $m \times k$, $n \times m$, $k \times n$, $k \times m$ і $k \times m$. Отже, $(AB)^\top$ і $B^\top A^\top$ мають однакові розміри. Далі, для довільних i, j маємо

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}, \quad d_{ji} = b_{1j}a_{i1} + b_{2j}a_{i2} + \ldots + b_{nj}a_{in}\,.$$

Оскільки $d_{ji} = c_{ij}$, то $B^\top A^\top = (AB)^\top$. □

Твердження 26 (властивості рядків і стовпців матриці добутку)**.**
а) *Кожен стовпець матриці AB є лінійною комбінацією стовпців першого множника A, причому коефіцієнти цієї лінійної комбінації беруться з відповідного стовпця другого множника B.*
б) *Кожен рядок матриці AB є лінійною комбінацією рядків другого множника B, причому коефіцієнти цієї лінійної комбінації беруться з відповідного рядка першого множника A.*

Доведення. Нехай

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \quad \text{і} \quad B = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1k} \\ b_{21} & b_{22} & \ldots & b_{2k} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n1} & b_{n2} & \ldots & b_{nk} \end{pmatrix}.$$

Тоді j-й стовпець матриці AB можна записати як

$$\begin{pmatrix} a_{11}b_{1j} + a_{12}b_{2j} + \ldots + a_{1n}b_{nj} \\ a_{21}b_{1j} + a_{22}b_{2j} + \ldots + a_{2n}b_{nj} \\ \ldots \\ a_{m1}b_{1j} + a_{m2}b_{2j} + \ldots + a_{mn}b_{nj} \end{pmatrix} = b_{1j}\begin{pmatrix} a_{11} \\ a_{21} \\ \ldots \\ a_{m1} \end{pmatrix} + b_{2j}\begin{pmatrix} a_{12} \\ a_{22} \\ \ldots \\ a_{m2} \end{pmatrix} + \ldots + b_{nj}\begin{pmatrix} a_{1n} \\ a_{2n} \\ \ldots \\ a_{mn} \end{pmatrix},$$

тобто є лінійною комбінацією стовпців матриці A з коефіцієнтами, які беруться із j-го стовпця матриці B. Це доводить пункт а). Щоб довести б), досить транспонувати матрицю AB і послатися на пункт а) (при транспонуванні стовпці перейдуть у рядки, рядки – у стовпці, а множники A і B поміняються місцями). □

Наслідок 17. *Ранг добутку двох матриць не перевищує рангу кожного із множників.*

Доведення. Оскільки кожен стовпець матриці AB є лінійною комбінацією стовпців матриці A, то, відповідно до твердження 13, маємо

$$r(AB) = r_{\text{ст}}(AB) \leq r_{\text{ст}}(A) = r(A).$$

Аналогічно

$$r(AB) = r_{\text{ряд}}(AB) \leq r_{\text{ряд}}(B) = r(B).$$

Тому

$$r(AB) \leq \min(r(A), r(B)). \qquad \square$$

Для квадратної матриці A можна визначити її натуральні степені: $A^1 = A$ і $A^{k+1} = A^k \cdot A$ для $k \geq 1$. З асоціативності множення матриць випливає, що для довільних натуральних чисел m і k виконується рівність $A^{m+k} = A^m \cdot A^k$.

Наявність степенів матриці дозволяє для довільного многочлена $f(x) = a_m x^m + a_{m_1} x^{m-1} + \ldots + a_1 x + a_0$ визначити значення $f(A)$ цього многочлена від квадратної матриці A:

$$f(A) := a_m \cdot A^m + a_{m_1} \cdot A^{m-1} + \ldots + a_1 \cdot A + a_0 \cdot E.$$

4.3. Обернена матриця

Матриця B називається *лівою оберненою* до матриці A, якщо $BA = E$. Аналогічно B називається *правою оберненою* до A , якщо $AB = E$.

Наприклад, матриця $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ буде лівою оберненою до матриці $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$ (а A – правою оберненою до B), бо

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

Вправа 13. *Нехай A – матриця розміру $m \times n$. Доведіть, що коли $m > n$, то для A не існує правої оберненої матриці, а якщо $m < n$, то для A не існує лівої оберненої.*

Із вправи 13 випливає, що лише для квадратних матриць можуть існувати одночасно як ліва обернена матриця, так і права. Тому далі будемо розглядати лише квадратні матриці.

Твердження 27. *Якщо для квадратної матриці A існують ліва обернена B і права обернена C, то $B = C$.*

Доведення. $B = B \cdot E = B \cdot AC = BA \cdot C = E \cdot C = C$. □

Тому у випадку квадратної матриці A можна говорити про *двосторонню обернену* (чи просто про *обернену*) до A матрицю. Оскільки із твердження 27 одразу випливає, що для матриці A існує не більше однієї оберненої, то в разі існування такої матриці будемо позначати її через A^{-1}. Таким чином, для матриці A^{-1} маємо

$$A \cdot A^{-1} = A^{-1} \cdot A = E. \tag{4.6}$$

Квадратна матриця, для якої існує обернена, називається *оборотною*.

Твердження 28 (найпростіші властивості оберненої матриці)**.** *Якщо A і B – оборотні матриці, то матриці A^{-1}, AB і $A^\top$ також оборотні. При цьому*
а) $(A^{-1})^{-1} = A$;
б) $(AB)^{-1} = B^{-1}A^{-1}$;
в) $(A^\top)^{-1} = (A^{-1})^\top$.

Доведення. а) Випливає з рівності (4.6).

б) Маємо

$$AB \cdot B^{-1}A^{-1} = A \cdot BB^{-1} \cdot A^{-1} = A \cdot E \cdot A^{-1} = AE \cdot A^{-1} = A \cdot A^{-1} = E.$$

Аналогічно доводиться рівність $B^{-1}A^{-1} \cdot AB = E$.

в) Транспонуючи рівність (4.6), одержуємо

$$(A^{-1})^\top \cdot A^\top = A^\top \cdot (A^{-1})^\top = E^\top = E.$$

Отже, $(A^{-1})^\top$ є оберненою матрицею до $A^\top$. □

Вправа 14. *Чи правильно, що для оборотних матриць A і B виконується рівність $(A + B)^{-1} = A^{-1} + B^{-1}$?*

Зауваження. Рівність $(AB)^{-1} = B^{-1}A^{-1}$ і необхідність виконання обернених дій у порядку, зворотному до початкового, можна проілюструвати таким прикладом. Розглянемо три дії: одягання шкарпеток, черевиків і светра. Коли дії комутують (одягання черевиків і светра), то й порядок обернених дій – роздягання – може бути довільним. Якщо ж дії не комутують (шкарпетки і черевики), то роздягатись можна лише в зворотному порядку.

Назвемо матрицю *елементарною*, якщо вона одержується з одиничної матриці за допомогою одного елементарного перетворення рядків або стовпців. Таким чином, маємо три типи елементарних матриць:

а) матриця

$$E_{ij} = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ & \ddots & & & & & \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ & & & \ddots & & & \\ 0 & \dots & 1 & \dots & 0 & \dots & 0 \\ & & & & & \ddots & \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \\ & & i & & j & & \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}, \qquad (4.7)$$

яка одержується з одиничної перестановкою i-го та j-го рядків (стовпців);

б) матриця

$$E_{ij}(a) = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ & \ddots & & & & & \\ 0 & \dots & 1 & \dots & a & \dots & 0 \\ & & & \ddots & & & \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ & & & & & \ddots & \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \\ & & i & & j & & \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}, \qquad (4.8)$$

яка одержується з одиничної додаванням до i-го рядка j-го, помноженого на a (додаванням до j-го стовпця i-го, помноженого на a);

в) матриця

$$E_i(a) = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 \\ & \ddots & & & \\ 0 & \dots & a & \dots & 0 \\ & & & \ddots & \\ 0 & \dots & 0 & \dots & 1 \\ & & i & & \end{pmatrix} \begin{matrix} \\ \\ i \\ \\ \\ \end{matrix}, \qquad (4.9)$$

яка одержується з одиничної множенням i-го рядка (стовпця) на число $a \neq 0$.

Твердження 29. *Множення матриці A на елементарну матрицю зліва (справа) виконує відповідне елементарне перетворення рядків (стовпців) матриці A.*

Доведення. Це випливає з теореми 26 про властивості рядків і стовпців матриці добутку. Покажемо, наприклад, чому множення матриці A на $E_{ij}(a)$ справа рівносильне додаванню до j-го стовпця матриці A її i-го стовпця, помноженого на a. Справді, нехай $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n$ – стовпці матриці A. Тоді за теоремою 26 при $k \neq j$ k-й стовпець матриці $A \cdot E_{ij}(a)$ можна записати як

$$0 \cdot \boldsymbol{a}_1 + \ldots + 0 \cdot \boldsymbol{a}_{k-1} + 1 \cdot \boldsymbol{a}_k + 0 \cdot \boldsymbol{a}_{k+1} + \ldots + 0 \cdot \boldsymbol{a}_n = \boldsymbol{a}_k,$$

а j-й стовпець матриці $A \cdot E_{ij}(a)$ як

$$0 \cdot \boldsymbol{a}_1 + \ldots + 0 \cdot \boldsymbol{a}_{i-1} + a \cdot \boldsymbol{a}_i + 0 \cdot \boldsymbol{a}_{i+1} + \ldots + 1 \cdot \boldsymbol{a}_j + 0 \cdot \boldsymbol{a}_{j+1} + \ldots + 0 \cdot \boldsymbol{a}_n = \boldsymbol{a}_j + a \cdot \boldsymbol{a}_i.$$

Отже, матриця $A \cdot E_{ij}(a)$ одержується з A додаванням до j-го стовпця матриці A її i-го стовпця, помноженого на a. □

Твердження 30. *Для кожної елементарної матриці існує обернена, яка також буде елементарною матрицею.*

Доведення. Елементарну матрицю E' можна записати у вигляді добутку $E' = E' \cdot E = E \cdot E'$. Тепер наше твердження випливає із твердження 29 і того, що для кожного елементарного перетворення рядків/стовпців існує обернене перетворення, яке також є елементарним перетворенням і яке можна замінити множенням із потрібного боку на відповідну елементарну матрицю. □

Лема 7. *Для матриці A ліва обернена існує тоді й лише тоді, коли матриця A є невиродженою.*

Доведення. Необхідність. Нехай A – матриця порядку n. Якщо існує матриця B, яка є лівою оберненою до A, то з рівності $BA = E$ і наслідку 17 отримуємо

$$n \geq \operatorname{rank} A \geq \operatorname{rank} BA = \operatorname{rank} E = n\,.$$

Отже, $\operatorname{rank} A = n$ і матриця A – невироджена.

Достатність. Нехай тепер матриця A є невиродженою. Елементарними перетвореннями рядків матрицю A можна звести до ступінчастого

вигляду. Оскільки $\operatorname{rank} A = n$, то ступінчастий вигляд не містить нульових рядків, а тому насправді є трикутним. Але трикутну матрицю у свою чергу можна звести елементарними перетвореннями рядків до одиничної матриці. Позаяк кожному елементарному перетворенню рядків відповідає множення зліва на відповідну елементарну матрицю, то отримуємо рівність

$$B_k \dots B_2 B_1 A = E\,,$$

де $B_k, \dots, B_2, B_1$ – деякі елементарні матриці. Але тоді матриця $B = B_k \dots B_2 B_1$ є лівою оберненою до A. □

Аналогічно доводиться і двоїста лема 8.

Лема 8. *Для матриці A права обернена існує тоді й лише тоді, коли матриця A є невиродженою.*

Із цих двох лем і твердження 27 одразу випливає така теорема.

Теорема 26 (критерій існування оберненої матриці)**.** *Обернена матриця A^{-1} існує тоді й лише тоді, коли матриця A є невиродженою.*

Твердження 31. *Якщо A – довільна $(m \times n)$-матриця, а B і C – невироджені квадратні матриці порядків m і n відповідно, то*

$$\operatorname{rank} A = \operatorname{rank} BA = \operatorname{rank} AC$$

(*тобто множення на невироджену матрицю не змінює рангу матриці*).

Доведення. Оскільки невироджена матриця є оборотною, то з наслідку 17 одержуємо

$$\operatorname{rank} A \geq \operatorname{rank} BA \geq \operatorname{rank}(B^{-1} \cdot BA) = \operatorname{rank}(B^{-1}B \cdot A) = \operatorname{rank} EA = \operatorname{rank} A\,.$$

Отже, $\operatorname{rank} A = \operatorname{rank} BA$. Рівність $\operatorname{rank} A = \operatorname{rank} AC$ доводиться аналогічно. □

Обернена матриця є корисним інструментом при дослідженні квадратних СЛР $A\boldsymbol{x} = \boldsymbol{b}$ із невиродженою матрицею A. За теоремою Кронекера–Капеллі про визначеність така СЛР має єдиний розв'язок, який можна обчислити так:

$$A^{-1}\boldsymbol{b} = A^{-1}(A\boldsymbol{x}) = (A^{-1}A)\boldsymbol{x} = E\boldsymbol{x} = \boldsymbol{x}.$$

Знаходити розв'язок СЛР таким методом особливо зручно тоді, коли доводиться розв'язувати багато систем із тією самою основною матрицею A, але різними стовпцями b вільних членів. Справді, у такому разі

досить один раз обчислити матрицю A^{-1}, а далі обчислювати лише добутки $A^{-1}\boldsymbol{b}$. Але для цього треба вміти обчислювати обернену матрицю.

Твердження 29 і спосіб його використання при доведенні леми 7 дають зручний метод обчислення матриці A^{-1}. Для цього до матриці A дописуємо справа одиничну матрицю E такого ж порядку й отримуємо матрицю $(A|E)$. Потім за допомогою елементарних перетворень рядків матриці $(A|E)$ зводимо її ліву частину A до одиничної матриці E. Якщо матриці $B_k, \ldots, B_2, B_1$ – елементарні, що відповідають цим перетворенням рядків, то маємо

$$(A|E) \rightsquigarrow (B_k \ldots B_2 B_1 A | B_k \ldots B_2 B_1 E) = (E|B).$$

Із доведення леми 7 одразу випливає, що отримана у правій частині матриця B – це і є A^{-1}.

Приклад 11. Знайдемо обернену матрицю для матриці $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 4 & 5 & 7 \end{pmatrix}$:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 3 & 4 & 0 & 1 & 0 \\ 4 & 5 & 7 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -1 & -2 & -2 & 1 & 0 \\ 0 & -3 & -5 & -4 & 0 & 1 \end{array}\right) \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & -1 & 0 \\ 0 & 0 & 1 & 2 & -3 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & -5 & 9 & -3 \\ 0 & 1 & 0 & -2 & 5 & -2 \\ 0 & 0 & 1 & 2 & -3 & 1 \end{array}\right) \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & -1 & 1 \\ 0 & 1 & 0 & -2 & 5 & -2 \\ 0 & 0 & 1 & 2 & -3 & 1 \end{array}\right).$$

Отже, $A^{-1} = \begin{pmatrix} -1 & -1 & 1 \\ -2 & 5 & -2 \\ 2 & -3 & 1 \end{pmatrix}$.

Варіацією описаного методу є спосіб обчислення A^{-1} за допомогою елементарних перетворень стовпців. Для цього до матриці A дописуємо знизу одиничну матрицю E такого ж порядку і далі елементарними перетвореннями стовпців отриманої матриці зводимо її верхню частину A до одиничної матриці E (елементарні матриці $C_1, C_2, \ldots, C_k$ відповідають перетворенням стовпців):

$$\left(\frac{A}{E}\right) \rightsquigarrow \left(\frac{AC_1C_2 \ldots C_k}{EC_1C_2 \ldots C_k}\right) = \left(\frac{E}{A^{-1}}\right).$$

4.4. Задачі

4.1. Покажіть, що лінійне перетворення

$$\varphi_\alpha : (x, y) \mapsto (x\cos\alpha - y\sin\alpha, x\sin\alpha + y\cos\alpha)$$

простору $\mathbb{R}^2$ можна інтерпретувати як поворот площини навколо початку координат на кут α. Випишіть матрицю $[\varphi_\alpha]$ цього перетворення і обчисліть добуток $[\varphi_\alpha] \cdot [\varphi_\beta]$.

4.2. Доведіть, що а) коли $m \geq n$, то кожен підпростір простору P^n є ядром деякого лінійного відображення $\varphi : P^n \to P^m$;

б) коли $m \leq n$, то кожен підпростір простору P^m є образом деякого лінійного відображення $\varphi : P^n \to P^m$.

4.3. а) Наведіть приклад дійсної матриці A другого порядку, для якої виконується рівність $A^2 = -E$.

б) Наведіть приклад дійсних матриць A і B другого порядку, для яких виконується рівність $AB = -BA$, причому $AB \neq 0$.

4.4.* Доведіть, що для кожної виродженої матриці A існують такі ненульові матриці B і C, що $AB = CA = 0$.

4.5. а) Знайдіть необхідні й достатні умови існування розв'язку матричного рівняння $AX = B$.

б) Аналогічне завдання для матричного рівняння $XA = B$.

4.6. Доведіть, що для кожної квадратної матриці A порядку n існує такий многочлен $f(x)$ степеня $\leq n^2$, що $f(A) = 0$.

4.7. Нехай A – квадратна матриця порядку n. Доведіть, що матричне рівняння $AX = B$

а) має єдиний розв'язок для кожної матриці B порядку n тоді й лише тоді, коли матриця A – невироджена;

б) має єдиний розв'язок для деякої матриці B порядку n тоді й лише тоді, коли матриця A – невироджена.

4.8. Чи правильно, що коли стовпці квадратної матриці A є лінійно незалежними, то такими будуть і стовпці матриці A^2?

4.9.* Нехай $(m \times n)$-матриця A має ранг r. Доведіть, що A можна розкласти в добуток $A = BC$, де множники B і C мають розміри $m \times r$ і $r \times n$ відповідно.

4.10.** Доведіть *нерівність Сильвестра*: для довільних матриці A розміру $m \times k$ і матриці B розміру $k \times n$ виконується нерівність

$$\operatorname{rank} A + \operatorname{rank} B \leq \operatorname{rank}(AB) + k.$$

4.11.* Нехай A, B, C – квадратні матриці порядку n. Доведіть, що коли $ABC = 0$, то $\operatorname{rank} A + \operatorname{rank} B + \operatorname{rank} C \leq 2n$.

4.12. Доведіть, що $(m \times n)$-матриця A має ліву обернену тоді й лише тоді, коли $\operatorname{rank} A = n$, а праву обернену – тоді й лише тоді, коли $\operatorname{rank} A = m$.

4.13.° Доведіть, що в тілі кватерніонів система "правих" лінійних рівнянь

$$ix + jy = 1, \quad kx - y = i$$

має єдиний розв'язок, а система "лівих" рівнянь

$$xi + yj = 1, \quad xk - y = i$$

розв'язків не має. Це дає приклад матриці над тілом, яка є оборотною, але транспонована до якої не є оборотною.

4.14.° Нехай $A = (a_{ij})_{i,j \in \mathbb{N}}$ – нескінченна матриця, причому

$$a_{ij} = \begin{cases} 1, & \text{якщо } j - i = 1; \\ 0, & \text{якщо } j - i \neq 1. \end{cases}$$

Доведіть, що $A \cdot A^{\top} = E$, але $A^{\top} \cdot A \neq E$.

4.15. Доведіть, що є нескінченно багато дійсних матриць другого порядку, які задовольняють рівність $A^2 = A$.

4.16. Кронекерівським добутком $A \times B$ матриць $A = (a_{ij})_{m \times n}$ і $B = (b_{kl})_{p \times q}$ називається матриця

$$A \times B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{pmatrix}$$

розміру $mp \times nq$. Доведіть, що кронекерівський добуток матриць має такі властивості:

а) $(\alpha A) \times B = A \times (\alpha B) = \alpha(A \times B)$;

б) $(A + B) \times C = A \times C + B \times C$;

в) $A \times (B + C) = A \times B + A \times C$;

г) $(A \times B)^\top = A^\top \times B^\top$;

д) якщо добутки AB і CD мають зміст, то $(A \times C)(B \times D) = (AB \times CD)$.

4.17. Доведіть, що кронекерівський добуток $A \times B$ невироджених матриць A і B також є невиродженою матрицею.

4.18. Доведіть, що перестановками рядків і стовпців матрицю $A \times B$ можна звести до матриці $B \times A$.

4.19. а)* Доведіть, що для довільної матриці $A \in M_{m \times n}(\mathbb{R})$ рангу r кожна з матриць $AA^\top$ і $A^\top A$ є симетричною матрицею рангу r.

б) Чи правильне аналогічне твердження для матриць із комплексними коефіцієнтами?

4.20.° Доведіть *теорему Фредгольма*: СЛР $A\boldsymbol{x} = \boldsymbol{b}$ із дійсними коефіцієнтами буде сумісною тоді й лише тоді, коли стовпець $\boldsymbol{b}$ вільних членів є ортогональним до всіх розв'язків спряженої однорідної СЛР $A^\top \boldsymbol{y} = \boldsymbol{0}$.

4.21.* Доведіть, що, коли елементарними перетвореннями стовпців звести матрицю $\left(\frac{A}{E}\right)$ до такого вигляду $\left(\frac{C}{B}\right)$, щоб у верхній частині ненульові стовпці матриці C стали лінійно незалежними, то сукупність продовжень у нижній частині B нульових стовпців матриці C утворює ФСР однорідної СЛР $A\boldsymbol{x} = \boldsymbol{0}$.

5. Підстановки

5.1. Поняття підстановки

Підстановкою на множині M називається взаємно однозначне відображення множини M на себе (тобто взаємно однозначне перетворення множини M).

Значення функції f у точці x можна позначати по-різному: $f(x)$, fx, xf, x^f. Для підстановок ми будемо зазвичай використовувати традиційніше перше позначення, однак у деяких випадках останнє позначення є зручнішим.

Якщо множина $M = \{m_1, m_2, \ldots, m_n\}$ – скінченна (а нас буде цікавити лише цей випадок), то підстановку $\pi : M \to M$ можна задавати таблицею, явно вказуючи для кожного елемента $m \in M$ його образ $\pi(m)$:

$$\pi = \begin{pmatrix} m_1 & m_2 & m_3 & \ldots & m_{n-1} & m_n \\ \pi(m_1) & \pi(m_2) & \pi(m_3) & \ldots & \pi(m_{n-1}) & \pi(m_n) \end{pmatrix}. \tag{5.1}$$

Очевидно, що порядок стовпців у правій частині запису (5.1) може бути довільним.

Елементи скінченної множини M можна занумерувати (фактично вище ми це вже зробили). Тоді з кожною підстановкою $\pi = \left(\begin{smallmatrix} m_1 & m_2 & \ldots & m_n \\ m_{i_1} & m_{i_2} & \ldots & m_{i_n} \end{smallmatrix}\right)$ на множині M природно пов'язується підстановка $\overline{\pi} = \left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{smallmatrix}\right)$ на множині $N = \{1, 2, \ldots, n\}$ номерів елементів. Навпаки, за підстановкою $\overline{\pi}$ легко відновлюється початкова підстановка π. Тому далі будемо розглядати лише підстановки на множині $N = \{1, 2, \ldots, n\}$ перших n натуральних чисел. Множина всіх підстановок на множині N позначається S_n.

Якщо розглядаються підстановки на множині $\{1, 2, \ldots, n\}$, то запис підстановки у вигляді

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}, \tag{5.2}$$

тобто, коли числа у верхньому рядку йдуть у природному порядку, будемо називати *стандартним*. При стандартному записі кожна підстановка π однозначно визначається своїм нижнім рядком, тобто *перестановкою* $(\pi(1), \pi(2), \ldots, \pi(n))$ чисел $1, 2, \ldots, n$. Цим переходом від підстановки π до перестановки $(\pi(1), \pi(2), \ldots, \pi(n))$ і назад ми часто будемо користуватися.

Теорема 27. *Множина S_n містить $n!$ підстановок.*

Доведення. Будемо записувати підстановки у стандартному вигляді (5.2). На перше місце в нижньому рядку ми можемо поставити довільний елемент множини $\{1, 2, \ldots, n\}$, тобто i_1 можемо вибрати n способами. Оскільки підстановка відображає різні елементи в різні, то на друге місце ми поставимо довільний елемент, відмінний від i_1. Отже, елемент i_2 можна вибрати $n-1$ способом. На третьому місці має стояти елемент, відмінний як від i_1, так і від i_2. Тому i_3 можливо вибрати $n-2$ способами і т. д. Нарешті, якщо елементи $i_1, i_2, \ldots, i_{n-1}$ уже вибрані, то i_n можна вибрати лише одним способом – це той елемент із $\{1, 2, \ldots, n\}$, який у нижньому рядку ще не зустрічався.

Позаяк на кожному кроці кількість способів вибору чергового елемента не залежить від того, які саме елементи вже вибрані, то загальна кількість способів заповнити нижній рядок така:

$$n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!\,. \qquad \square$$

Якщо π і τ – дві підстановки із S_n, то природно визначається їх *суперпозиція* як перетворень множини $N = \{1, 2, \ldots, n\}$:

$$(\pi \cdot \tau)(i) = \tau(\pi(i))$$

(увага! першою виконується ліва підстановка π). Але у випадку підстановок замість суперпозиції перетворень зазвичай говорять про *множення* підстановок, а результат суперпозиції $\pi \cdot \tau$ називають *добутком* підстановок. Перемножимо, наприклад, дві підстановки з S_n:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 1 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix}.$$

Враховуючи, що суперпозиція взаємно однозначних перетворень також є взаємно однозначним перетворенням, то добуток двох підстановок із S_n завжди буде підстановкою з S_n[11].

Теорема 28 (про властивості множення підстановок)**.**

а) *Множення підстановок* ***асоціативне***: $\pi \cdot (\tau \cdot \mu) = (\pi \cdot \tau) \cdot \mu$ *для довільних підстановок* $\pi, \tau, \mu \in S_n$;

б) *множення підстановок, узагалі кажучи,* ***не комутативне***: *для кожного* $n > 2$ *існують такі підстановки* $\pi, \tau \in S_n$, *що* $\pi \cdot \tau \neq \tau \cdot \pi$;

в) ***тотожна підстановка*** $\varepsilon = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$ *має властивості нейтрального елемента* (*одиниці*) *для множення, тобто* $\pi \cdot \varepsilon = \varepsilon \cdot \pi = \pi$ *для кожної підстановки* $\pi \in S_n$;

[11] Нагадуємо, що множити можна тільки підстановки на одній і тій же множині.

г) для кожної підстановки $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ ***обернена підстановка*** $\pi^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$ *має властивості оберненого елемента, тобто* $\pi \cdot \pi^{-1} = \pi^{-1} \cdot \pi = \varepsilon$.

Доведення. а) Підстановки є частковим випадком відображень, а множення довільних відображень є асоціативним.

б) Наприклад,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix} \neq$$

$$\neq \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}.$$

в) Оскільки для всіх x маємо $\varepsilon(x) = x$, то для всіх $i \in N$

$$(\pi \cdot \varepsilon)(i) = \varepsilon(\pi(i)) = \pi(i) \quad \text{та} \quad (\varepsilon \cdot \pi)(i) = \pi(\varepsilon(i)) = \pi(i).$$

г) Очевидно. □

Якщо множників більше, ніж два, то результат множення може залежати не лише від порядку, в якому виписані множники, а й від порядку виконання дій (адже кожного разу можна перемножити лише два множники). Порядок виконання дій зазвичай визначається за допомогою розстановки дужок: дії у внутрішніх дужках виконуються раніше. Виявляється, що, коли множення є асоціативним, то результат залежить лише від порядку множників.

Твердження 32. *Якщо множення асоціативне, то значення добутку* $a_1 a_2 \cdots a_n$ *не залежить від способу розстановки дужок.*

Доведення. Застосуємо індукцію за кількістю множників. Для $n \leq 2$ твердження тривіальне, а для $n = 3$ воно збігається з асоціативним законом.

Нехай тепер $n > 3$. У двох різних способах розстановки дужок у добутку $a_1 a_2 \cdots a_n$ виділимо дію, яка виконується останньою: нехай

$$u = (a_1 \cdots a_k) \cdot (a_{k+1} \cdots a_n) \quad \text{і} \quad v = (a_1 \cdots a_m) \cdot (a_{m+1} \cdots a_n).$$

Якщо $k = m$, то рівність $u = v$ одразу випливає із припущення індукції. Тому можна вважати, що $k < m$. За припущенням індукції можна

перейти до розстановок

$$u = (a_1 \cdots a_k) \cdot \big((a_{k+1} \cdots a_m) \cdot (a_{m+1} \cdots a_n)\big)$$

і

$$v = \big((a_1 \cdots a_k) \cdot (a_{k+1} \cdots a_m)\big) \cdot (a_{m+1} \cdots a_n)\,.$$

Позначимо:

$$a = a_1 \cdots a_k, \quad b = a_{k+1} \cdots a_m, \quad c = a_{m+1} \cdots a_n.$$

Рівність $u = v$ тепер випливає із закону асоціативності:

$$u = a \cdot (b \cdot c) = (a \cdot b) \cdot c = v. \qquad \square$$

5.2. Поняття групи

У математиці часто зустрічаються різні дії на множинах, які задовольняють умови а), в) і г) теореми 28. Спостереження про те, що багато властивостей таких дій випливають тільки із цих умов і не залежать від природи елементів самої множини, привело до загального поняття групи.

Означення 16. ***Групою*** *називається непорожня множина G з визначеною на ній бінарною дією $\cdot$, яка задовольняє такі умови (аксіоми групи) :*

(1) ***асоціативність****:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \textit{для довільних} \quad a, b, c \in G\ ;$$

(2) ***існування нейтрального елемента****: існує такий елемент e, що*

$$a \cdot e = e \cdot a = a \quad \textit{для довільного} \quad a \in G\ ;$$

(3) ***оборотність****: для кожного $a \in G$ існує такий елемент b (він називається* ***оберненим*** *до a), що*

$$a \cdot b = b \cdot a = e\ .$$

Якщо дія комутативна, тобто $a \cdot b = b \cdot a$ для всіх a і b, то група називається *комутативною* або *абелевою*.

Зазвичай дія $\cdot$ називається *множенням*, а нейтральний елемент e – *одиницею* групи G. Обернений до a елемент позначають a^{-1} (коректність цього позначення обґрунтовується нижче у твердженні 34.б). Однак у

конкретних група дія може називатися інакше і позначатися іншим символом. Зокрема, в абелевих групах дія часто називається *додаванням* із використання відповідної адитивної термінології (нейтральний елемент називають *нулем*, замість оберненого говорять про *протилежний* елемент, і т. д.).

Із теореми 28 випливає, що множина S_n є групою відносно множення підстановок, причому при $n > 2$ ця група буде некомутативною. Її називають *симетричною групою степеня n*.

Багато прикладів груп, переважно комутативних, уже зустрічалося раніше. Легко перевіряється, що комутативними групами відносно додавання будуть множини $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ і $\mathbb{C}$ цілих, раціональних, дійсних і комплексних чисел відповідно. Комутативними групами відносно множення є множини $\mathbb{Q}^*$, $\mathbb{R}^*$ і $\mathbb{C}^*$ ненульових раціональних, дійсних і комплексних чисел. Усі ці числові групи є нескінченними. Прикладом скінченної числової групи відносно множення є множина $\mathbb{C}_n$ комплексних коренів степеня n з 1 – це випливає із твердження 3 про мультиплікативну замкненість $\mathbb{C}_n$.

Важливий приклад некомутативної групи з'явився у нас нещодавно.

Твердження 33. *Множина $GL_n(P)$ усіх невироджених квадратних матриць порядку n із коефіцієнтами з поля P утворює групу відносно множення матриць.*

Доведення. За теоремою 26 матриця буде невиродженою тоді й лише тоді, коли вона має обернену. За твердженням 28 добуток оборотних матриць також є оборотною матрицею, тому множина $GL_n(P)$ замкнена відносно множення. Множення невироджених матриць є асоціативним, позаяк таким є множення довільних матриць. Інші дві аксіоми групи випливають із того, що одинична матриця E є невиродженою і що для невиродженої матриці A обернена матриця A^{-1} також є оборотною, а тому невиродженою. □

Твердження 34 (найпростіші властивості груп)**.**

а) У кожній групі існує єдиний нейтральний елемент.

б) У кожній групі для кожного елемента існує єдиний обернений елемент.

в) У кожній групі групі можна скорочувати як зліва, так і справа.

г) Кожне з рівнянь $ax = b$, $ya = b$ має у групі єдиний розв'язок.

Доведення. а) З означення нейтрального елемента випливає, що, коли кожен з елементів e_1 і e_2 є нейтральним, то

$$e_1 = e_1 \cdot e_2 = e_2.$$

б) Нехай кожен з елементів b і c є оберненим до a. Тоді з асоціативності множення випливає, що

$$b = b \cdot e = b \cdot ac = ba \cdot c = e \cdot c = c.$$

в) Нехай $ab = ac$. Тоді $a^{-1} \cdot ab = a^{-1} \cdot ac$. Але

$$a^{-1} \cdot ab = a^{-1}a \cdot b = e \cdot b = c$$

і, аналогічно, $a^{-1} \cdot ac = c$. Отже, $b = c$. Так само доводиться імплікація $ba = ca \Rightarrow b = c$.

г) Домноживши рівняння $ax = b$ на a^{-1} зліва, отримуємо

$$a^{-1} \cdot b = a^{-1} \cdot ax = a^{-1}a \cdot x = e \cdot x = x.$$

Отже, розв'язком рівняння $ax = b$ може бути лише $x = a^{-1}b$. Легко перевіряється, що це справді розв'язок

$$a \cdot a^{-1}b = a^{-1}a \cdot b = e \cdot b = b.$$

Подібним чином доводиться, що єдиним розв'язком рівняння $ya = b$ є $y = ba^{-1}$. □

Але скорочувати з різних сторін можна лише в комутативних групах. У некомутативній групі з рівності $ba = ac$, узагалі кажучи, не випливає, що $b = c$. Наприклад, для підстановок маємо

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

але

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \neq \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

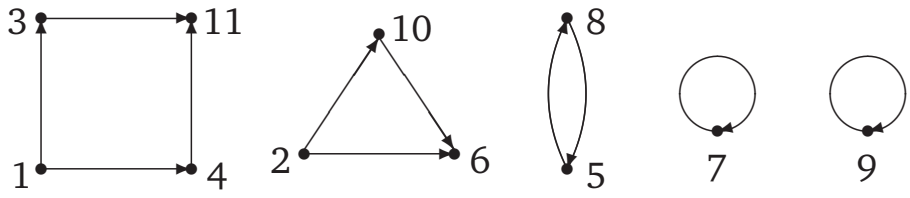
Вправа 15. *Наведіть приклад таких невироджених матриць A, B і C порядку 2, що $BA = AC$, але $B \neq C$.*

5.3. Розклад підстановки у добуток циклів

Із кожною підстановкою $\pi \in S_n$ пов'язується *граф дії* Γ_π цієї підстановки. Це орієнтований n-вершинний граф, вершини якого занумеровані числами від 1 до n і який містить стрілку з вершини i у вершину j тоді й лише тоді, коли $\pi(i) = j$. Наприклад, для підстановки

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 10 & 11 & 1 & 8 & 2 & 7 & 5 & 9 & 6 & 4 \end{pmatrix} \tag{5.3}$$

цей граф виглядає так:



Цей граф має ту властивість, що з кожної вершини виходить рівно одна стрілка і в кожну вершину заходить рівно одна стрілка. Якщо ми почнемо з якоїсь вершини a рухатися по стрілках графа: $a \to b \to c \to \ldots$, то першою вершиною, яка повториться, буде a (інакше у вершину, яка повториться першою, буде заходити дві стрілки). Тому компонентами зв'язності графа Γ_π будуть *цикли*. Зокрема, граф дії підстановки (5.3) містить по одному циклу довжини 2, 3 і 4 відповідно та два цикли довжини 1.

Зауважимо, що цикли довжини 1 відповідають тим елементам $i \in \{1, 2, \ldots, n\}$, для яких $\pi(i) = i$, тобто *нерухомим точкам* підстановки π. Цикли, які містять більше однієї вершини, називають *нетривіальними*.

Із графом Γ_π пов'язаний так званий *цикловий запис* підстановки, коли елементи кожного циклу записуються послідовно і виділяються круглими дужками.

Запис $(abc \ldots d)$ означає, що a переходить у b, b – у c, ... , а останній елемент d переходить в a. Наприклад, цикловий запис підстановки (5.3) має вигляд

$$(1\ 3\ 11\ 4)(2\ 10\ 6)(5\ 8)(7)(9).$$

Оскільки різні цикли циклового запису не мають спільних елементів, то цикловий запис ще називають *розкладом підстановки в добуток незалежних циклів*. Якщо множина, на якій діє підстановка, відома, то в цикловому записі часто лишають лише нетривіальні цикли, а нерухомі точки опускають. Зокрема, для підстановки (5.3) такий скорочений запис матиме вигляд

$$(1\ 3\ 11\ 4)(2\ 10\ 6)(5\ 8).$$

Зауважимо, що цикловий запис підстановки не є однозначним: цикли можна виписувати у довільному порядку, а всередині кожного циклу починати можна з довільної його вершини. Наприклад, цикловий запис підстановки (5.3) може бути і таким:

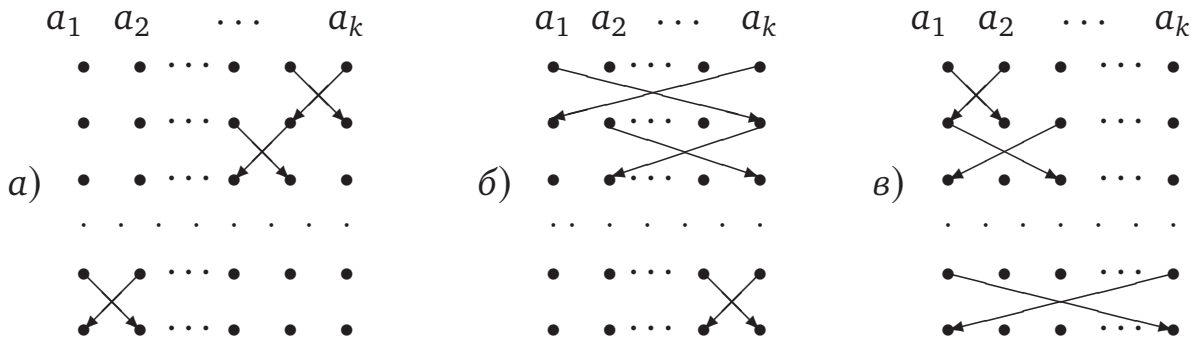
$$(10\ 6\ 2)(7)(4\ 1\ 3\ 11)(5\ 8)(9).$$

Вправа 16. *Як за цикловим записом підстановки* π *знайти цикловий запис оберненої підстановки* π^{-1}*?*

Якщо підстановка містить лише один нетривіальний цикл, то вона також називається *циклом*. Цикли довжини 2 називають *транспозиціями*. Два цикли називаються *незалежними*, якщо вони не мають спільних елементів. Цикловий запис підстановки фактично є розкладом підстановки в добуток незалежних циклів.

Теорема 29. *Кожна підстановка розкладається в добуток транспозицій.*

Доведення. Позаяк кожну підстановку можна розкласти в добуток циклів, то досить довести, що кожен цикл розкладається в добуток транспозицій. Розкласти цикл у добуток транспозицій можна різними способами. Три способи такого розкладу безпосередньо видно з рисунків:



Цим рисункам відповідають такі розклади:
$(a_1\, a_2\, \ldots\, a_{k-1}\, a_k) = (a_{k-1}\, a_k)\cdots(a_{k-2}\, a_{k-1})\cdot(a_2\, a_3)\cdot(a_1\, a_2)$ (рис. а);
$(a_1\, a_2\, \ldots\, a_{k-1}\, a_k) = (a_{k-1}\, a_k)\cdots(a_{k-2}\, a_{k-1})\cdot(a_2\, a_3)\cdot(a_1\, a_2)$ (рис. б);
$(a_1\, a_2\, \ldots\, a_{k-1}\, a_k) = (a_1\, a_2)\cdot(a_1\, a_3)\cdots(a_1\, a_k)$ (рис. в). □

Зауваження. Уже з доведення теореми 29 видно, що розклад підстановки в добуток транспозицій не є однозначним. Із рівності

$$(ab)(bc)(ab) = (ac)$$

випливає, що й кількість множників у розкладі може бути різною.

Твердження 35. *Кожна транспозиція розкладається в добуток непарної кількості транспозицій сусідніх елементів.*

Доведення. Безпосередньо перевіряється, що транспозиція $(k\ l)$, де $k < l$, розкладається в добуток

$$(k\ l) = (k\ k{+}1)(k{+}1\ k{+}2)\cdots(l{-}2\ l{-}1)(l{-}1\ l)(l{-}2\ l{-}1)\cdots(k\ k{+}1),$$

кількість множників у якому дорівнює $2(l-k)-1$. □

Звідси і з теореми 29 отримуємо наслідок 18.

Наслідок 18. *Кожна підстановка розкладається в добуток транспозицій сусідніх елементів.*

5.4. Парні та непарні підстановки

Говорять, що в перестановці $a_1, a_2, \ldots, a_n$ елементів $1, 2, \ldots n$ елементи a_i й a_j утворюють *інверсію*, або інверсну пару, якщо $i < j$, але $a_i > a_j$ (тобто, якщо більший елемент зустрічається раніше, ніж менший). Під кількістю інверсій підстановки (5.1) розуміють суму кількості інверсій у верхньому рядку $m_1, m_2, \ldots, m_n$ і кількості інверсій у нижньому рядку $\pi(m_1), \pi(m_2), \ldots, \pi(m_n)$. Наприклад, підстановка

$$\pi = \begin{pmatrix} 2 & 5 & 3 & 4 & 1 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix}$$

має 13 інверсій – 6 інверсій у верхньому рядку і 7 інверсій – у нижньому.

Кількість інверсій підстановки π позначають $N(\pi)$.

Підстановка називається *парною*, якщо вона має парну кількість інверсій, і *непарною* у протилежному випадку. І хоча число інверсій підстановки π залежить від способу її запису (оскільки порядок елементів у верхньому рядку може бути довільним), виявляється, що парність підстановки від її запису вже не залежить.

Твердження 36. *Парність кількості інверсій $N(\pi)$ підстановки π є властивістю самої підстановки і не залежить від способу її запису.*

Доведення. Розглянемо два записи

$$\begin{pmatrix} \ldots & a & b & \ldots \\ \ldots & c & d & \ldots \end{pmatrix} \quad \text{і} \quad \begin{pmatrix} \ldots & b & a & \ldots \\ \ldots & d & c & \ldots \end{pmatrix} \tag{5.4}$$

підстановки π, які відрізняються один від другого перестановкою двох сусідніх стовпців. В обох записах усі інверсії у верхніх рядках однакові, за винятком пари a і b. Якщо у першому записі ці елементи утворюють інверсію, то в другому – ні, і навпаки. Тому кількість інверсій у верхніх рядках записів (5.4) відрізняється на 1. З аналогічних причин кількість інверсій у нижніх рядках записів (5.4) теж відрізняється на 1. Проте тоді загальна кількість інверсій у другому записі підстановки π або на

2 менша, ніж у першому, або така сама, або на 2 більша. Але парність кількості інверсій в обох записах однакова.

Перестановками стовпців від довільного запису підстановки π можна перейти до стандартного запису (5.2). Отже, при довільному записі підстановки парність кількості інверсій буде така сама, як при стандартному, а тому не залежить від способу її запису. □

Зауважимо, що стандартний запис тотожної підстановки взагалі не містить інверсій. Тому тотожна підстановка є парною.

Знаком $\operatorname{sign}\pi$ підстановки π називається число $\operatorname{sign}\pi = (-1)^{N(\pi)}$. Із твердження 36 випливає, що знак підстановки є властивістю самої підстановки, бо не залежить від способу її запису.

Лема 9. *Якщо* α *– транспозиція сусідніх елементів, то підстановки* π *та* $\alpha\pi$ *мають протилежні знаки.*

Доведення. Нехай $\alpha = (k\ k{+}1)$ і

$$\pi = \begin{pmatrix} \dots & k & k+1 & \dots \\ \dots & a & b & \dots \end{pmatrix}.$$

Тоді

$$\alpha\pi = \begin{pmatrix} \dots & k & k+1 & \dots \\ \dots & b & a & \dots \end{pmatrix}.$$

Якщо $a < b$, то ці числа не утворюють інверсію в підстановці π, але утворюють інверсію в підстановці $\alpha\pi$. Тому при переході від π до $\alpha\pi$ кількість інверсій збільшується на 1. Якщо ж $a > b$, то навпаки – при переході від π до $\alpha\pi$ число інверсій зменшується на 1. В обох випадках числа $N(\pi)$ та $N(\alpha\pi)$ відрізняються на 1, а тому π та $\alpha\pi$ мають протилежні знаки. □

Твердження 37. *а) Кожна транспозиція є непарною підстановкою.*

б) Множення підстановки зліва на довільну транспозицію змінює парність підстановки на протилежну.

в) Парність підстановки збігається з парністю кількості множників у розкладі підстановки в добуток транспозицій. Зокрема, парність кількості множників не залежить від способу розкладу підстановки в добуток транспозицій.

г) Якщо $n > 1$*, то в* S_n *кількість парних підстановок дорівнює кількості непарних і дорівнює* $n!/2$*.*

д) $\operatorname{sign}(\pi_1\pi_2) = \operatorname{sign}\pi_1 \cdot \operatorname{sign}\pi_2$*. Зокрема, добуток підстановок однакової парності є парною підстановкою, а добуток підстановок різної парності – непарною.*

е) Підстановка й обернена до неї мають однакову парність.

є) Множина парних підстановок із S_n утворює групу.

Доведення. а) За твердженням 35 довільну транспозицію τ можна розкласти в добуток $\tau = \mu_{2k-1} \cdots \mu_2\mu_1$ непарної кількості транспозицій сусідніх елементів. Перепишемо цей добуток у вигляді $\mu_{2k-1} \cdots \mu_2\mu_1\varepsilon$, де ε – тотожна підстановка. Оскільки тотожна підстановка є парною і для кожного j множення на μ_j міняє, за лемою 9, знак підстановки $\mu_{j-1} \cdots \mu_2\mu_1\varepsilon$ на протилежний, то τ має знак $(-1)^{2k-1} = -1$, а тому є непарною.

б) Нехай $\tau = \mu_{2k-1} \cdots \mu_2\mu_1$ – розклад транспозиції τ у добуток непарної кількості транспозицій сусідніх елементів. Тоді твердження випливає з леми 9 і того, що множення на τ можна замінити множенням на добуток $\mu_{2k-1} \cdots \mu_2\mu_1$.

в) Нехай $\pi = \tau_m \cdots \tau_2\tau_1$ – розклад підстановки π у добуток транспозицій. Позаяк

$$\tau_m \cdots \tau_2\tau_1 = \tau_m \cdots \tau_2\tau_1\varepsilon,$$

то з попереднього пункту випливає, що $\operatorname{sign}\pi = (-1)^m \operatorname{sign}\varepsilon = (-1)^m$. Отже, парність підстановки π і парність числа m збігаються.

г) Нехай $n > 1$, B – множина парних підстановок з S_n, а C – множина непарних підстановок з S_n. Поставимо у відповідність кожній підстановці $\pi \in B$ підстановку $f(\pi) = (1\ 2)\pi$. За пунктом б) підстановка $f(\pi)$ є непарною, а тому f є відображенням із B в C. Це відображення є ін'єктивним: справді, рівність $f(\pi_1) = f(\pi_2)$ означає, що $(1\ 2)\pi_1 = (1\ 2)\pi_2$. Але в групі S_n можна скорочувати зліва, а тому $\pi_1 = \pi_2$.

З ін'єктивності відображення f випливає, що множина C не може містити менше елементів, ніж B, тобто $|B| \le |C|$.

Аналогічно доводиться ін'єктивність відображення $g : C \to B$, $\nu \mapsto (1\ 2)\nu$, із чого випливає нерівність $|B| \ge |C|$. Отже, $|B| = |C|$. Оскільки $|B| + |C| = |S_n| = n!$, то $|B| = |C| = n!/2$.

д) Нехай

$$\pi_1 = \tau_m \cdots \tau_2\tau_1 \quad \text{і} \quad \pi\pi_2 = \mu_k \cdots \mu_2\mu_1$$

– розклади у добуток транспозицій. Тоді

$$\pi_1\pi_2 = \tau_m \cdots \tau_2\tau_1\mu_k \cdots \mu_2\mu_1$$

і з пункту в) випливає, що

$$\operatorname{sign}(\pi_1\pi_2) = (-1)^{m+k} = (-1)^m \cdot (-1)^k = \operatorname{sign}\pi_1 \cdot \operatorname{sign}\pi_2.$$

е) Оскільки добуток $\pi \cdot \pi^{-1} = \varepsilon$ є парною підстановкою, то з попереднього пункту випливає, що множники π і π^{-1} повинні мати однакову парність.

є) Добуток парних підстановок є парною підстановкою, тому множення не виводить за межі множини парних підстановок. Множення довільних підстановок є асоціативним, тому асоціативним є і множення парних підстановок. Крім того, нейтральний елемент для множення підстановок – тотожна підстановка – є парною, й обернена до парної підстановки є парною. Отже, усі вимоги до групи виконуються. □

Група парних підстановок з S_n називається *знакозмінною* групою степеня n і позначається A_n.

5.5. Задачі

5.1. *Матрицею підстановки* π з S_n називається така $(0,1)$-матриця $P_\pi = (a_{ij})$ порядку n, що $a_{ij} = 1$ тоді й лише тоді, коли $\pi(i) = j$. Доведіть, що:

а) $(0,1)$-матриця P буде матрицею деякої підстановки тоді й лише тоді, коли в кожному рядку і в кожному стовпці вона містить рівно одну одиницю;

б) $P_\pi \cdot P_\tau = P_{\pi\tau}$;

в) $P_{\pi^{-1}} = P_\pi^\top$.

5.2. Нехай $1\cdot l_1 + 2\cdot l_2 + \cdots + n\cdot l_n = n$. Знайдіть кількість тих підстановок з S_n, які мають рівно l_1 циклів довжини 1, рівно l_2 циклів довжини 2, ..., рівно l_n циклів довжини n.

5.3. Доведіть, що знак $\operatorname{sign}\pi$ підстановки $\pi \in S_n$ такий:

$$\operatorname{sign}\pi = \prod_{1\le i<j\le n} \frac{\pi(j)-\pi(i)}{j-i}\,.$$

5.4. Нехай перестановка $a_1, a_2, \ldots, a_{j-1}, k, a_{j+1}, \ldots, a_n$ має m інверсій, а послідовність $a_1, a_2, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n$, яка одержується із цієї перестановки викиданням члена $a_j = k$, має m' інверсій. Доведіть, що $(-1)^m = (-1)^{m'} \cdot (-1)^{j+k}$.

5.5. Якщо підстановка $\pi \in S_n$ має k незалежних циклів (рахуючи і цикли довжини 1), то число $d(\pi) = n - k$ називається *декрементом* підстановки π. Доведіть, що

а) $\operatorname{sign}\pi = (-1)^{d(\pi)}$;

б) підстановку π можна подати у вигляді добутку $d(\pi)$ транспозицій;

в) підстановку π не можна подати у вигляді добутку менше ніж $d(\pi)$ транспозицій.

5.6. Доведіть, що найменша кількість транспозицій, якими перестановку $a_1, a_2, \ldots, a_n$ можна перевести в перестановку $b_1, b_2, \ldots, b_n$ тих же елементів, дорівнює декременту підстановки

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}.$$

5.7.°* Доведіть, що кожна підстановка з S_n розкладається в добуток транспозицій із множини $\{\pi_1, \pi_2, \ldots, \pi_{n-1}\}$ тоді й лише тоді, коли граф, що відповідає цій множині транспозицій, буде деревом.

5.8.°* Доведіть, що цикл довжини n можна розкласти в добуток $n-1$ транспозицій n^{n-2} способами.

5.9. Позначимо через $\widehat{c}(n,k)$ кількість тих підстановок з S_n, цикловий розклад яких містить рівно k циклів, причому всі вони неодиничні. Доведіть, що

$$\widehat{c}(n+1,k) = n\widehat{c}(n,k) + n\widehat{c}(n-1,k-1).$$

5.10. *Таблицею інверсій* перестановки $a_1, a_2, \ldots, a_n$ називається набір чисел $(b_1, b_2, \ldots, b_n)$, де b_i – це кількість тих інверсій, в яких i є меншою компонентою (тобто b_i дорівнює кількості тих чисел, які є більшими за i й розташовані в перестановці лівіше i).

а) Доведіть, що кожен набір чисел $(b_1, b_2, \ldots, b_n)$, де $0 \le b_i \le n-i$, буде таблицею інверсій деякої перестановки.

б) Як за набором чисел $(b_1, b_2, \ldots, b_n)$ відновити перестановку, для якої цей набір є таблицею інверсій?

5.11. Нехай $(b_1, b_2, \ldots, b_n)$ – таблиця інверсій, яка відповідає перестановці $a_1, a_2, \ldots, a_n$. Якій перестановці відповідає таблиця інверсій $(n-1-b_1, n-2-b_2, \ldots, 0-b_n)$?

5.12.* Елемент a_i називається *правостороннім максимумом* перестановки $a_1, a_2, \ldots, a_n$, якщо $a_i > a_j$ для всіх $j > i$ (наприклад, у перестановці $n, n-1, \ldots, 2, 1$ кожен елемент є правостороннім максимумом). Підрахуйте середню кількість правосторонніх максимумів серед усіх перестановок чисел $1, 2, \ldots, n$.

5.13.* Доведіть, що всі $n!$ перестановок із S_n можна впорядкувати π_1, π_2, $\ldots$, $\pi_{n!}$ таким чином, щоб для кожного $i \in \{1, 2, \ldots, n\}$ набори $(\pi_1(i), \pi_2(i), \ldots, \pi_{n!}(i))$ були однакові з точністю до циклічного зсуву.

5.14.** Нехай $n > 1$. Скількома способами можна розставити дужки в добуткові $a_1 a_2 \cdots a_n$?

6. Визначники

Нині визначники займають досить скромне місце як у математиці в цілому, так і в лінійній алгебрі зокрема. Однак не завжди було так. Досить порівняти кількість присвячених визначникам задач у перших виданнях класичного збірника задач з вищої алгебри Фаддєєва і Сомінського і в останніх. А в XIX ст. визначники вважалися набагато важливішими за матриці, з яких вони одержуються. Видана на початку XX ст. "Історія визначників" Мура складалася із чотирьох! томів.

Корисність визначників часто мотивують тим, що з їх допомогою можна одержати явні компактні формули для обчислення оберненої матриці або для знаходження розв'язків квадратної системи лінійних рівнянь. Однак ця компактність оманлива: ці формули мало придатні для практичних обчислень вже для матриць чи систем порядку 4.

Значно кориснішими визначники є в деяких теоретичних міркуваннях. Наприклад, за допомогою визначників легко побачити, як залежать елементи оберненої матриці від кожного з елементів початкової матриці, або дати критерій невиродженості матриці. Пізніше в курсі лінійної алгебри ми побачимо, що для деяких проблем (наприклад, знаходження власних значень лінійного перетворення) визначники є просто незамінним інструментом.

6.1. Означення й основні властивості визначника

Розглянемо на евклідовій площині $\mathbb{R}^2$ два вектори $\boldsymbol{a}$ і $\boldsymbol{b}$, що виходять із початку координат. Якщо ці вектори неколінеарні, то один із кутів, які вони утворюють, буде меншим за 180°. Якщо в межах цього кута від $\boldsymbol{a}$ до $\boldsymbol{b}$ треба рухатися проти годинникової стрілки (рис. 7.а), то впорядковану пару $(\boldsymbol{a}, \boldsymbol{b})$ векторів назвемо *додатно орієнтованою*. Якщо ж треба рухатися за годинниковою стрілкою (рис. 7.б), то цю пару називатимемо *від'ємно орієнтованою*.

Кожна пара $(\boldsymbol{a}, \boldsymbol{b})$ векторів, що виходять з початку координат, визначає певний паралелограм (рис. 7.в). Припишемо цьому паралелограму *орієнтовану площу* $S(\boldsymbol{a}, \boldsymbol{b})$, абсолютна величина якої дорівнює звичайній площі цього паралелограма, і яка має знак "+", якщо пара $(\boldsymbol{a}, \boldsymbol{b})$ є додатно орієнтованою, і знак "–", якщо ця пара від'ємно орієнтована.

З означення орієнтованої площі одразу випливає, що

$$S(\boldsymbol{b}, \boldsymbol{a}) = -S(\boldsymbol{a}, \boldsymbol{b}) \tag{6.1}$$

і

$$S(-\boldsymbol{a}, \boldsymbol{b}) = -S(\boldsymbol{a}, \boldsymbol{b}).$$

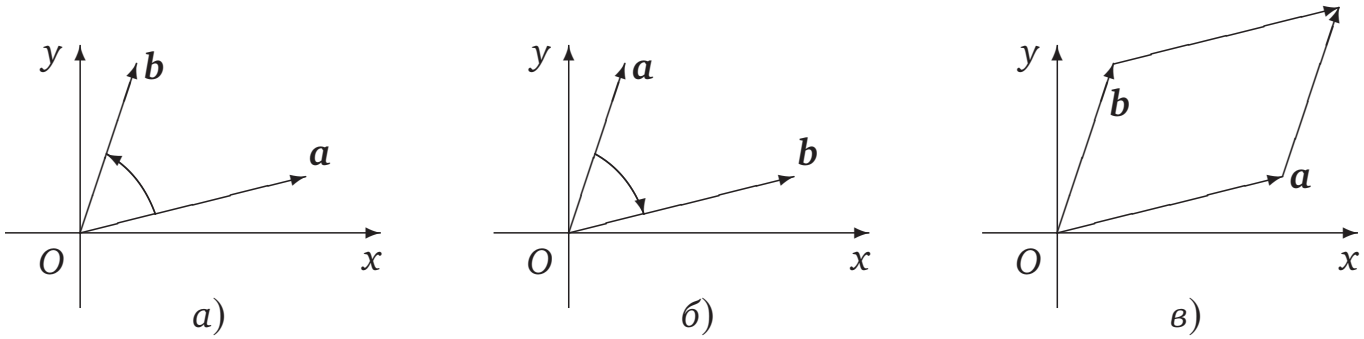


Рис. 7

Остання рівність легко узагальнюється: для довільного дійсного числа k виконується рівність

$$S(k\boldsymbol{a}, \boldsymbol{b}) = kS(\boldsymbol{a}, \boldsymbol{b}). \tag{6.2}$$

Трохи складніше перевіряється (зробіть це!) випадок, коли вектор $\boldsymbol{a}$ розпадається в суму $\boldsymbol{a} = \boldsymbol{a}_1 + \boldsymbol{a}_2$ векторів $\boldsymbol{a}_1$ і $\boldsymbol{a}_2$, тоді з рис. 8

$$S(\boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{b}) = S(\boldsymbol{a}_1, \boldsymbol{b}) + S(\boldsymbol{a}_2, \boldsymbol{b}). \tag{6.3}$$

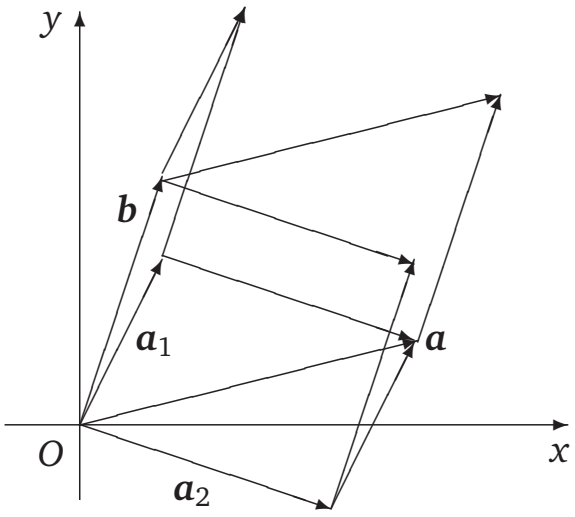


Рис. 8

За допомогою рівності (6.1) легко доводиться, що для другого аргументу виконуються аналоги рівностей (6.2) і (6.3):

$$S(\boldsymbol{a}, k\boldsymbol{b}) = kS(\boldsymbol{a}, \boldsymbol{b}), \qquad S(\boldsymbol{a}, \boldsymbol{b}_1 + \boldsymbol{b}_2) = S(\boldsymbol{a}, \boldsymbol{b}_1) + S(\boldsymbol{a}, \boldsymbol{b}_2).$$

Зауважимо, що для одиничних векторів $\boldsymbol{i}$ та $\boldsymbol{j}$, які лежать на осях Ox і Oy відповідно, маємо

$$S(\boldsymbol{i}, \boldsymbol{j}) = 1. \tag{6.4}$$

Аналогічні поняття можна визначити і у тривимірному просторі $\mathbb{R}^3$. Некомпланарну трійку векторів $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ будемо називати *додатно орієнтованою*, якщо, дивлячись із кінця вектора $\boldsymbol{a}$ на площину, в якій лежать вектори $\boldsymbol{b}$ і $\boldsymbol{c}$, ми бачимо пару $(\boldsymbol{b}, \boldsymbol{c})$ додатно орієнтованою. У противному разі трійка $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ називатиметься *від'ємно орієнтованою*.

Легко бачити, що коли у трійці $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ переставити місцями два сусідні вектори, то її орієнтація зміниться на протилежну. Отже, трійки $(\boldsymbol{a}, \boldsymbol{c}, \boldsymbol{b})$ і $(\boldsymbol{b}, \boldsymbol{a}, \boldsymbol{c})$ мають орієнтацію, протилежну до орієнтації трійки $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$. Трійки $(\boldsymbol{b}, \boldsymbol{c}, \boldsymbol{a})$ і $(\boldsymbol{c}, \boldsymbol{a}, \boldsymbol{b})$ мають таку ж орієнтацію, як і початкова трійка, а трійка $(\boldsymbol{c}, \boldsymbol{b}, \boldsymbol{a})$ — орієнтацію, протилежну до початкової.

Кожна трійка $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ векторів, що виходять із початку координат, визначає у просторі $\mathbb{R}^3$ певний паралелепіпед. Як і у випадку площини, цьому паралелепіпеду можна приписати *орієнтований об'єм* $V(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$, абсолютна величина якого дорівнює звичайному об'ємові цього паралелепіпеда, і який має знак "+", якщо трійка векторів є додатно орієнтованою, і знак "–"у протилежному випадку.

Орієнтований об'єм $V(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ паралелепіпеда має властивості, аналогічні властивостям (6.1)–(6.7) орієнтованої площі паралелограма (випливає з того, що властивості (6.1)–(6.7) виконуються для орієнтованої площі основи цього паралелепіпеда, породженої векторами $\boldsymbol{a}$ і $\boldsymbol{b}$):

1) орієнтований об'єм змінює знак на протилежний, якщо переставити місцями два сусідні вектори (аналог властивості (6.1));

2) для довільного дійсного числа k виконується рівність

$$V(k\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) = kV(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}); \tag{6.5}$$

3) якщо $\boldsymbol{a} = \boldsymbol{a}_1 + \boldsymbol{a}_2$ векторів $\boldsymbol{a}_1$ і $\boldsymbol{a}_2$, то

$$V(\boldsymbol{a}_1 + \boldsymbol{a}_2, \boldsymbol{b}, \boldsymbol{c}) = V(\boldsymbol{a}_1, \boldsymbol{b}, \boldsymbol{c}) + V(\boldsymbol{a}_2, \boldsymbol{b}, \boldsymbol{c}); \tag{6.6}$$

4) для одиничних векторів $\boldsymbol{i}, \boldsymbol{j}$ та $\boldsymbol{k}$, що лежать на осях Ox, Oy і Oz відповідно, маємо

$$V(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}) = 1. \tag{6.7}$$

Зауважимо, що об'єм $V(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ буде додатним тоді й лише тоді, коли орієнтація трійки $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$ збігається з орієнтацією стандартної трійки $(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$ базисних векторів тривимірного простору.

Виникає природне бажання узагальнити ці поняття – паралелепіпеда, побудованого на векторах $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$, та його орієнтованого об'єму –

на простір $\mathbb{R}^n$ довільної розмірності. А ще краще – на довільний арифметичний простір P^n.

При цьому, правда, виникає кілька запитань: а що таке паралелепіпед в $\mathbb{R}^n$ (тим паче у просторі P^n), що називати об'ємом цього паралелепіпеда, що таке орієнтація набору векторів і т. д.

Головним для нас буде поняття орієнтованого об'єму паралелепіпеда. І ми визначимо це поняття дуже характерним для математики шляхом: ми поки що не знаємо, що це за об'єкт, але він повинен мати такі й такі властивості. І якщо об'єкт із такими властивостями справді існує, то саме його і будемо називати орієнтованим об'ємом паралелепіпеда[12].

Які ж властивості орієнтованої площі паралелограма в $\mathbb{R}^2$ і орієнтованого об'єму паралелепіпеда в $\mathbb{R}^3$ хотілося б мати і в загальному випадку? Для відповіді на це питання нам знадобиться поняття, наведене в означенні 17.

Означення 17. *Визначена на векторному просторі P^n функція*

$$f : \underbrace{P^n \times P^n \times \cdots \times P^n}_{k \text{ разів}} \to P$$

від k векторних аргументів називається ***полілінійною****, якщо вона задовольняє такі дві умови:*

(1) *для довільних індексу i $(1 \le i \le k)$ та скаляра $\alpha \in P$ виконується рівність*

$$f(\boldsymbol{v}_1, \ldots, \alpha\boldsymbol{v}_i, \ldots, \boldsymbol{v}_k) = \alpha f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_k);$$

(2) *для довільного індексу i $(1 \le i \le k)$ виконується рівність*

$$f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i' + \boldsymbol{v}_i'', \ldots, \boldsymbol{v}_k) = f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i', \ldots, \boldsymbol{v}_k) + f(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i'', \ldots, \boldsymbol{v}_k).$$

Іншими словами, така функція повинна бути лінійною за кожним аргументом (при фіксованих інших аргументах). А оскільки аргументів багато, то вона й називається полілінійною.

[12] Показовою в цьому сенсі є історія з поняттям неперервної функції. Довго під неперервними розуміли функції, графіки яких можна намалювати, не відриваючи олівця від паперу. Потім виникла потреба дати строге математичне означення такої функції. На початку XIX ст. потрібне означення з'явилося і все було чудово: усі функції, які до того вважалися неперервними, це означення задовольняли. Однак за кілька десятків років з'явилися приклади функцій, які це означення задовольняли, але не були неперервними із традиційного погляду. Зокрема, вони не були гладкими у жодній своїй точці. У палкій дискусії, що розгорілася, перемогли прихильники формального підходу: неперервними стали вважати ті і тільки ті функції, що мають властивості, які вимагаються у формальному означенні.

Твердження 38. *Якщо серед аргументів є нульовий вектор, то значення полілінійної функції на такому наборі дорівнює* 0.

Доведення. Це випливає з рівностей

$$f(\boldsymbol{v}_1, \ldots, \mathbf{0}, \ldots, \boldsymbol{v}_k) = f(\boldsymbol{v}_1, \ldots, 0 \cdot \mathbf{0}, \ldots, \boldsymbol{v}_k) = 0 \cdot f(\boldsymbol{v}_1, \ldots, \mathbf{0}, \ldots, \boldsymbol{v}_k) = 0. \qquad \square$$

Як видно із наведених вище властивостей орієнтованої площі паралелограма та орієнтованого об'єму паралелепіпеда, вони будуть полілінійними функціями (відповідно з $\mathbb{R}^2 \times \mathbb{R}^2$ в $\mathbb{R}$ та з $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3$ в $\mathbb{R}$). Ще одним добре відомим прикладом полілінійної функції від двох агрументів є скалярний добуток векторів (як на площині $\mathbb{R}^2$, так і в просторі $\mathbb{R}^3$).

Орієнтована площа й орієнтований об'єм мають ще кілька властивостей, які бажано зберегти в загальному випадку:

– кількість аргументів збігається з розмірністю простору;

– *знакозмінність* (цю властивість ще називають *кососиметричністю*)[13]: якщо серед аргументів є два однакові, то значення функції дорівнює 0;

– *нормованість*: площа квадрата, породженого одиничними векторами $\boldsymbol{i}$ та $\boldsymbol{j}$, та об'єм куба, породженого одиничними векторами $\boldsymbol{i}$, $\boldsymbol{j}$ та $\boldsymbol{k}$, дорівнюють 1.

Твердження 39 (властивості знакозмінних полілінійних функцій)**.**

а) Якщо серед аргументів знакозмінної полілінійної функції f є пропорційні, то вона дорівнює 0.

б) Значення знакозмінної полілінійної функції f не змінюється, якщо до одного з аргументів додати довільне кратне іншого.

в) Значення знакозмінної полілінійної функції f не змінюється, якщо до одного з аргументів додати довільну лінійну комбінацію інших.

г) Значення знакозмінної полілінійної функції f змінюється на протилежне, якщо переставити місцями два аргументи.

Доведення. а) Використовуючи знакозмінність, маємо

$$f(\ldots, \boldsymbol{a}, \ldots, \alpha\boldsymbol{a}, \ldots) = \alpha f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}, \ldots) = 0.$$

б) Застосовуючи попередню властивість, маємо

$$f(\ldots, \boldsymbol{a} + \alpha\boldsymbol{b}, \ldots, \boldsymbol{b}, \ldots) = f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{b}, \ldots) + f(\ldots, \alpha\boldsymbol{b}, \ldots, \boldsymbol{b}, \ldots) =$$
$$= f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{b}, \ldots) + 0 = f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{b}, \ldots).$$

[13] Походження цих термінів стане зрозумілим трохи пізніше.

в) Це випливає з попереднього пункту, бо додавання до вектора $\boldsymbol{a}$ лінійної комбінації $\beta_1\boldsymbol{b}_1 + \cdots + \beta_m\boldsymbol{b}_m$ можна замінити послідовним додаванням до $\boldsymbol{a}$ векторів $\beta_1\boldsymbol{b}_1, \ldots, \beta_m\boldsymbol{b}_m$.

г) Одержуємо зі знакозмінності і рівностей

$$\begin{gathered} 0 = f(\ldots, \boldsymbol{a}+\boldsymbol{b}, \ldots, \boldsymbol{a}+\boldsymbol{b}, \ldots) = f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{a}, \ldots) + \\ + f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{b}, \ldots) + f(\ldots, \boldsymbol{b}, \ldots, \boldsymbol{a}, \ldots) + f(\ldots, \boldsymbol{b}, \ldots, \boldsymbol{b}, \ldots) = \\ = f(\ldots, \boldsymbol{a}, \ldots, \boldsymbol{b}, \ldots) + f(\ldots, \boldsymbol{b}, \ldots, \boldsymbol{a}, \ldots). \end{gathered}$$

□

Зауважимо, що саме із властивістю г) останнього твердження, яка випливає зі знакозмінності функції f, і пов'язане походження терміна "знакозмінна функція".

Наслідок 19. *Якщо аргументи $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ знакозмінної полілінійної функції f лінійно залежні, то $f(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k) = 0$.*

Доведення. Якщо вектори $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ – лінійно залежні, то один із них є лінійною комбінацією інших. Без обмеження загальності можемо вважати, що $\boldsymbol{v}_1 = \alpha_2\boldsymbol{v}_2 + \cdots + \alpha_k\boldsymbol{v}_k$. Тоді із тверджень 39.в і 38 випливає, що

$$\begin{gathered} f(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k) = f(\boldsymbol{v}_1 - \alpha_2\boldsymbol{v}_2 - \cdots - \alpha_k\boldsymbol{v}_k, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k) = \\ = f(\boldsymbol{0}, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k) = 0. \end{gathered}$$

□

Якщо впорядкованій n-ці векторів із простору P^n поставити у відповідність матрицю, стовпцями якої є ці вектори, то одержимо квадратну матрицю порядку n із коефіцієнтами з поля P. Зрозуміло, що ця відповідність між упорядкованими n-ками векторів і квадратними матрицями порядку n є взаємно однозначною. Враховуючи це зауваження, приходимо до наступного узагальнення орієнтованих площі й об'єму.

Означення 18. ***Визначником*** *порядку n над полем P називається функція* det*, яка визначена на множині $M_n(P)$ усіх квадратних матриць порядку n із коефіцієнтами з поля P, набуває значень у полі P і задовольняє такі умови*:

(1) *функція* det *є полілінійною функцією від набору векторів-стовпців матриці*;

(2) *функція* det *є знакозмінною, тобто значення* det *дорівнює* 0*, якщо серед стовпців матриці є два однакові*;

(3) *функція* det *є нормованою, тобто значення* det *від одиничної матриці E дорівнює* 1.

Визначник[14] квадратної матриці A позначають $\det A$ або $|A|$. Якщо матриця задана явно:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix},$$

то її визначник позначають

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

Наголосимо, що визначник матриці є вже не матрицею, а елементом поля P, тобто числом.

Одразу постає кілька питань:

– чи завжди, тобто для довільних натурального числа n і поля P, функція det існує?

– якщо така функція існує, то наскільки однозначно вона визначена?

– якщо функція det існує і визначена однозначно, то як її можна обчислити?

Швидко ми одержимо повну відповідь на всі ці питання.

Теорема 30 (явна формула для визначника)**.** *Визначник квадратної матриці* (a_{ij}) *порядку* n *повинен обчислюватися за формулою*

$$\det(a_{ij}) = \sum_{\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{smallmatrix}\right) \cdot a_{i_1 1} a_{i_2 2} \cdots a_{i_n n}\,, \tag{6.8}$$

де сума береться по всіх підстановках $\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{smallmatrix}\right)$ *із* S_n.

Доведення. Позначимо стовпці матриці (a_{ij}) через $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, …, $\boldsymbol{a}_n$. Тоді матрицю (a_{ij}) можна записати у вигляді впорядкованого набору векторів $(\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_n)$. Розглянемо також одиничні вектори-стовпці

$$\boldsymbol{e}_1 = (1, 0, \dots, 0)^\top, \quad \boldsymbol{e}_2 = (0, 1, 0, \dots, 0)^\top, \quad \dots, \quad \boldsymbol{e}_n = (0, \dots, 0, 1)^\top.$$

Розклавши перший стовпець матриці (a_{ij}) у суму

$$\boldsymbol{a}_1 = a_{11}\boldsymbol{e}_1 + a_{21}\boldsymbol{e}_2 + \dots + a_{n1}\boldsymbol{e}_n$$

[14] Визначник ще називають *детермінантом*. Це той же визначник, тільки латинською. Звідси і позначення $\det A$ для визначника матриці A.

і використовуючи лінійність функції det за першим аргументом, можна розкласти $\det(a_{ij})$ у суму n визначників:

$$\det(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) =$$
$$= a_{11}\det(\boldsymbol{e}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) + a_{21}\det(\boldsymbol{e}_2, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) + \cdots + a_{n1}\det(\boldsymbol{e}_n, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n).$$

Розклавши далі другий стовпець матриці (a_{ij}) у суму

$$\boldsymbol{a}_2 = a_{12}\boldsymbol{e}_1 + a_{22}\boldsymbol{e}_2 + \cdots + a_{n2}\boldsymbol{e}_n$$

і використовуючи лінійність функції det за другим аргументом, можна кожен із цих n визначників у свою чергу розкласти в суму n визначників. У результаті отримаємо вже n^2 доданків. І так далі. Зрештою одержимо розклад

$$\det(a_{ij}) = \sum \det(a_{i_1 1}\boldsymbol{e}_{i_1}, a_{i_2 2}\boldsymbol{e}_{i_2}, \ldots, a_{i_n n}\boldsymbol{e}_{i_n}) =$$
$$= \sum a_{i_1 1}a_{i_2 2}\cdots a_{i_n n}\det(\boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \ldots, \boldsymbol{e}_{i_n}) \qquad (6.9)$$

визначника $\det(a_{ij})$ у суму n^n доданків. Якщо серед індексів $i_1, i_2, \ldots, i_n$ є однакові, то за твердженням 39.а матимемо $\det(\boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \ldots, \boldsymbol{e}_{i_n}) = 0$. Тому треба розглянути ті і тільки ті доданки у правій частині суми (6.9), для яких усі індекси $i_1, i_2, \ldots, i_n$ є попарно різними, тобто утворюють перестановку чисел $1, 2, \ldots, n$.

Розглянемо підстановку $\pi = \left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{smallmatrix}\right)$ та її розклад $\pi = \alpha_1\alpha_2\cdots\alpha_k$ в добуток транспозицій. Тоді $\operatorname{sign}\pi = (-1)^k$. Кожній транспозиції $\alpha = (ij)$ поставимо у відповідність перестановку векторів $\boldsymbol{e}_i$ і $\boldsymbol{e}_j$ у довільному впорядкованому наборі векторів $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$. Із рівності $\pi = \alpha_1\alpha_2\cdots\alpha_k\epsilon$ випливає, що, коли ми почнемо з набору $(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n)$ і послідовно виконаємо перестановки векторів, які відповідають транспозиціям α_k, $\ldots$, α_2, α_1, то отримаємо набір $\boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \ldots, \boldsymbol{e}_{i_n}$.

Оскільки набору $(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n)$ відповідає одинична матриця E з визначником 1, а при кожній перестановці двох векторів визначник змінює знак на протилежний, то

$$\det(\boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \ldots, \boldsymbol{e}_{i_n}) = (-1)^k = \operatorname{sign}\left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{smallmatrix}\right).$$

Звідси та з рівності (6.9) випливає твердження теореми. □

Таким чином, якщо функція det існує, то вона повинна обчислюватися за формулою (6.8). Однак тепер уже неважко довести, що функція, яка задається правою частиною рівності (6.8), справді задовольняє всі вимоги з означення визначника.

Твердження 40. *Функція*

$$f\big((a_{ij})\big) = \sum_{\left(\begin{smallmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{smallmatrix}\right)\in S_n} \operatorname{sign}\left(\begin{smallmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}a_{i_2 2}\cdots a_{i_n n} \tag{6.10}$$

задовольняє всі вимоги з означення визначника квадратної матриці (a_{ij}) *порядку* n.

Доведення. 1) Якщо елементи k-го стовпця $\boldsymbol{a}_k = (a_{1k}, a_{2k}, \dots, a_{nk})^\top$ матриці (a_{ij}) помножити на скаляр α, то матимемо

$$\sum_{\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\in S_n} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}\cdots \alpha a_{i_k k}\cdots a_{i_n n} =$$

$$= \alpha\cdot \sum_{\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\in S_n} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}\cdots a_{i_k k}\cdots a_{i_n n}.$$

Отже,

$$f(\boldsymbol{a}_1, \dots, \alpha\boldsymbol{a}_k, \dots, \boldsymbol{a}_n) = \alpha f(\boldsymbol{a}_1, \dots, \boldsymbol{a}_k, \dots, \boldsymbol{a}_n).$$

2) Якщо k-й стовпець розпадається в суму двох: $\boldsymbol{a}_k = \boldsymbol{a}'_k + \boldsymbol{a}''_k$, $a_{ik} = a'_{ik} + a''_{ik}$ $(i = 1, \dots, n)$, то маємо

$$\sum_{\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\in S_n} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}\cdots (a'_{ik} + a''_{ik})\cdots a_{i_n n} =$$

$$= \sum_{\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\in S_n} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}\cdots a'_{ik}\cdots a_{i_n n} +$$

$$+ \sum_{\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\in S_n} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & k & \dots & n\\ i_1 & \dots & i_k & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}\cdots a''_{ik}\cdots a_{i_n n}\ .$$

Отже,

$$f(\boldsymbol{a}_1, \dots, \boldsymbol{a}'_k + \boldsymbol{a}''_k, \dots, \boldsymbol{a}_n) = f(\boldsymbol{a}_1, \dots, \boldsymbol{a}'_k, \dots, \boldsymbol{a}_n) + f(\boldsymbol{a}_1, \dots, \boldsymbol{a}''_k, \dots, \boldsymbol{a}_n).$$

3) Якщо переставити k-й і m-й стовпці матриці (a_{ij}), то в кожному доданку

$$\operatorname{sign}\left(\begin{smallmatrix}1 & \dots & k & \dots & m & \cdots & n\\ i_1 & \dots & i_k & \dots & i_m & \dots & i_n\end{smallmatrix}\right)\cdot a_{i_1 1}\cdots a_{i_k k}\cdots a_{i_m m}\cdots a_{i_n n}$$

суми (6.10) треба буде переставити місцями множники $a_{i_k k}$ і $a_{i_m m}$ (від чого доданок не зміниться), а в підстановці $\left(\begin{smallmatrix} 1 & \dots & k & \dots & m & \dots & n \\ i_1 & \dots & i_k & \dots & i_m & \dots & i_n \end{smallmatrix}\right)$ переставити в нижньому рядку i_k та i_m (тобто виконати транспозицію, від чого знак підстановки зміниться на протилежний). Таким чином, кожен доданок суми (6.10) змінить знак на протилежний, а тому і вся сума змінить знак на протилежний.

4) Нарешті, якщо матриця (a_{ij}) збігається з одиничною матрицею E, то $a_{ij} = 0$, якщо $i \neq j$, і $a_{kk} = 1$ для всіх k. Тому сума (6.10) міститиме лише один ненульовий доданок

$$\operatorname{sign}\left(\begin{smallmatrix} 1 & \dots & k & \dots & n \\ 1 & \dots & k & \dots & n \end{smallmatrix}\right) \cdot 1 \cdot 1 \cdots 1 = 1.$$

Тому $f(E) = 1$.

Таким чином, функція $f\big((a_{ij})\big)$ є полілінійною, знакозмінною і нормованою. Отже, усі вимоги з означення визначника виконано. □

Із теореми 30 і твердження 40 випливає, що функція det існує і визначена однозначно. До того ж із її полілінійності і знакозмінності випливає, що вона має всі властивості, перераховані у твердженні 39.

6.2. Обчислення визначників

Теорема 30 дає правила обчислення визначників другого і третього порядків:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}, \tag{6.11}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \tag{6.12}$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Але вже для $n = 4$ формула (6.8) стає громіздкою, бо містить 24 доданки. Для ще більших n кількість доданків стрімко зростає і формула (6.8) стає непридатною для реальних обчислень. Так уже для $n = 10$ ця формула містить $10! = 3628800$ доданків, кожен з яких є добутком 10 множників.

Сказане зовсім не означає, що формула (6.8) не є корисною. Навпаки, у багатьох теоретичних міркуваннях вона навіть дуже потрібна.

Ми вже пересвідчилися в цьому при доведенні твердження 40 про коректність означення визначника. Доведення двох наступних тверджень лише підтверджують цю тезу.

Теорема 31. $\det A^\top = \det A$.

Доведення. Нехай $A = (a_{ij})$ і $A^\top = (b_{ij}) = (a_{ji})$. Тоді

$$\det A^\top = \sum_{\pi\in S_n} \operatorname{sign}\pi \cdot b_{\pi(1)1} b_{\pi(2)2} \cdots b_{\pi(n)n} = \sum_{\pi\in S_n} \operatorname{sign}\pi \cdot a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}\,.$$

Розглянемо підстановку

$$\tau = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

яка є оберненою до

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Якщо підстановка π пробігає всю множину S_n, то й обернена до неї підстановка τ також пробігає всю множину S_n. Крім того, пряма й обернена підстановки мають однакову парність. Тому

$$\det A^\top = \sum_{\pi\in S_n} \operatorname{sign}\pi \cdot a_{\tau(1)1} a_{\tau(2)2} \cdots a_{\tau(n)n} =$$

$$= \sum_{\tau\in S_n} \operatorname{sign}\tau \cdot a_{\tau(1)1} a_{\tau(2)2} \cdots a_{\tau(n)n} = \det A\,.$$

□

Наслідок 20. *При обчисленні визначника квадратної матриці її рядки і стовпці рівноправні. Зокрема, визначник матриці є полілінійною знакозмінною нормованою функцією від її рядків.*

Як наслідок із цього наслідку маємо, що твердження 39 і наслідок 19 будуть правильними і для рядків визначника.

Твердження 41. *Визначник трикутної матриці дорівнює добуткові її діагональних елементів.*

Доведення. Із попередньої теореми випливає, що досить обмежитися випадком верхньої трикутної матриці. Нехай

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}.$$

З'ясуємо, який вигляд мають у цьому випадку ненульові доданки суми (6.8). Зауважимо, що кожен доданок

$$\operatorname{sign}\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \cdot a_{i_1 1} a_{i_2 2} \cdots a_{i_n n} \tag{6.13}$$

містить рівно по одному множнику з кожного стовпця і з кожного рядка матриці. Ненульовим множником із першого стовпця може бути лише a_{11}. Оскільки цей елемент належить першому рядку, то з першого рядка більше множників вибирати не можна. Тому ненульовим множником із другого стовпця може бути лише a_{22}. У третьому стовпці вже не можна брати елементи ні з першого рядка, ні з другого. Тому у третьому стовпці можна взяти лише a_{33}. Міркуючи аналогічно далі, бачимо, що для того, щоб доданок (6.13) був ненульовим, із кожного стовпця треба брати лише діагональний елемент.

Таким чином, у випадку трикутної матриці сума (6.8) містить лише один ненульовий доданок, в якому фігурує добуток $a_{11}a_{22}\cdots a_{nn}$ діагональних елементів. Цьому добуткові відповідає підстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, яка є парною. Тому цей добуток треба брати зі знаком "+". Отже,

$$\det A = a_{11}a_{22}\cdots a_{nn}. \qquad \square$$

Твердження 42. *Якщо матриця $A = (a_{ij})$ має вигляд*

$$A = \begin{pmatrix} B & D \\ 0 & C \end{pmatrix},$$

де B і C — квадратні матриці, то $\det A = \det B \cdot \det C$.

Доведення. Нехай матриця B має порядок k, а C – порядок m. Тоді A має порядок $n = k + m$. Добуток

$$a_{i_1 1} a_{i_2 2} \cdots a_{i_k k} a_{i_{k+1} k+1} \cdots a_{i_n n} \tag{6.14}$$

буде ненульовим лише у випадку, коли множники $a_{i_1 1}$, $a_{i_2 2}$, …, $a_{i_k k}$ із перших k стовпців матриці A належать матриці B, тобто, коли

$$\{i_1, i_2, \dots, i_k\} = \{1, 2, \dots, k\}.$$

Але тоді

$$\{i_{k+1}, i_{k+2}, \dots, i_n\} = \{k+1, k+2, \dots, n\}$$

і множники $a_{i_{k+1} k+1}$, …, $a_{i_n n}$ належать матриці C. Крім того, пов'язана з добутком (6.14) підстановка $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ розпадається в об'єднання

двох підстановок – підстановки $\pi_1 = \left(\begin{smallmatrix} 1 & 2 & \dots & k \\ i_1 & i_2 & \dots & i_k \end{smallmatrix}\right)$ на множині $\{1, 2, \dots, k\}$ і підстановки $\pi_2 = \left(\begin{smallmatrix} k+1 & k+2 & \dots & n \\ i_{k+1} & i_{k+2} & \dots & i_n \end{smallmatrix}\right)$ на множині $\{k+1, k+2, \dots, n\}$.

Оскільки всі елементи множини $\{1, 2, \dots, k\}$ менші за всі елементи множини $\{k+1, k+2, \dots, n\}$, то кожна інверсія підстановки π буде або інверсією підстановки π_1, або інверсією підстановки π_2. Тому кількість інверсій N підстановки π дорівнює $N = N_1 + N_2$, де N_i — кількість інверсій підстановки π_i. Але тоді $\operatorname{sign}\pi = \operatorname{sign}\pi_1 \cdot \operatorname{sign}\pi_2$.

Таким чином, враховуючи лише ненульові доданки із розкладу визначника $\det A$, отримуємо

$$\det A = \sum_{\left(\begin{smallmatrix} 1 & 2 \dots n \\ i_1 & i_2 \dots i_n \end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix} 1 & 2 \dots n \\ i_1 & i_2 \dots i_n \end{smallmatrix}\right) \cdot a_{i_1 1} a_{i_2 2} \cdots a_{i_n n} =$$

$$= \sum_{\left(\begin{smallmatrix} 1 \dots k \\ i_1 \dots i_k \end{smallmatrix}\right), \left(\begin{smallmatrix} k+1 \dots n \\ i_{k+1} \dots i_n \end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix} 1 \dots k \\ i_1 \dots i_k \end{smallmatrix}\right) \operatorname{sign}\left(\begin{smallmatrix} k+1 \dots n \\ i_{k+1} \dots i_n \end{smallmatrix}\right) \cdot a_{i_1 1} \cdots a_{i_k k} a_{i_{k+1} k+1} \cdots a_{i_n n} =$$

$$= \sum_{\left(\begin{smallmatrix} 1 \dots k \\ i_1 \dots i_k \end{smallmatrix}\right),} \operatorname{sign}\left(\begin{smallmatrix} 1 \dots k \\ i_1 \dots i_k \end{smallmatrix}\right) \cdot a_{i_1 1} \cdots a_{i_k k} \cdot \sum_{\left(\begin{smallmatrix} k+1 \dots n \\ i_{k+1} \dots i_n \end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix} k+1 \dots n \\ i_{k+1} \dots i_n \end{smallmatrix}\right) \cdot a_{i_{k+1} k+1} \cdots a_{i_n n} =$$

$$= \det B \cdot \det C. \qquad \square$$

Тепер у нас є достатньо засобів, щоб запропонувати значно ефективніший метод обчислення визначників, ніж використання явної формули (6.8). За аналогією з відповідним методом розв'язування систем лінійних рівнянь його також можна назвати *методом Гаусса*:

1) Елементарними перетвореннями рядків і стовпців зводимо матрицю визначника до трикутного вигляду (кілька останніх рядків при цьому можуть виявитися нульовими). При таких перетвореннях визначник може змінюватися, однак, як випливає з полілінійності і знакозмінності визначника та твердження 39.б, зі зміни легко контролюються. Справді, при множенні/діленні якогось рядка або стовпця на число α визначник множиться/ділиться на це число; при перестановці двох рядків (або стовпців) визначник змінює знак на протилежний; при додаванні до одного рядка (або стовпця) кратного іншого рядка (відповідно стовпця) визначник не змінюється.

2) Визначник отриманої трикутної матриці легко обчислюється: за твердженням 41 він дорівнює добуткові діагональних елементів.

Приклад 12.

$$\begin{vmatrix} 2 & 3 & 3 & 3 \\ 3 & 2 & 3 & 3 \\ 3 & 3 & 2 & 3 \\ 3 & 3 & 3 & 2 \end{vmatrix} = \begin{vmatrix} 11 & 11 & 11 & 11 \\ 3 & 2 & 3 & 3 \\ 3 & 3 & 2 & 3 \\ 3 & 3 & 3 & 2 \end{vmatrix} =$$

(до першого рядка додали всі інші, визначник при цьому не змінився)

$$= 11 \cdot \begin{vmatrix} 1 & 1 & 1 & 1 \\ 3 & 2 & 3 & 3 \\ 3 & 3 & 2 & 3 \\ 3 & 3 & 3 & 2 \end{vmatrix} =$$

(із першого рядка винесли множник 11)

$$= 11 \cdot \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{vmatrix} =$$

(від кожного рядка, починаючи із другого, відняли потроєний перший рядок; визначник при цьому не змінився)

$$= 11 \cdot 1 \cdot (-1) \cdot (-1) \cdot (-1) = -11.$$

(Визначник трикутної матриці дорівнює добуткові діагональних елементів.)

Теорема 32. *Для квадратної матриці A такі умови рівносильні:*

а) рядки матриці A лінійно незалежні;

б) стовпці матриці A лінійно незалежні;

в) матриця A – невироджена;

г) $\det A \neq 0$*;*

д) існує обернена матриця A^{-1}.

Доведення. Рівносильність умов а), б) і в) випливає з означення рангу матриці і теореми 15 про рівність рядкового і стовпцевого рангів. Рівносильність умов в) і д) – із критерію існування оберненої матриці (теорема 26). Тому досить довести рівносильність умов в) і г).

в) $\Rightarrow$ г). Якщо ранг матриці A дорівнює її порядку, то елементарними перетвореннями рядків і стовпців її можна звести до діагонального вигляду з ненульовими елементами на діагоналі. Визначник такої матриці дорівнює добуткові діагональних елементів і є ненульовим. Оскільки при елементарних перетвореннях рядків і стовпців властивість визначника бути нульовим (відповідно ненульовим) не змінюється, то $\det A \neq 0$.

г) $\Rightarrow$ в. Випливає з наслідку 19. □

6.3. Мінори

Нехай A – довільна матриця (не обов'язково квадратна). *Мінором* порядку k матриці A називається визначник квадратної матриці порядку k, що складається з елементів, які стоять на перетині певних k рядків і k стовпців матриці A (зі збереженням відносного порядку цих рядків і стовпців). Якщо потрібно явно вказати номери вибраних рядків і стовпців, то мінор порядку k позначають $M^{\{j_1,\dots,j_k\}}_{\{i_1,\dots,i_k\}}$ (знизу – номери вибраних рядків, угорі – стовпців).

Якщо матриця A має розміри $m \times n$, то A має рівно $\binom{m}{k}\binom{n}{k}$ мінорів порядку k (k рядків можна вибрати $\binom{m}{k}$ способами, а k стовпців — $\binom{n}{k}$ способами). Мінорами порядку 1 матриці A є її елементи.

Найбільший із порядків ненульових мінорів матриці A називається *мінорним рангом* матриці A і позначається $r_{\min}(A)$. Отже, $r_{\min}(A) = r$, якщо серед мінорів r–го порядку матриці A є хоча б один ненульовий, а всі мінори більших порядків дорівнюють 0.

Теорема 33 (про мінорний ранг матриці)**.** $r_{\min}(A) = \operatorname{rank}(A)$.

Доведення. Нехай $\operatorname{rank}(A) = r$. Тоді для довільного $k > r$ будь-які k рядків матриці A будуть лінійно залежними. Для довільного мінора порядку k його рядки будуть частинами рядків матриці A, а тому й поготів будуть лінійно залежними. Але визначник із лінійно залежними рядками дорівнює 0. Тому кожен мінор порядку $k > r$ дорівнює 0 і $r_{\min}(A) \le r$.

Розглянемо тепер підматрицю A', утворену r лінійно незалежними рядками матриці A. Її рядковий ранг дорівнює r, а тому і стовпцевий ранг має дорівнювати r. За теоремою 32 мінор, утворений r лінійно незалежними стовпцями підматриці A', буде ненульовим, а тому $r_{\min}(A) \ge r$. Разом із попередньою нерівністю це дає $r_{\min}(A) = r$. □

Наслідок 21. *При елементарних перетвореннях рядків і/або стовпців матриці її мінорний ранг не змінюється.*

Для квадратної матриці A порядку n особливу роль відіграють мінори $(n-1)$–го порядку. Такий мінор одержується викреслюванням із матриці одного рядка й одного стовпця. Якщо викреслюються i–й рядок та j–й стовпець, то відповідний мінор будемо називати *доповняльним* мінором елемента a_{ij} матриці A і позначати $\overline{M}{}^{j}_{i}$.

Зауваження. Аналогічно можна визначити доповняльний мінор $\overline{M}{}^{\{j_1,\dots,j_k\}}_{\{i_1,\dots,i_k\}}$ для довільного мінора $M^{\{j_1,\dots,j_k\}}_{\{i_1,\dots,i_k\}}$ квадратної матриці.

6.4. Алгебричні доповнення

Розглянемо суму тих доданків із (6.8), в яких одним із множників є елемент a_{ij}, і винесемо спільний множник за дужки:

$$\sum_{\left(\begin{smallmatrix}1 & \dots & j & \dots & n\\ i_1 & \dots & i & \dots & i_n\end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & j & \dots & n\\ i_1 & \dots & i & \dots & i_n\end{smallmatrix}\right) \cdot a_{i_1 1} \cdots a_{ij} \cdots a_{i_n n} =$$

$$= a_{ij} \cdot \left(\sum_{\left(\begin{smallmatrix}1 & \dots & j & \dots & n\\ i_1 & \dots & i & \dots & i_n\end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & j & \dots & n\\ i_1 & \dots & i & \dots & i_n\end{smallmatrix}\right) a_{i_1 1} \cdots a_{i_{j-1},j-1} \cdot a_{i_{j+1},j+1} \cdots a_{i_n n} \right). \quad (6.15)$$

Вираз у дужках у правій частині рівності (6.15) називається *алгебричним доповненням* елемента a_{ij} і позначається A_{ij}.

Для даного i в кожному доданку суми (6.8) зустрічається один і тільки один множник із i–го рядка матриці $A = (a_{ij})$. Це ж саме можна сказати і про елементи j–го стовпця. Тому з означення алгебричного доповнення елемента матриці одразу випливає така теорема.

Теорема 34 (про розклад визначника за своїм рядком або стовпцем)**.**

$$\det A = \sum_{k=1}^{n} a_{ik} A_{ik} = \sum_{k=1}^{n} a_{kj} A_{kj} \,. \quad (6.16)$$

Розклади (6.16) називають також *розкладами Лапласа*. Щоб ці розклади можна було використовувати для обчислення визначників, треба вміти обчислювати алгебричні доповнення елементів.

Теорема 35. *$A_{ij} = (-1)^{i+j} \overline{M}_i^j$, де $\overline{M}_i^j$ — доповняльний мінор елемента a_{ij}.*

Доведення. Спочатку за підстановкою

$$\pi = \begin{pmatrix} 1 & \dots & j & \dots & n \\ i_1 & \dots & i & \dots & i_n \end{pmatrix},$$

із S_n, яка визначає знак доданка $a_{i_1 1} \cdots a_{ij} \cdots a_{i_n n}$ в розкладі (6.8) визначника матриці $A = (a_{ij})$, побудуємо підстановку

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n-1 \\ l_1 & l_2 & \dots & l_{n-1} \end{pmatrix}$$

із S_{n-1} за таким правилом: викреслюємо в підстановці π стовпець $\binom{j}{i}$, а потім зменшуємо на 1 всі ті елементи верхнього рядка, які більші за j, і всі ті елементи нижнього рядка, які більші за i. Парність побудованої таким чином підстановки τ визначає знак доданка

$$a_{i_1 1} \cdots a_{i_{j-1} j-1} a_{i_{j+1} j+1} \cdots a_{i_n n}$$

в аналогічному розкладі мінора $\overline{M}_i^j$.

З'ясуємо, як пов'язані знаки підстановок π і τ. Нехай кількість тих чисел, які більші i та стоять у нижньому рядку підстановки π зліва від i, дорівнює t. Тоді зліва від i стоїть $(j-1)-t$ чисел, менших i, а решта $(i-1)-(j-1-t) = i-j+t$ чисел, менших i, стоїть справа від i. Тому кількість інверсій, які утворює число i в підстановці π, дорівнює $t+(i-j+t)$. Ці й лише ці інверсії зникають при переході від π до підстановки τ. Отже,

$$\operatorname{sign}\pi = (-1)^{i-j+2t}\operatorname{sign}\tau = (-1)^{(i+j)+2(t-j)}\operatorname{sign}\tau = (-1)^{(i+j)}\operatorname{sign}\tau\,.$$

Таким чином, кожен доданок з алгебричного доповнення

$$A_{ij} = \sum_{\left(\begin{smallmatrix}1 & \dots & j & \dots & n\\ i_1 & \dots & i & \dots & i_n\end{smallmatrix}\right)} \operatorname{sign}\left(\begin{smallmatrix}1 & \dots & j & \dots & n\\ i_1 & \dots & i & \dots & i_n\end{smallmatrix}\right) a_{i_1 1} \cdots a_{i_{j-1},j-1} \cdot a_{i_{j+1},j+1} \cdots a_{i_n n}$$

одержується множенням на $(-1)^{i+j}$ відповідного доданка з розкладу мінора $\overline{M}_i^j$. Тому $A_{ij} = (-1)^{i+j}\overline{M}_i^j$. □

Із теорем 34 і 35 одразу випливає наслідок.

Наслідок 22. *Для довільних i-го рядка та j-го стовпця виконується рівність*

$$\det A = \sum_{i=1}^{n}(-1)^{i+j}a_{ij}\overline{M}_i^j = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\overline{M}_i^j\,. \tag{6.17}$$

Зауваження. **1.** Рівність (6.17) інколи беруть за основу рекурентного означення визначника: визначник матриці порядку 1 визначають правилом $\det(a) := a$, а для $n > 1$ визначник матриці $A = (a_{ij})$ порядку n визначають через його розклад за першим рядком:

$$\det A := \sum_{k=1}^{n}(-1)^{1+k}a_{1k}\overline{M}_1^k\,.$$

2. Для практичного обчислення визначників рівність (6.17) (чи рівносильна їй рівність (6.16)) у загальному випадку є малопридатною: її послідовне застосування до визначника порядку n спочатку дасть n визначників порядку $n-1$, потім $n(n-1)$ визначників порядку $n-2$, потім $n(n-1)(n-2)$ визначників порядку $n-3$ і т. д. Зрештою, ми одержимо – із відповідними множниками – $n(n-1)(n-2)\cdots 3\cdot 2$ визначників порядку 1, тобто ті ж самі $n!$ доданків, що і в явній формулі (6.8) для обчислення визначника. Однак рівність (6.17) стає корисною, якщо майже всі коефіцієнти якогось рядка або стовпця є нульовими – тоді її використання не призводить до стрімкого зростання кількості доданків.

Як приклад використання розкладу (6.17) обчислимо так званий *визначник Вандермонда*

$$V_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{vmatrix},$$

який знадобиться нам пізніше. Спочатку від кожного рядка, починаючи з останнього і завершуючи другим, віднімемо попередній рядок, помножений на x_1. При такому перетворенні визначник не змінюється. Тоді k-й рядок отриманого визначника матиме вигляд

$$\begin{gathered}(x_1^{k-1} - x_1^{k-2}\cdot x_1, x_2^{k-1} - x_2^{k-2}\cdot x_1, \dots, x_n^{k-1} - x_n^{k-2}\cdot x_1) = \\ = (0, x_2^{k-2}(x_2 - x_1), \dots, x_n^{k-2}(x_n - x_1)).\end{gathered}$$

Тому

$$V_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & x_2 - x_1 & x_3 - x_1 & \dots & x_n - x_1 \\ 0 & x_2(x_2 - x_1) & x_3(x_3 - x_1) & \dots & x_n(x_n - x_1) \\ \dots & \dots & \dots & \dots & \dots \\ 0 & x_2^{n-2}(x_2 - x_1) & x_3^{n-2}(x_3 - x_1) & \dots & x_n^{n-2}(x_n - x_1) \end{vmatrix}.$$

Розкриємо цей визначник за першим стовпцем, а потім із кожного стовпця винесемо спільний лінійний множник:

$$V_n = (-1)^{1+1} \cdot 1 \cdot \begin{vmatrix} x_2 - x_1 & x_3 - x_1 & \dots & x_n - x_1 \\ x_2(x_2 - x_1) & x_3(x_3 - x_1) & \dots & x_n(x_n - x_1) \\ \dots & \dots & \dots & \dots \\ x_2^{n-2}(x_2 - x_1) & x_3^{n-2}(x_3 - x_1) & \dots & x_n^{n-2}(x_n - x_1) \end{vmatrix} =$$

$$= (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1) \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_2 & x_3 & \dots & x_n \\ x_2^2 & x_3^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_2^{n-2} & x_3^{n-2} & \dots & x_n^{n-2} \end{vmatrix}.$$

Останнім множником ми отримали знову визначник Вандермонда, тільки його порядок на одиницю менший. Застосовуючи до нього аналогічні міркування, одержимо

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_2 & x_3 & \dots & x_n \\ x_2^2 & x_3^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_2^{n-2} & x_3^{n-2} & \dots & x_n^{n-2} \end{vmatrix} = (x_3 - x_2)(x_4 - x_2) \cdots (x_n - x_2) \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_3 & x_4 & \dots & x_n \\ x_3^2 & x_4^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_3^{n-3} & x_4^{n-3} & \dots & x_n^{n-3} \end{vmatrix}.$$

Ми знову отримали визначник Вандермонда, тільки його порядок уже менший на 2. Міркуючи подібним чином далі, ми зрештою одержимо

$$V_n = (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1) \cdot (x_3 - x_2)(x_4 - x_2) \cdots (x_n - x_2) \cdots$$
$$\cdots (x_{n-1} - x_{n-2})(x_n - x_{n-2}) \cdot (x_n - x_{n-1}) = \prod_{n \geq j > i \geq 1} (x_j - x_i).$$

Зауважимо, що визначник Вандермонда дорівнює 0 тоді й лише тоді, коли серед чисел $x_1, x_2, \cdots, x_n$ є однакові.

Теорема 36 (про розклад визначника за чужим рядком або стовпцем)**.** *Якщо $i \neq j$, то*

$$\sum_{k=1}^{n} a_{jk} A_{ik} = \sum_{k=1}^{n} a_{kj} A_{ki} = 0\,. \tag{6.18}$$

Доведення. Із теореми 35 випливає, що коли елемент a_{kj} матриці $A = (a_{kj})$ замінити якимось іншим елементом a'_{kj}, то його алгебричне доповнення A_{kj} не зміниться – при обчисленні A_{kj} k-й рядок та j-й стовпець викреслюються. Розглянемо тепер матрицю A', яка одержується з A заміною

її i-го рядка j-м (тобто $a'_{ik} = a_{jk}$). Тоді алгебричні доповнення елементів i-го рядка матриці A' збігаються з алгебричними доповненнями відповідних елементів i-го рядка матриці A.

Оскільки $i \neq j$, то матриця A' має два однакових рядки. Тому її визначник дорівнює 0. Разом із рівністю (6.16) це дає

$$0 = \det A' = \sum_{k=1}^{n} a'_{ik} A_{ik} = \sum_{k=1}^{n} a_{jk} A_{ik}.$$

Друга з рівностей (6.18) доводиться аналогічно. □

Замінимо кожен елемент a_{ij} квадратної матриці $A = (a_{ij})$ його алгебричним доповненням A_{ij}. Транспонована до утвореної матриці матриця $A^* = (A_{ij})$ називається *приєднаною* до матриці A.

Теорема 37 (про явний вигляд оберненої матриці)**.** *Якщо визначник матриці $A = (a_{ij})$ не дорівнює 0, то обернена до A матриця існує і має вигляд*

$$A^{-1} = \frac{1}{\det A} \cdot (A^*)^\top = \frac{1}{\det A} \cdot (A_{ji}). \tag{6.19}$$

Доведення. Добуток i-го рядка матриці A на j-й стовпець матриці $(A^*)^\top$ – це добуток i-го рядка матриці A на її j-й рядок, тобто сума

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn}.$$

Якщо $i = j$, то ця сума дорівнює $\det A$ (теорема 34 про розклад визначника за своїм рядком). У противному разі ця сума дорівнює 0 (теорема 36 про розклад визначника за чужим рядком). Тому

$$A \cdot (A^*)^\top = \begin{pmatrix} \det A & 0 & \dots & 0 \\ 0 & \det A & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \det A \end{pmatrix} = \det A \cdot E, \tag{6.20}$$

де E — одинична матриця. □

Зрозуміло, що коли коефіцієнтами матриці A є цілі числа, то такими будуть і коефіцієнти матриці A^*. Тому з теореми 6.19 одразу випливає такий наслідок.

Наслідок 23. *Якщо визначник матриці A із цілими коефіцієнтами дорівнює ± 1, то обернена матриця A^{-1} також має цілі коефіцієнти.*

Для теоретичних міркувань інколи зручно мати формули, які б не вимагали зведення системи лінійних рівнянь до трапецієподібного вигляду, а виражали її розв'язок безпосередньо через коефіцієнти системи. Для визначених квадратних систем такі формули справді існують, хоча й малопридатні для практичного використання.

Теорема 38 (Крамер). *Квадратна система лінійних рівнянь $A\boldsymbol{x} = \boldsymbol{b}$ буде визначеною тоді й лише тоді, коли її основна матриця A є невиродженою. Якщо матриця A — невироджена, то єдиний розв'язок $(x_1, x_2, \ldots, x_n)$ системи $A\boldsymbol{x} = \boldsymbol{b}$ знаходимо за формулами*

$$x_k = \frac{\Delta_k}{\Delta}, \qquad k = 1, 2, \ldots, n, \tag{6.21}$$

де Δ — визначник матриці A, а Δ_k — визначник матриці, яку одержуємо з A заміною k-го стовпця стовпцем $\boldsymbol{b}$ вільних членів.

Доведення. Перша частина теореми випливає із другої теореми Кронекера – Капеллі: квадратна система $A\boldsymbol{x} = \boldsymbol{b}$ буде визначеною тоді й лише тоді, коли ранг матриці A дорівнює її порядку, тобто, коли матриця A – невироджена.

Нехай тепер матриця A є невиродженою і $(x_1, \ldots, x_n)$ – розв'язок системи $A\boldsymbol{x} = \boldsymbol{b}$. Тоді

$$x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n = \boldsymbol{b}\,,$$

де $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ — стовпці матриці A. Враховуючи, що при додаванні до одного зі стовпців матриці лінійної комбінації інших стовпців її визначник не змінюється, отримуємо

$$x_k\Delta = x_k \det(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \ldots, \boldsymbol{a}_n) = \det(\boldsymbol{a}_1, \ldots, x_k\boldsymbol{a}_k, \ldots, \boldsymbol{a}_n) =$$
$$= \det(\boldsymbol{a}_1, \ldots, \boldsymbol{b} - x_1\boldsymbol{a}_1 - \cdots - x_{k-1}\boldsymbol{a}_{k-1} - x_{k+1}\boldsymbol{a}_{k+1} - \cdots - x_n\boldsymbol{a}_n, \ldots, \boldsymbol{a}_n) =$$
$$= \det(\boldsymbol{a}_1, \ldots, \boldsymbol{b}, \ldots, \boldsymbol{a}_n) = \Delta_k\,.$$

Позаяк $\Delta \neq 0$, то $x_k = \dfrac{\Delta_k}{\Delta}$. □

Формули (6.21) називаються *формулами Крамера* або *правилом Крамера*.

За правилом Крамера для знаходження розв'язку квадратної системи порядку n потрібно обчислити $n + 1$ визначників порядку n. Це вимагає набагато більших обчислень, ніж метод Гаусса. Іншим суттєвим недоліком формул Крамера є "чутливість" визначників до зміни їх коефіцієнтів: незначна зміна останніх, наприклад, у межах похибки вимірювання,

може приводити до зміни визначника в багато разів (детальніше обґрунтування цього твердження вимагає знайомства з теорією наближених обчислень). У той же час для більшості СЛР , що виникають на практиці, коефіцієнти відомі лише наближено.

Теорема 39 (Коші)**.** *Для довільних квадратних матриць A і B однакового порядку виконується рівність*

$$\det(AB) = \det A \cdot \det B\,. \tag{6.22}$$

Доведення. Нехай A і B — матриці порядку n. Якщо $\det A = 0$, то $\operatorname{rank} A < n$. Але тоді, за наслідком 17, $\operatorname{rank} AB \le \operatorname{rank} A < n$ і $\det(AB) = 0$. Тому в цьому разі $\det(AB) = 0 = \det A \cdot \det B$.

Аналогічно розбирається випадок $\det B = 0$. Тому далі можна вважати, що $\det A \neq 0$ і $\det B \neq 0$.

Оскільки в цьому випадку матриця A є невиродженою, то елементарними перетвореннями рядків (причому, не використовуючи множення рядка на число) її можна звести до діагонального вигляду. Але елементарному перетворенню рядків відповідає множення зліва на відповідну елементарну матрицю. Отже, існують такі елементарні матриці $A_1, \ldots, A_m$, що

$$A_m \cdots A_1 A = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_n \end{pmatrix}. \tag{6.23}$$

Якщо при зведенні A до діагонального вигляду перестановка рядків виконувалася p разів, то із цієї рівності випливає, що

$$(-1)^p \det A = \det(A_m \cdots A_1 A) = a_1 a_2 \cdots a_n.$$

Аналогічно, зводячи невироджену матрицю B до діагонального вигляду елементарними перетвореннями стовпців, одержуємо рівності

$$BB_1 \cdots B_k = \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ 0 & b_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_n \end{pmatrix} \tag{6.24}$$

і

$$(-1)^q \det B = \det(BB_1 \cdots B_k) = b_1 b_2 \cdots b_n,$$

де q – кількість перестановок стовпців при зведенні B до діагонального вигляду. Із рівностей (6.23) і (6.24) випливає, що

$$A_m \cdots A_1 ABB_1 \cdots B_k =$$
$$= \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 & 0 & \dots & 0 \\ 0 & b_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & 0 & \dots & 0 \\ 0 & a_2 b_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n b_n \end{pmatrix}.$$

З іншого боку, добуток $A_m \cdots A_1 ABB_1 \cdots B_k$ можна розглядати як застосування до матриці елементарних перетворень рядків (яким відповідають елементарні матриці $A_1, \dots, A_m$), а потім елементарних перетворень стовпців (яким відповідають елементарні матриці $B_1, \dots, B_k$). Оскільки при цьому виконується p перестановок рядків і q перестановок стовпців, то

$$(-1)^{p+q} \det(AB) = \det(A_m \cdots A_1 ABB_1 \cdots B_k) = a_1 b_1 \cdot a_2 b_2 \cdots a_n b_n.$$

Але

$$a_1 b_1 \cdot a_2 b_2 \cdots a_n b_n = a_1 a_2 \cdots a_n \cdot b_1 b_2 \cdots b_n = (-1)^p \det A \cdot \det(-1)^q B.$$

Отже, і в цьому випадку $\det(AB) = \det A \cdot \det B$. □

Наслідок 24. *Якщо матриця A є невиродженою, то*

$$\det A^{-1} = \frac{1}{\det A}.$$

Наслідок 25. *Нехай A є квадратною матрицею із цілими коефіцієнтами. Обернена матриця A^{-1} буде мати цілі коефіцієнти тоді й лише тоді, коли* $\det A = \pm 1$.

Доведення. Достатність умови вже доведено – це наслідок 23. Необхідність випливає з рівностей

$$1 = \det E = \det(A \cdot A^{-1}) = \det A \cdot \det A^{-1}.$$

Справді, якщо $\det A \neq \pm 1$, то $\det A^{-1}$ не є цілим числом, а тому матриця A^{-1} не може мати цілі коефіцієнти. □

Вправа 17. *Наведіть контрприклад до рівності*

$$\det(A + B) = \det A + \det B.$$

6.5. Задачі

6.1. Нехай A — квадратна матриця порядку 3. Знайдіть найбільше значення, якого може набувати $\det A$, якщо

а) усі коефіцієнти матриці A дорівнюють ± 1;

б) усі коефіцієнти матриці A дорівнюють 0 або 1[15].

6.2. Нехай усі функції f_{ij} — диференційовні. Доведіть, що

а)
$$\begin{vmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots \\ f_{n1} & f_{n2} & \dots & f_{nn} \end{vmatrix}' =$$

$$= \sum_{i=1}^{n} \begin{vmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ \dots & \dots & \dots & \dots \\ f'_{i1} & f'_{i2} & \dots & f'_{in} \\ \dots & \dots & \dots & \dots \\ f_{n1} & f_{n2} & \dots & f_{nn} \end{vmatrix} = \sum_{j=1}^{n} \begin{vmatrix} f_{11} & \dots & f'_{1j} & \dots & f_{1n} \\ f_{21} & \dots & f'_{2j} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ f_{n1} & \dots & f'_{nj} & \dots & f_{nn} \end{vmatrix}.$$

б)
$$\begin{vmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots \\ f_{n1} & f_{n2} & \dots & f_{nn} \end{vmatrix}' = \sum_{i,j=1}^{n} \frac{df_{ij}}{dx} A_{ij}.$$

6.3. *Вронскіаном* набору $f_1(x), f_2(x), \dots, f_n(x)$ диференційовних функцій називається визначник

$$\begin{vmatrix} f_1 & f_2 & \dots & f_n \\ f'_1 & f'_2 & \dots & f'_n \\ \dots & \dots & \dots & \dots \\ f_1^{(n-2)} & f_2^{(n-2)} & \dots & f_n^{(n-2)} \\ f_1^{(n-1)} & f_2^{(n-1)} & \dots & f_n^{(n-1)} \end{vmatrix}.$$

Знайдіть його похідну.

6.4. Доведіть, що завжди існує матриця $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$ із заданими значеннями мінорів $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = P$, $\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} = Q$, $\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} = R$.

[15] Ця задача є частковим випадком *проблем Адамара* (у загальному випадку досі нерозв'язаних): якого найбільшого значення може набувати визначник n–го порядку, якщо всі його елементи належать множині $\{-1, 1\}$ або множині $\{0, 1\}$?

6.5. Нехай $\operatorname{rank} A = r$, $k < r$ і $M^{\{j_1,\dots,j_k\}}_{\{i_1,\dots,i_k\}}$ — ненульовий мінор порядку k. Доведіть, що існують такі індекси i та j, що мінор $M^{\{j,j_1,\dots,j_k\}}_{\{i,i_1,\dots,i_k\}}$ порядку $k+1$ також буде ненульовим.

6.6. Нехай у матриці A є ненульовий мінор M порядку k, а всі мінори порядку $k+1$, які містять мінор M, дорівнюють 0. Доведіть, що $\operatorname{rank} A = k$.

6.7*. (**Формула Біне – Коші**) Доведіть, що мінор k-го порядку матриці AB виражається через мінори матриць A і B таким чином:

$$M^{\{j_1,\dots,j_k\}}_{\{i_1,\dots,i_k\}}(AB) = \sum_{\{l_1,\dots,l_k\}} M^{\{l_1,\dots,l_k\}}_{\{i_1,\dots,i_k\}}(A) \cdot M^{\{j_1,\dots,j_k\}}_{\{l_1,\dots,l_k\}}(B)\,.$$

6.8. Квадратна матриця A називається *цілком невід'ємною* (відповідно *цілком додатною*), якщо всі мінори всіх можливих порядків цієї матриці є невід'ємними (відповідно додатними). Доведіть, що добуток двох цілком невід'ємних (цілком додатних) матриць також буде цілком невід'ємною (цілком додатною) матрицею.

6.9. Нехай A — матриця порядку n і $r(A) < n$. Доведіть, що для довільного i набір $(A_{i1}, A_{i2}, \dots, A_{in})$ алгебричних доповнень буде розв'язком однорідної системи лінійних рівнянь $A\boldsymbol{x} = \boldsymbol{0}$.

6.10*. Нехай $A = (a_{ij})$ — невироджена квадратна матриця порядку n, M — мінор матриці A^{-1}, M' — алгебричне доповнення відповідного мінора матриці $A^\top$. Доведіть, що $M \cdot |A| = M'$.

6.11*. Нехай A — матриця порядку n і $N = \{1, 2, \dots, n\}$. *Алгебричним доповненням* мінора $M^{\{j_1,\dots,j_k\}}_{\{i_1,\dots,i_k\}}$ порядку k називається мінор $M^{N\setminus\{j_1,\dots,j_k\}}_{N\setminus\{i_1,\dots,i_k\}}$ порядку $n-k$, узятий зі знаком $(-1)^{i_1+\dots+i_k+j_1+\dots+j_k}$. Доведіть **теорему Лапласа:** якщо у квадратній матриці A порядку n довільним чином вибрано k рядків (або k стовпців), $1 \le k < n$, то сума добутків усіх мінорів порядку k, що містяться у вибраних рядках (стовпцях), на їх алгебричні доповнення дорівнює $\det A$.

6.12*. Нехай A – дійсна $(m\times n)$-матриця і $m \ge n$. Доведіть, що $\det(A^\top \cdot A) = \sum_M M^2$, де сума береться по всіх $\binom{m}{n}$ мінорах M порядку n матриці A.

6.13. *Кутовим мінором* порядку k квадратної матриці називається мінор $M^{\{1,2,\dots,k\}}_{\{1,2,\dots,k\}}$. Нехай усі кутові мінори матриці A не дорівнюють 0. Доведіть, що A можна розкласти в добуток $A = UB$ нижньої трикутної матриці U з одиницями на діагоналі і верхньої трикутної матриці B, причому такий розклад єдиний.

6.14. Доведіть такі властивості приєднаної матриці:

а) $(A^\top)^* = (A^*)^\top$; б) $(A^{-1})^* = (A^*)^{-1}$; в)* $(AB)^* = B^*A^*$.

6.15. Нехай A – квадратна матриця порядку n. Доведіть, що $|A^*| = |A|^{n-1}$.

6.16. Доведіть, що коли матриця A

а) симетрична або кососиметрична непарного порядку, то приєднана матриця A^* – симетрична;

б) кососиметрична парного порядку, то приєднана матриця A^* – кососиметрична.

6.17*. Доведіть, що

а) кожна невироджена матриця є асоційованою з деякою матрицею;

б) кожна квадратна матриця рангу 1 є асоційованою з деякою матрицею.

6.18*. Доведіть, що кожну матрицю A другого порядку, в якої сума діагональних елементів дорівнює 0, можна подати у вигляді $A = XY - YX$.

6.19*. Доведіть, що

$$\begin{vmatrix} \binom{k}{r} & \binom{k}{r+1} & \dots & \binom{k}{r+n-1} \\ \binom{k+1}{r} & \binom{k+1}{r+1} & \dots & \binom{k+1}{r+n-1} \\ \dots & \dots & \dots & \dots \\ \binom{k+n-1}{r} & \binom{k+n-1}{r+2} & \dots & \binom{k+n-1}{r+n-1} \end{vmatrix} = \frac{\binom{n+k-1}{n}\binom{n+k-2}{n}\dots\binom{n+k-r}{n}}{\binom{n+r-1}{n}\binom{n+r-2}{n}\dots\binom{n}{n}}.$$

6.20**. Нехай ε — первісний корінь степеня n з 1. Доведіть, що

$$\begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{vmatrix} = \prod_{k=0}^{n-1} (a_0 + \varepsilon^k a_1 + \varepsilon^{2k} a_2 + \dots + \varepsilon^{(n-1)k} a_{n-1}).$$

6.21* Нехай A, B, C і D — комплексні матриці однакового порядку, причому матриці C і D — невироджені й комутують. Доведіть, що $\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = 0$ тоді й лише тоді, коли $\det(AD - BC) = 0$.

6.22** Доведіть, що довільний набір $a_1, a_2, \ldots, a_n$ взаємно простих цілих чисел можна взяти за елементи першого рядка деякої цілочислової матриці з визначником 1.

7. Кільця класів лишків

7.1. Бінарні відношення

У попередніх розділах ми вже зустрічалися з поняттям відношення еквівалентності (див. підрозділ 1.2) і різними прикладами таких відношень. Зупинимось трохи докладніше на властивостях відношень узагалі і відношень еквівалентності зокрема.

Нагадаємо, що *відношенням* (або *бінарним відношенням*) на непорожній множині M називається довільна підмножина $\Re \subseteq M \times M$ декартового квадрата множини M. Той факт, що елементи x і y *є у відношенні* $\Re$ (тобто що впорядкована (x, y) належить відношенню $\Re$) зазвичай позначають $x\Re y$.

У математиці і поза нею є багато прикладів різних природних бінарних відношень. Ось лише деякі:

1. Відношення *рівності* "$=$", *строгого порядку* "$<$" або *нестрогого порядку* "$\leq$" на різних числових множинах.

2. Відношення *подільності* "$a \mid b$" (a ділить b) на множині цілих або натуральних чисел.

3. Відношення *паралельності* "$\|$" або перпендикулярності "$\perp$" на множині всіх прямих площини.

4. Відношення *подібності* на множині всіх фігур площини.

5. Відношення "*бути родичем*" або "*бути підлеглим*" на множині людей.

Дуже часто розглядають лише такі бінарні відношення $\Re$, які задовольняють певні додаткові умови. Серед таких додаткових умов найважливішими є такі:

а) *рефлексивність*: якщо $a\Re a$ для всіх $a \in M$;

б) *антирефлексивність*: якщо $(a, a) \notin \Re$ для всіх $a \in M$;

в) *симетричність*: якщо для всіх $a, b \in M$ із $a\Re b$ випливає $b\Re a$;

г) *антисиметричність*: якщо для всіх $a, b \in M$ із $a\Re b$ і $b\Re a$ випливає $a = b$;

д) *транзитивність*: якщо для всіх $a, b, c \in M$ із $a\Re b$ і $b\Re c$ випливає $a\Re c$.

Бінарне відношення, яке є рефлексивним, транзитивним та антисиметричним, називається відношенням *часткового порядку* (або просто відношенням порядку, або частковим порядком). Для позначення часткового порядку зазвичай використовують символ $\leq$. Сама ж множина

із заданим на ній частковим порядком називається *частково впорядкованою*.

Приклади частково впорядкованих множин:

1. Множина натуральних $\mathbb{N}$, цілих $\mathbb{Z}$, раціональних $\mathbb{Q}$ або дійсних $\mathbb{R}$ чисел зі звичайним відношенням порядку.

2. Множина $\mathfrak{B}(M)$ усіх підмножин деякої множини M відносно теоретико-множинного включення $\subseteq$.

3. Відношення *подільності* "$a \mid b$" (a ділить b) на множині $\mathbb{N}$ натуральних чисел також є відношенням часткового порядку.

Кажуть, що два елементи a та b частково впорядкованої множини M є *порівнянними*, якщо $a \leq b$ або $b \leq a$. Як видно із двох останніх прикладів, у частково впорядкованій множині можуть бути непорівнянні елементи (наприклад, дві підмножини однакової скінченної потужності в $\mathfrak{B}(M)$ або два прості числа в $\mathbb{N}$). Саме тому порядок називається частковим. Якщо ж будь-які два елементи є порівнянними, то порядок називається *лінійним*, а частково впорядкована множина – *лінійно впорядкованою* (або *ланцюгом*). Лінійним є звичайний порядок $\leq$ на множинах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ або $\mathbb{R}$.

Поруч із відношенням часткового порядку $\leq$ часто розглядають відношення *строгого часткового порядку* $<$. Воно так само є транзитивним та антисиметричним, але замість рефлексивності вимагають антирефлексивність. Строгим частковим порядком буде звичайне відношення $<$ на множинах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ та відношення строгого включення $\subset$ на $\mathfrak{B}(M)$.

Відношення, яке є лише рефлексивним і транзитивним, називають *квазіпорядком*. Таким, зокрема, є відношення подільності на множині $\mathbb{Z}$.

Другим важливим класом бінарних відношень, поруч із частковими порядками, є відношення еквівалентності. Нагадаємо, що *відношенням еквівалентності* на множині M називається таке бінарне відношення на M, яке є рефлексивним, симетричним та транзитивним. Найчастіше відношення еквівалентності позначається символом $\sim$. Якщо $a \sim b$, то кажуть, що елемент a еквівалентний елементу b.

Зі згаданих раніше прикладів відношеннями еквівалентності будуть відношення рівності (на довільній множині), відношення паралельності на множині прямих площини, відношення подібності на множині фігур площини та відношення "*бути родичем*" на множині людей.

Множина $\overline{a} = \{b \in M \mid a \sim b\}$ всіх елементів, еквівалентних елементу a, називається *класом еквівалентності* елемента a.

Із рефлексивності відношення еквівалентності випливає, що $a \in \overline{a}$. Крім того, як показано у твердженні 1, два класи еквівалентності $\overline{a}$ і $\overline{b}$ або не перетинаються, або збігаються. Тому, якщо $b \in \overline{a}$, то $\overline{b} = \overline{a}$. Це означає, що довільний елемент класу еквівалентності можна вибирати *представником* цього класу.

Оскільки кожен елемент $a \in M$ належить класу $\overline{a}$, то об'єднання всіх класів еквівалентності збігається з M. Таким чином, множина класів еквівалентності відношення $\sim$ утворює розбиття множини M, тобто M розпадається в об'єднання множин, що не перетинаються.

Справедливе і зворотне твердження:

Твердження 43. *Довільне розбиття $M = \bigcup_{i \in I} M_i$ множини M визначає на M відношення еквівалентності, класи еквівалентності якого збігаються із блоками M_i, $i \in I$, цього розбиття.*

Доведення. Справді, покладемо $x \sim y$ тоді й лише тоді, коли x та y належать одному блокові M_i даного розбиття. Очевидно, що $\sim$ є відношенням еквівалентності, класи еквівалентності якого збігаються із блоками M_i. □

Приклад 13. Нехай M – множина студентів механіко-математичного факультету. Множина M розбивається на академічні групи. Відповідне відношення еквівалентності виглядає так: $x \sim y$ тоді й лише тоді, коли студенти x та y вчаться в одній академічній групі.

Сукупність $\{\overline{a} \mid a \in M\}$ класів еквівалентності називається *фактор-множиною* множини M за відношенням еквівалентності $\sim$ і позначається $M/\sim$. Наголошуємо, що елементами фактор-множини $M/\sim$ є саме класи еквівалентності, а не елементи множини M. Так, у прикладі зі студентами мехмату M елементами фактор-множини будуть не студенти, а академічні групи.

Для кожної фактор-множини $M/\sim$ визначається сюр'єктивне відображення $\pi : M \to M/\sim$, $\pi(x) := \overline{x}$, яке називається *канонічною проекцією* M на фактор-множину $M/\sim$ або *відображенням факторизації*.

Нехай тепер на множині M задана деяка бінарна *дія* (або *операція*) $* : M \times M \to M$, тобто правило, яке кожній упорядкованій парі (a, b) елементів множини M ставить у відповідність єдиним чином визначений елемент $a * b$ цієї множини. Прикладами є звичні нам дії додавання і

множення цілих (раціональних, дійсних, комплексних) чисел, додавання векторів, множення підстановок, додавання і множення матриць, знаходження найбільшого спільного дільника та найменшого спільного кратного двох натуральних чисел, операції об'єднання, перетину та симетричної різниці підмножин деякої множини тощо.

Кажуть, що відношення еквівалентності $\sim$ на множині M *узгоджене з дією* $*$, якщо з того, що $a \sim a'$ та $b \sim b'$, випливає, що $a * b \sim a' * b'$.

Якщо відношення еквівалентності $\sim$ узгоджене з дією $*$, то на фактор-множині $M/\sim$ можна визначити індуковану дію за правилом:

$$\overline{a} * \overline{b} := \overline{a * b}. \tag{7.1}$$

Таке визначення дії на $M/\sim$ є коректним, бо не залежить від вибору представників класів $\overline{a}$ і $\overline{b}$. Справді, у разі вибору інших представників $a' \in \overline{a}$ і $b' \in \overline{b}$ маємо: $a \sim a$ і $b \sim b$. Але тоді з узгодженості дії з відношенням еквівалентності випливає, що $a' * b' \sim a * b$. Тому $\overline{a' * b'} = \overline{a * b}$.

Зазвичай ті операції на множинах, що виникають у математиці, мають певні властивості, список яких регулярно повторюється. Найважливішими із цих властивостей є:

(1) *асоціативність*: для довільних елементів x, y та z виконується рівність $(x * y) * z = x * (y * z)$;

(2) *комутативність*: для довільних елементів x та y справедлива рівність $x * y = y * x$;

(3) *існування нейтрального елемента*: існує такий елемент e, що для кожного x справджується рівність $e * x = x * e = x$;

(4) *існування оберненого елемента*: для кожного елемента x існує такий елемент x', що $x * x' = x' * x = e$.

Твердження 44. *Нехай відношення еквівалентності $\sim$ на множині M і дія $*$ — узгоджені. Якщо дія $*$ має якусь властивість із списку* (1)–(4)*, то визначена правилом* (7.1) *індукована дія на фактор-множині $M/\sim$ також має цю властивість.*

Доведення. Нехай дія $*$ на множині M є асоціативною. Тоді

$$(\overline{x} * \overline{y}) * \overline{z} = \overline{x * y} * \overline{z} = \overline{(x * y) * z} = \overline{x * (y * z)} = \overline{x} * \overline{y * z} = \overline{x} * (\overline{y} * \overline{z}).$$

Отже, індукована дія на фактор-множині $M/\sim$ також є асоціативною.

Збереження комутативності перевіряється аналогічно.

Із рівності

$$\overline{x} * \overline{e} = \overline{x * e} = \overline{x}$$

випливає, що коли e є нейтральним елементом для множини M, то клас $\overline{e}$ є нейтральним елементом для фактор-множини $M/\sim$.

Нарешті, якщо $x * x' = x' * x = e$, то

$$\overline{x} * \overline{x'} = \overline{x * x'} = \overline{e} = \overline{x' * x} = \overline{x'} * \overline{x}.$$

Отже, клас $\overline{x'}$ є оберненим до класу $\overline{x}$. □

7.2. Кільця і поля

Нагадаємо (див. підрозділ 1.2), що *кільцем* називається непорожня множина K, в якій визначено додавання і множення елементів, причому ці операції задовольняють такі умови:

а) відносно додавання множина K утворює комутативну групу;

б) множення є асоціативним, тобто для довільних елементів x, y та z виконується рівність $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

в) дії додавання та множення поєднані дистрибутивними законами, тобто для довільних елементів x, y та z маємо

$$(x + y) \cdot z = x \cdot z + y \cdot z, \qquad x \cdot (y + z) = x \cdot y + x \cdot z.$$

Кільце K називається *комутативним*, якщо множення є комутативним (тобто $x \cdot y = y \cdot x$ для довільних $x, y \in K$). Якщо для множення є нейтральний елемент (який для кілець традиційно називається *одиницею* і позначається символом 1), то кільце називається *кільцем з одиницею*.

Приклад 14. 1. Множина $\mathbb{Z}$ цілих чисел зі звичними додаванням та множенням утворює комутативне кільце з одиницею.

2. Множина $2\mathbb{Z}$ парних цілих чисел зі звичними додаванням та множенням утворює комутативне кільце, але без одиниці.

3. Множина дійсних квадратних матриць $M_n(\mathbb{R})$ порядку n відносно додавання та множення матриць утворює кільце з одиницею (нею буде одинична матриця). Якщо $n > 1$, то це кільце буде некомутативним.

4. Множина $\mathrm{Map}(\mathbb{R})$ усіх дійсних функцій зs звичайними додаванням та множенням функцій утворює комутативне кільце з одиницею. Тут нейтральним елементом (нулем) для додавання буде функція, яка тотожно

дорівнює нулю, а нейтральним елементом (одиницею) для множення — функція, яка тотожно дорівнює одиниці.

Вправа 18. *Перевірте, що множина* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *цілих гауссових чисел відносно додавання та множення комплексних чисел утворює комутативне кільце з одиницею.*

Комутативне кільце з одиницею, в якому для кожного ненульового елемента існує обернений, називається *полем*. У нас уже були приклади числових полів – множини раціональних $\mathbb{Q}$, дійсних $\mathbb{R}$ та комплексних $\mathbb{C}$ чисел. У наступному підрозділі ми познайомимося з важливими прикладами нечислових полів.

7.3. Кільця класів лишків

Зафіксуємо натуральне число n. Будемо говорити, що цілі числа a і b *порівнянні* (або *конгруентні*) *за модулем числа* n (і записувати $a \equiv b \pmod{n}$), якщо різниця $a - b$ ділиться на n. Вираз вигляду $a \equiv b \pmod{n}$ називатимемо *конгруенцією за модулем* n.

Твердження 45. $a \equiv b \pmod{n}$ *тоді й лише тоді, коли* a *і* b *мають однакові остачі від ділення на* n.

Доведення. Поділимо a і b на n з остачею: $a = nq_1 + r_1$ і $b = nq_2 + r_2$, де $r_1, r_2 \in \{0, 1, \ldots, n-1\}$. За означенням $a \equiv b \pmod{n}$) тоді й лише тоді, коли $a - b$ ділиться на n. Оскільки

$$a - b = n(q_1 - q_2) + (r_1 - r_2),$$

то $a - b$ ділиться на n тоді й лише тоді, коли на n ділиться різниця $r_1 - r_2$. Але $0 \leq |r_1 - r_2| < n$. Тому $r_1 - r_2$ ділиться на n тоді й лише тоді, коли $r_1 - r_2 = 0$, тобто, коли $r_1 = r_2$. □

Із цього твердження одразу випливає, що відношення конгруентності за модулем числа n є відношенням еквівалентності. Класи еквівалентності цього відношення називаються *класами лишків за модулем числа* n. Клас лишків, що містить число a, позначають $\overline{a}$. Зрозуміло, що

$$\overline{a} = \{\ldots, -2n + a, -n + a, a, n + a, 2n + a, 3n + a, \ldots\}.$$

Наслідок 26. *Є рівно* n *різних класів лишків за модулем числа* n. *Існує природна взаємно однозначна відповідність між класами лишків за модулем числа* n *та остачами від ділення на* n.

Множину класів лишків за модулем числа n (тобто фактор-множину множини $\mathbb{Z}$ за відношенням конгруентності за модулем n) позначають $\mathbb{Z}_n$.

Зауваження. Відношення $a \equiv b \pmod{n}$ можна визначати для довільного цілого числа n. Але для $n = 0$ всі класи еквівалентності виходять одноелементними (тобто відношення $a \equiv b \pmod{0}$ збігається з відношенням рівності), для $n = 1$ отримуємо лише один клас еквівалентності, а відношення $a \equiv b \pmod{n}$ і $a \equiv b \pmod{(-n)}$ очевидним чином збігаються. Тому далі ми вважатимемо, що $n > 1$.

Систему з n чисел, узятих по одному з кожного класу лишків за модулем n, називають *повною системою лишків*. При $n = 5$ повними системами лишків є, наприклад, такі системи: $\{0, 1, 2, 3, 4\}$, $\{-2, -1, 0, 1, 2\}$, $\{21, 5, -3, 14, -7\}$ і т. д. Перша система складається з найменших невід'ємних лишків із кожного класу, друга – із найменших за абсолютним значенням лишків із кожного класу, третя – з випадкових 5 чисел, узятих по одному з кожного класу.

Теорема 40. *Якщо* $a_1 \equiv b_1 \pmod{n}$ *і* $a_2 \equiv b_2 \pmod{n}$, *то*
а) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$;
б) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$.

Доведення. Якщо $a_1 \equiv b_1 \pmod{n}$ і $a_2 \equiv b_2 \pmod{n}$, то кожне з чисел $a_1 - b_1$ і $a_2 - b_2$ ділиться на n. Але тоді число

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2)$$

також ділиться на n. Тому $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$. На n ділиться і число

$$a_1 \cdot a_2 - b_1 \cdot b_2 = a_1 \cdot a_2 - a_1 \cdot b_2 + a_1 \cdot b_2 - b_1 \cdot b_2 = a_1 \cdot (a_2 - b_2) + (a_1 - b_1) \cdot b_2.$$

Тому $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$. □

Таким чином, відношення конгруентності за модулем числа n узгоджене з додаванням та множенням цілих чисел. Це дозволяє нам визначити додавання і множення класів лишків:

$$\overline{a} + \overline{b} := \overline{a + b}\,; \quad \overline{a} \cdot \overline{b} := \overline{ab}\,. \tag{7.2}$$

Наприклад, за модулем 5 маємо $\overline{2}+\overline{4} = \overline{6}$, $\overline{3}\cdot\overline{4} = \overline{12}$. Але за модулем 5 $\overline{6} = \overline{1} = \overline{11} = \overline{-4} = \ldots$, $\overline{12} = \overline{2} = \overline{7} = \overline{17} = \ldots$. Тому за модулем 5

будуть правильними і рівності $\overline{2}+\overline{4}=\overline{1}$, $\overline{2}+\overline{4}=\overline{-4}$, $\overline{3}\cdot\overline{4}=\overline{7}$ тощо. Щоб уникнути вказаної неоднозначності, традиційно представниками різних класів лишків за модулем n вибирають повну систему лишків $\{0,1,\ldots,n-1\}$. Тоді $\mathbb{Z}_n=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}$.

Приклад 15. Таблиці додавання та множення для $\mathbb{Z}_5=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$ мають вигляд

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Приклад 16. Таблиці додавання та множення для $\mathbb{Z}_6=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$ мають вигляд:

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

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Теорема 41. *Відносно додавання і множення множина $\mathbb{Z}_n$ утворює комутативне кільце з одиницею.*

Доведення. У кільці $\mathbb{Z}$ цілих чисел додавання є асоціативним, комутативним, для додавання є нейтральний елемент 0, і для кожного числа існує протилежне. Так само множення є асоціативним, комутативним і для множення є нейтральний елемент 1. Оскільки відношення конгруентності за модулем n узгоджене з додаванням та множенням цілих чисел, то із твердження 44 випливає, що всі ці властивості мають і додавання та множення в $\mathbb{Z}_n$. Лишається тільки перевірити, що додавання і множення в $\mathbb{Z}_n$ пов'язані дистрибутивними законами. Це справді так (множення комутативне, тому досить перевірити лише один із цих законів):

$$\overline{x}\cdot(\overline{y}+\overline{z})=\overline{x}\cdot\overline{y+z}=\overline{x\cdot(y+z)}=\overline{x\cdot y+x\cdot z}=$$
$$=\overline{x\cdot y}+\overline{x\cdot z}=\overline{x}\cdot\overline{y}+\overline{x}\cdot\overline{z}.$$

□

Кільце $\mathbb{Z}_n$ називається *кільцем класів лишків* за модулем числа n.

Порівнюючи таблиці множення для $\mathbb{Z}_5$ і $\mathbb{Z}_6$, легко помітити принципову відмінність між ними: у $\mathbb{Z}_5$ кожен ненульовий клас є оборотним (і тому $\mathbb{Z}_5$ є навіть полем, а не просто комутативним кільцем з одиницею), а в $\mathbb{Z}_6$ ненульові класи $\overline{2}$, $\overline{3}$ і $\overline{4}$ обернених не мають. Тому з'ясуємо, коли для елемента $\overline{k}$ кільця $\mathbb{Z}_n$ існує обернений. Нам знадобиться така лема.

Лема 10. *Найбільший спільний дільник цілих чисел a і b збігається з найменшим додатним числом із множини $I = \{xa + yb \mid x, y \in Z\}$.*

Доведення. Нехай $d = x_0a+y_0b$ — найменше додатне число з I. Очевидно, що кожен спільний дільник чисел a та b буде і дільником усіх чисел вигляду $xa + yb$, а тому буде й дільником числа d. Тому a і b не мають спільних дільників, більших за d. Покажемо тепер, що d є спільним дільником a і b. Для цього поділимо a на d з остачею: $a = qd + r$. Тоді

$$r = a - qd = a - q(x_0a + y_0b) = (1 - qx_0)a - qy_0b.$$

Отже, $r \in I$. Але $0 \leq r < d$, а d є найменшим додатним числом з I. Тому $r = 0$ і a ділиться на d. Аналогічно доводиться, що b ділиться на d. □

Наслідок 27. *Цілі числа a і b будуть взаємно простими тоді й лише тоді, коли існують такі цілі числа x і y, що $xa + yb = 1$.*

Теорема 42. *Для елемента $\overline{k} \in \mathbb{Z}_n$ обернений існує тоді й лише тоді, коли k та n взаємно прості.*

Доведення. Необхідність. Нехай клас $\overline{k}$ із $\mathbb{Z}_n$ є оборотним, а клас $\overline{k'}$ є оберненим до $\overline{k}$. Тоді $\overline{k} \cdot \overline{k'} = \overline{1}$, тобто $kk' \equiv 1 \pmod{n}$. Це означає, що $kk' - 1$ ділиться на n, тобто існує таке ціле число m, що $kk' - 1 = mn$. Але тоді кожен спільний дільник чисел k та n буде і дільником числа $1 = kk' - mn$. Отже, k та n — взаємно прості.

Достатність. Нехай k та n — взаємно прості. Тоді за наслідком 27 знайдуться такі цілі числа m та l, що $1 = k \cdot m + n \cdot l$. Переходячи до класів лишків за модулем числа n, отримуємо

$$\overline{1} = \overline{k \cdot m} + \overline{n \cdot l} = \overline{k} \cdot \overline{m} + \overline{n} \cdot \overline{l}.$$

Але $\overline{n} = \overline{0}$. Тому $\overline{1} = \overline{k} \cdot \overline{m}$ і клас $\overline{m}$ є оберненим до класу $\overline{k}$. □

Наслідок 28. *У кільці $\mathbb{Z}_n$ є рівно $\varphi(n)$ оборотних елементів.*

Доведення. Це випливає з того, що повна система лишків $\{0, 1, \ldots, n-1\}$ за модулем числа n містить рівно $\varphi(n)$ елементів, взаємно простих із числом n. □

Наслідок 29. *Кільце $\mathbb{Z}_n$ буде полем тоді й лише тоді, коли n — просте число.*

Доведення. Необхідність. Нехай n — складене число. Тоді n розкладається в добуток $n = k \cdot m$, де $1 < k < n$. Числа k і n не є взаємно простими, бо мають спільний дільник $k > 1$. Але тоді з теореми 42 випливає, що для ненульового елемента $\overline{k}$ кільця $\mathbb{Z}_n$ не існує оберненого. Отже, $\mathbb{Z}_n$ не є полем.

Достатність. Нехай тепер n — просте число. Тоді всі ненульові елементи повної системи лишків $\{0, 1, \ldots, n-1\}$ за модулем n будуть взаємно простими з n. Отже, за теоремою 42, усі ненульові елементи кільця $\mathbb{Z}_n$ мають обернені. Тому $\mathbb{Z}_n$ є полем. □

Кажуть, що в комутативному кільці K *можна скорочувати на елемент* a, якщо для довільних $x, y \in K$ із рівності $ax = ay$ випливає рівність $x = y$.

Твердження 46. *У кільці $\mathbb{Z}_n$ можна скорочувати на елемент $\overline{a}$ тоді й лише тоді, коли $\overline{a}$ є оборотним.*

Доведення. Нехай $\overline{a}$ є оборотним елементом, $\overline{b}$ є елементом, оберненим до $\overline{a}$, і $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$. Маємо такий ланцюжок імплікацій:

$$\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} \implies \overline{b} \cdot (\overline{a} \cdot \overline{x}) = \overline{b} \cdot (\overline{a} \cdot \overline{y}) \implies$$
$$\implies (\overline{b} \cdot \overline{a}) \cdot \overline{x} = (\overline{b} \cdot \overline{a}) \cdot \overline{y} \implies \overline{1} \cdot \overline{x} = \overline{1} \cdot \overline{y} \implies \overline{x} = \overline{y}.$$

Отже, на $\overline{a}$ можна скорочувати.

Нехай тепер елемент $\overline{a}$ не є оборотним. Можна вважати, що $0 < a < n$. Із теореми 42 випливає, що числа a і n — не взаємно прості, а тому вони мають спільний дільник k, де $1 < k < n$. Нехай $a = a_0 k$, $n = n_0 k$. Тоді $1 < n_0 < 2n_0 \leq n$. Зокрема, $\overline{n_0} \neq \overline{2n_0}$. Але

$$\overline{a} \cdot \overline{n_0} = (\overline{a_0} \cdot \overline{k}) \cdot \overline{n_0} = \overline{a_0} \cdot (\overline{k} \cdot \overline{n_0}) = \overline{a_0} \cdot \overline{n} = \overline{a_0} \cdot \overline{0} = \overline{0},$$

$$\overline{a} \cdot \overline{2n_0} = \overline{a} \cdot (\overline{2} \cdot \overline{n_0}) = \overline{2} \cdot (\overline{a} \cdot \overline{n_0}) = \overline{0}.$$

Отже, $\overline{a} \cdot \overline{n_0} = \overline{a} \cdot \overline{2n_0}$, але $\overline{n_0} \neq \overline{2n_0}$. Тому на $\overline{a}$ скорочувати не можна. □

Теорема 43 (Ойлер). *Якщо $\overline{a}$ – оборотний елемент кільця $\mathbb{Z}_n$, то*

$$\overline{a}^{\,\varphi(n)} = \overline{1}.$$

Доведення. Нехай

$$\overline{b_1},\ \overline{b_2},\ \ldots,\ \overline{b_{\varphi(n)}} \tag{7.3}$$

– усі оборотні елементи кільця $\mathbb{Z}_n$. Із теореми 42 випливає, що добуток оборотних елементів знову є оборотним. Тому всі елементи

$$\overline{ab_1},\ \overline{ab_2},\ \ldots,\ \overline{ab_{\varphi(n)}} \tag{7.4}$$

також є оборотними. Елементи (7.4) попарно різні, оскільки з рівності $\overline{ab_t} = \overline{ab_s}$ і твердження 46 випливає, що $\overline{b_t} = \overline{b_s}$, звідки $t = s$. Тому елементи (7.4) це ті ж самі елементи (7.3), тільки, можливо, в іншому порядку. Але тоді

$$\overline{b_1} \cdot \overline{b_2} \cdots \overline{b_{\varphi(n)}} = \overline{ab_1} \cdot \overline{ab_2} \cdots \overline{ab_{\varphi(n)}} = \overline{a}^{\,\varphi(n)} \cdot \overline{b_1} \cdot \overline{b_2} \cdots \overline{b_{\varphi(n)}}\,.$$

Скорочуючи ліву і праву частини цієї рівності на оборотні елементи $\overline{b_1}$, $\overline{b_2}$, …, $\overline{b_{\varphi(n)}}$ одержуємо $\overline{1} = \overline{a}^{\,\varphi(n)}$. □

Теорему 43 можна переформулювати в термінах конгруенцій.

Теорема 43′. *Нехай n — фіксоване натуральне число, a — довільне ціле число, взаємно просте з n. Тоді $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Оскільки для простого числа p $\varphi(p) = p - 1$, то з теореми Ойлера одразу випливають наслідки.

Наслідок 30 (мала теорема Ферма). *Якщо p — просте число і $\overline{a}$ — ненульовий елемент поля $\mathbb{Z}_p$, то $\overline{a}^{\,p-1} = \overline{1}$.*

Малу теорему Ферма також можна переформулювати в термінах конгруенцій.

Наслідок 30′. *Якщо натуральне число a не ділиться на просте число p, то $a^{p-1} \equiv 1 \pmod{p}$.*

Або у трохи іншому вигляді запишемо малу теорему Ферма так.

Наслідок 30″. *Для довільних простого числа p і цілого невід'ємного числа a виконується конгруенція $a^p \equiv a \pmod{p}$.*

Вправа 19. *Доведіть рівносильність наслідків* 30, 30′ *і* 30′′.

Уперше мала теорема Ферма згадується в одному з листів Ферма 1640 року, однак без доведення. Перше відоме доведення належить Ляйбніцу, але він його не опублікував. Перше опубліковане доведення належить Ойлеру (у 1736 році). Ми наведемо ще два елементарні доведення малої теореми Ферма, які не використовують теореми Ойлера.

Доведення малої теореми Ферма за допомогою індукції. Будемо доводити її у формі наслідку 30′′, тобто покажемо, що для довільного цілого невід'много числа a число $a^p - a$ ділиться на p.

База індукції очевидна: якщо $a = 0$, то число $0^p - 0 = 0$ ділиться на p.

Припустимо тепер, що твердження правильне для всіх $a \le k$, і доведемо його для $a = k + 1$. Використовуючи біном Ньютона, можемо записати

$$(k+1)^p - (k+1) = k^p + 1 + \sum_{l=1}^{p-1} \binom{p}{l} k^l - k - 1 = (k^p - k) + \sum_{l=1}^{p-1} \binom{p}{l} k^l. \quad (7.5)$$

Доданок $k^p - k$ ділиться на p за припущенням індукції. Інші ж доданки містять множник – біноміальний коефіцієнт

$$\binom{p}{l} = \frac{p!}{l!(p-l)!},$$

чисельник $p!$ якого ділиться на p, а знаменник $l!(p-l)!$ при $1 \le l \le p-1$ є взаємно простим із p. Тому цей біноміальний коефіцієнт ділиться на p.

Отже, усі доданки у правій частині рівності (7.5) діляться на p, а тому різниця $(k+1)^p - (k+1)$ ділиться на p. □

Узагальненням біному Ньютона є так звана *поліноміальна теорема*:

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{\alpha+\beta+\cdots+\gamma=n \\ \alpha,\beta,\ldots,\gamma \ge 0}} \binom{n}{\alpha, \beta, \ldots, \gamma} x_1^\alpha x_2^\beta \cdots x_k^\gamma, \quad (7.6)$$

де *поліноміальний коефіцієнт* $\binom{n}{\alpha, \beta, \ldots, \gamma}$ має вигляд

$$\binom{n}{\alpha, \beta, \ldots, \gamma} = \frac{n!}{\alpha!\beta! \cdots \gamma!}.$$

Вправа 20. *Доведіть поліноміальну теорему.*

Доведення малої теореми Ферма за допомогою поліноміальної теореми. Якщо в поліноміальній теоремі покласти $n = p$ і $x_1 = x_2 = \cdots = x_k = 1$, то отримаємо

$$k^p = (1 + 1 + \cdots + 1)^p = \frac{p!}{p!0!\cdots 0!} + \frac{p!}{0!p!\cdots 0!} + \cdots + \frac{p!}{0!0!\cdots p!} +$$

$$+ \sum_{\substack{\alpha+\beta+\cdots+\gamma=p \\ p>\alpha,\beta,\ldots,\gamma\geq 0}} \frac{p!}{\alpha!\beta!\cdots\gamma!} = k + \sum_{\substack{\alpha+\beta+\cdots+\gamma=p \\ p>\alpha,\beta,\ldots,\gamma\geq 0}} \frac{p!}{\alpha!\beta!\cdots\gamma!}.$$

У правій частині цієї рівності кожен дріб

$$\frac{p!}{\alpha!\beta!\cdots\gamma!}$$

ділиться на p, бо чисельник $p!$ ділиться на p, а знаменник $\alpha!\beta!\cdots\gamma!$ при $p > \alpha, \beta, \ldots, \gamma \geq 0$ на p не ділиться. Тому різниця $k^p - k$ ділиться на p. □

Із теореми Ойлера випливає ще один важливий наслідок.

Наслідок 31. *Нехай $\overline{a}$ – оборотний елемент кільця $\mathbb{Z}_n$. Тоді елемент $\overline{a}^{\,\varphi(n)-1}$ буде оберненим до $\overline{a}$.*

Доведення. Справді, із теореми Ойлера випливає, що

$$\overline{a} \cdot \overline{a}^{\,\varphi(n)-1} = \overline{a}^{\,\varphi(n)} = \overline{1}.$$ □

Знаходження оберненого елемента за допомогою теореми Ойлера вимагає громіздких обчислень. Тому розглянемо ще один метод обчислення оберненого елемента (а заодно познайомимося з деякими поняттями, значення яких виходить далеко за межі задачі про обчислення оберненого елемента).

Лема 11. *Нехай $a = bq + r$. Тоді множина спільних дільників чисел a і b збігається із множиною спільних дільників чисел b і r.*

Доведення. Очевидно, що, коли число d ділить b і r, то воно ділить і число $a = bq + r$. Тому спільний дільник b і r буде спільним дільником a і b. Аналогічно, коли число d ділить a і b, то воно ділить і число $r = a - bq$. □

Нехай тепер a і b — натуральні числа. Поділимо a на b з остачею:

$$a = q_1 b + r_1. \tag{7.7}$$

Поділимо з остачею b на r_1:

$$b = q_2 r_1 + r_2. \tag{7.8}$$

Далі поділимо з остачею r_1 на r_2:

$$r_1 = q_3 r_2 + r_3. \tag{7.9}$$

І так далі. За теоремою про ділення з остачею

$$b > r_1 > r_2 > r_3 > \cdots . \tag{7.10}$$

Тому рано чи пізно ланцюжок має обірватися, тобто має відбутися ділення націло:

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}, \tag{7.11}$$

$$r_{k-2} = q_k r_{k-1} + r_k, \tag{7.12}$$

$$r_{k-1} = q_{k+1} r_k. \tag{7.13}$$

Теорема 44. *Остання ненульова остача r_k у побудованому вище ланцюжку остач*

$$a,\ b,\ r_1,\ \ldots,\ r_{k-3},\ r_{k-2},\ r_{k-1},\ r_k \tag{7.14}$$

є найбільшим спільним дільником чисел a і b.

Доведення. Із леми 11 випливає, що в кожної з пар чисел:

$$a \text{ і } b,\quad b \text{ і } r_1,\quad r_1 \text{ і } r_2,\quad \ldots,\quad r_{k-2} \text{ і } r_{k-1},\quad r_{k-1} \text{ і } r_k \tag{7.15}$$

множина спільних дільників одна й та сама. Але r_{k-1} ділиться на r_k, тому множина спільних дільників r_{k-1} і r_k збігається із множиною дільників числа r_k. Найбільшим серед цих дільників є саме число r_k. Тому r_k є найбільшим спільним дільником кожної з пар чисел (7.15), зокрема, пари a і b. □

Описаний процес знаходження найбільшого спільного дільника двох натуральних чисел називається *алгоритмом Евкліда*.

Цей алгоритм (точніше, рівності (7.7)–(7.12), які з'являються в процесі його роботи) можна використати і для знаходження оберненого

елемента в кільці $\mathbb{Z}_n$. Справді, нехай a і n — взаємно прості. Тоді найбільший спільний дільник a і n дорівнює 1. Із доведення теореми 42 випливає, що для знаходження елемента, оберненого до $\overline{a}$, досить знайти зображення $1 = a \cdot m + n \cdot l$ (тоді оберненим до $\overline{a}$ буде клас $\overline{m}$). Алгоритм Евкліда дозволяє знайти таке зображення.

Справді, нехай у процесі застосування алгоритму Евкліда ми отримали рівності

$$\begin{gathered} n = q_1 a + r_1, \\ a = q_2 r_1 + r_2, \\ r_1 = q_3 r_2 + r_3, \\ \dots, \\ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}, \\ r_{k-2} = q_k r_{k-1} + 1. \end{gathered}$$

Позначимо для зручності $r_0 = a$, $r_{-1} = n$. Щоб знайти зображення $1 = a \cdot m + n \cdot l$, будемо рухатися цими рівностями справа наліво. Перепишемо останню рівність у вигляді

$$1 = u_{k-2} r_{k-2} + v_{k-1} r_{k-1},$$

де $u_{k-2} = 1$, $v_{k-1} = -q_k$. Підставляючи сюди значення r_{k-1} із попередньої рівності, отримуємо

$$1 = u_{k-2} r_{k-2} + v_{k-1}(r_{k-3} - q_{k-1} r_{k-2}) = u_{k-3} r_{k-3} + v_{k-2} r_{k-2},$$

де $u_{k-3} = v_{k-1}$, $v_{k-2} = u_{k-2} - q_{k-1} v_{k-1}$. І так далі. Якщо ми вже знайшли зображення $1 = u_m r_m + v_{m+1} r_{m+1}$ через остачі r_m і r_{m+1}, то, використовуючи рівність $r_{m-1} = q_{m+1} r_m + r_{m+1}$, знаходимо зображення числа 1 через остачі r_{m-1} і r_m:

$$1 = u_m r_m + v_{m+1}(r_{m-1} - q_{m+1} r_m) = u_{m-1} r_{m-1} + v_m r_m,$$

де $u_{m-1} = v_{m+1}$, $v_m = u_m - q_{m+1} v_{m+1}$. На останньому кроці отримуємо потрібне зображення числа 1:

$$1 = u_{-1} r_{-1} + v_0 r_0 = u_{-1} n + v_0 a.$$

Приклад 17. У кільці $\mathbb{Z}_{25}$ знайдемо елемент, обернений до класу $\overline{11}$.

Спочатку зауважимо, що числа 11 та 25 – взаємно прості. Тому для класу $\overline{11}$ у кільці $\mathbb{Z}_{25}$ обернений існує. Алгоритм Евкліда дає такий ланцюжок рівностей:

$$25 = 2 \cdot 11 + 3, \quad 11 = 3 \cdot 3 + 2, \quad 3 = 1 \cdot 2 + 1.$$

Звідси отримуємо (жирним шрифтом виділено числа, які належать ланцюжку остач (7.14)):

$$1 = \mathbf{3} - 1 \cdot \mathbf{2} = \mathbf{3} - 1 \cdot (\mathbf{11} - 3 \cdot \mathbf{3}) = -1 \cdot \mathbf{11} + 4 \cdot \mathbf{3} = \\ = -1 \cdot \mathbf{11} + 4 \cdot (\mathbf{25} - 2 \cdot \mathbf{11}) = 4 \cdot \mathbf{25} - 9 \cdot \mathbf{11}.$$

Тому оберненим до класу $\overline{11}$ буде клас $\overline{-9} = \overline{-9 + 25} = \overline{16}$.

7.4. Задачі

7.1. Доведіть, що, коли ціле число b ділиться на найбільший спільний дільник d чисел a і n, то конгруенція $ax \equiv b \pmod{n}$ має за модулем n рівно d різних розв'язків.

7.2. Доведіть, що, коли конгруенція $x^2 \equiv a \pmod{65}$ є сумісною, то конгруенція $x^2 \equiv -a \pmod{65}$ також є сумісною.

7.3. Доведіть, що, коли для деякого простого числа p система цілочислових векторів лінійно незалежна над полем $\mathbb{Z}_p$, то вона лінійно незалежна і над полем $\mathbb{Q}$ раціональних чисел.

7.4. Нехай система цілочислових векторів лінійно незалежна над полем $\mathbb{Q}$ раціональних чисел. Доведіть, що ця система може бути лінійно залежною над полем $\mathbb{Z}_p$ лише для скінченної кількості простих чисел p.

7.5. а)** Доведіть, що СЛР

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & b_1\,, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}$$

із цілими коефіцієнтами має цілочисловий розв'язок тоді й лише тоді, коли для довільного k має розв'язок система

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & \equiv & b_1 \pmod{k}\,, \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & \equiv & b_m \pmod{k}\,. \end{array}$$

б) Чи можна в попередньому твердженні замість довільних цілих k обмежитися лише простими k?

7.6. Визначник $\begin{vmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{vmatrix}$ з елементами з кільця $\mathbb{Z}_n$ дорівнює 0. Чи зобов'язані його рядки бути пропорційними?

7.7.* Нехай визначник квадратної матриці A із цілими коефіцієнтами є взаємно простим із натуральним числом m. Доведіть, що в кільці $\mathbb{Z}_m$ система лінійних рівнянь $A\boldsymbol{x} = \boldsymbol{b}$ буде визначеною для кожного стовпця $\boldsymbol{b}$ вільних членів.

7.8. а) Підрахуйте кількість тих підмножин двовимірного векторного простору над полем $\mathbb{Z}_2$, які є його системами твірних.

б) Аналогічна задача для тривимірного простору.

7.9.* Доведіть, що не існує поля з 6 елементів.

8. Многочлени від однієї змінної

У математичному аналізі многочленами називаються функції вигляду

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \tag{8.1}$$

коефіцієнти a_0, a_1, a_2, …, a_n яких є довільними дійсними числами. Неважко переконатися (ми це зробимо в підрозділі 8.5), що два дійсні многочлени $f(x) = a_0 + a_1x + \cdots + a_nx^n$ і $g(x) = b_0 + b_1x + \cdots + b_nx^n$, збігаються як функції (тобто $f(x) = g(x)$ для всіх $x \in \mathbb{R}$) тоді й лише тоді, коли мають однакові коефіцієнти (тобто $a_0 = b_0$, $a_1 = b_1$, …, $a_n = b_n$).

Зрозуміло, що можна не обмежуватися лише дійсними многочленами, а розглядати вирази вигляду (8.1) із коефіцієнтами a_0, a_1, a_2, …, a_n із довільного поля P. Однак тоді трактування многочленів як функцій призводить до певної проблеми. Наприклад, многочлени x і x^p з коефіцієнтами з поля $\mathbb{Z}_p$ природно вважати різними (крім усього, у них різні степені). Однак із теореми Ферма випливає, що вони визначають одну й ту ж функцію $\mathbb{Z}_p \to \mathbb{Z}_p$. Більше того, для довільної множини коефіцієнтів K множина многочленів $K[x]$ із коефіцієнтами з K є нескінченною (нескінченною є вже множина їх степенів), однак у випадку скінченної множини K маємо лише скінченну кількість $|K|^{|K|}$ різних функцій $K \to K$.

Тому в алгебрі зручніше дотримуватися трохи іншого підходу і фактично ототожнювати многочлен (8.1) із послідовністю a_0, a_1, a_2, …, a_n його коефіцієнтів.

8.1. Арифметика кільця $K[x]$

Нехай K — довільне комутативне кільце з одиницею, x — новий символ, який будемо називати *невідомою* або *змінною*. *Многочленами (поліномами) від змінної x із коефіцієнтами з кільця K* називаються формальні суми вигляду

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\,, \tag{8.2}$$

де $a_0, a_1, \ldots, a_n \in K$. Елементи a_0, a_1, …, a_n називаються *коефіцієнтами* многочлена (8.2). Многочлен називається *нульовим*, якщо всі його коефіцієнти дорівнюють 0. Кожному ненульовому многочлену $f(x)$ приписується невід'ємне ціле число – максимальний індекс ненульового коефіцієнта – яке називається *степенем* многочлена $f(x)$ і позначається

$45f(x)$. Степінь нульового многочлена невизначений, однак інколи зручно вважати, що він дорівнює $-\infty$. Коефіцієнт a_0 називається *вільним членом* многочлена $f(x)$, коефіцієнт $a_{45f(x)}$ – *старшим коефіцієнтом*.

Вираз вигляду ax^k називається *одночленом*. На многочлен (8.2) можна дивитися як на суму одночленів. Якщо степінь многочлена (8.2) дорівнює n, то одночлен a_nx^n називається *старшим членом* многочлена $f(x)$.

Многочлени

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \text{ і } g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

вважаються рівними тоді й лише тоді, коли $45f(x) = 45g(x)$ і $a_0 = b_0$, $a_1 = b_1, \ldots, a_{45f(x)} = b_{45g(x)}$. Із цього означення випливає, що до кожного многочлена можна приєднувати (або, навпаки, опускати) довільну кількість одночленів вигляду $0 \cdot x^k$. Зокрема, $1 + x = 1 + x + 0 \cdot x^2 = 1 + x + 0 \cdot x^2 + 0 \cdot x^3$ і т. д.

Множину всіх многочленів із коефіцієнтами з кільця K позначають $K[x]$. Многочлени вигляду a_0 (тобто нульового степеня або нульовий) часто називають *константами* або *скалярами*. Якщо такий многочлен ототожнити з елементом $a_0 \in K$, то отримуємо занурення $K \hookrightarrow K[x]$.

Над многочленами можна визначити кілька природних дій:

додавання многочленів: дописавши, у разі потреби, члени з нульовими коефіцієнтами, можемо вважати, що $f(x) = \sum\limits_{i=0}^{n} a_ix^i$, $g(x) = \sum\limits_{i=0}^{n} b_ix^i$, тоді

$$f(x) + g(x) := \sum_{i=0}^{n}(a_i + b_i)x^i\,; \tag{8.3}$$

множення многочлена на елемент $a \in K$:

$$a \cdot \sum_{i=0}^{n} a_ix^i := \sum_{i=0}^{n}(aa_i)x^i\,; \tag{8.4}$$

множення многочленів: якщо $f(x) = \sum\limits_{i=0}^{n} a_ix^i$, $g(x) = \sum\limits_{j=0}^{m} b_jx^j$, то

$$f(x) \cdot g(x) := \sum_{k=0}^{n+m}\Big(\sum_{i+j=k} a_ib_j\Big)x^k\,. \tag{8.5}$$

Оскільки вільний член суми (добутку) двох многочленів є сумою (добутком) вільних членів доданків (множників), то занурення $K \hookrightarrow K[x]$ узгоджене з діями в K і $K[x]$.

Твердження 47.
а) $\deg(f+g) \le \max(\deg f, \deg g)$;
б) $\deg(f \cdot g) \le \deg f + \deg g$.

Доведення. Нехай $45f(x) = n$, $45g(x) = m$ і $n \ge m$. Тоді із правила (8.3) випливає, що $45(f+g) \le n$, а з правила (8.5) – що $45(f \cdot g) \le m+n$. □

Зауваження. **1.** Нерівності у твердженні 47 можуть бути строгими. Справді, над довільним кільцем K маємо

$$45(x^2+x) = 45(-x^2+1)) = 2,$$

але

$$45\big((x^2+x)+(-x^2+1)\big) = 45(x+1)) = 1.$$

Над кільцем $\mathbb{Z}_4$ маємо

$$45(2x^2+1) = 2, \quad \text{але} \quad 45(2x^2+1)^2 = 451 = 0.$$

2. Однак, якщо в кільці K добуток ненульових елементів не дорівнює нулю (так буде, наприклад, коли K є кільцем $\mathbb{Z}$ або полем), то із правила (8.5) випливає, що $45(f \cdot g) = 45f + 45g$. Зокрема, у цьому випадку добуток ненульових многочленів знову буде ненульовим многочленом.

Твердження 48. *Відносно дій додавання і множення множина многочленів $K[x]$ утворює комутативне кільце з одиницею.*

Доведення. Більшість законів (I), (II), (III), (IV), (IV′) і (V), які повинно задовольняти комутативне кільце з одиницею (див. підрозділ 1.2), зокрема, властивості додавання і комутативність множення, для множини $K[x]$ є очевидними. Неочевидними є тільки асоціативність множення і дистрибутивний закон. Асоціативність множення перевіримо зараз, а перевірку дистрибутивного закону полишаємо читачеві.

Нехай $f(x) = \sum\limits_{i=0}^{n} a_i x^i$, $g(x) = \sum\limits_{j=0}^{m} b_j x^j$, $h(x) = \sum\limits_{k=0}^{l} c_k x^k$. Тоді

$$f(x)g(x)\cdot h(x) = \sum_{p=0}^{n+m}\Big(\sum_{i+j=p} a_i b_j x^p\Big)\cdot \sum_{k=0}^{l} c_k x^k =$$

$$= \sum_{q=0}^{n+m+l} \Big(\sum_{p+k=q} \Big(\sum_{i+j=p} a_i b_j \Big) c_k \Big) x^q = \sum_{q=0}^{n+m+l} \Big(\sum_{i+j+k=q} a_i b_j c_k \Big) x^q =$$

$$= \sum_{q=0}^{n+m+l} \Big(\sum_{i+t=q} \Big(a_i \sum_{j+k=t} b_j c_k \Big) \Big) x^q = \sum_{i=0}^{n} a_i x^i \cdot \sum_{t=0}^{m+l} \Big(\sum_{j+k=t} b_j c_k x^t \Big) =$$

$$= f(x) \cdot g(x) h(x) . \qquad \square$$

Далі нас буде цікавити головним чином випадок, коли кільце коефіцієнтів K є полем (і щоб підкреслити це, замість K будемо писати P). Причин кілька: цей випадок і найпростіший, і найважливіший. До того ж є велика аналогія між властивостями кілець $\mathbb{Z}$ і $P[x]$. Причина цієї аналогії стане зрозумілішою пізніше, а зараз ми аналогію будемо лише фіксувати.

Твердження 49. *У кільці $P[x]$ многочленів із коефіцієнтами з поля P можна скорочувати.*

Доведення. Нехай $f(x) \neq 0$ і $f(x)g_1(x) = f(x)g_2(x)$. Тоді $f(x)(g_1(x) - g_2(x)) = 0$. Оскільки в кільці $P[x]$ добуток ненульових многочленів є ненульовим, то $g_1(x) - g_2(x) = 0$. Отже, $g_1(x) = g_2(x)$. $\square$

Теорема 45 (про ділення з остачею)**.** *Для довільних многочленів $f(x)$ і $g(x) \neq 0$ із $P[x]$ існують такі многочлени $q(x)$ і $r(x)$, що*

$$f(x) = q(x)g(x) + r(x) \quad і \quad r(x) = 0 \ \text{ або } \ \deg r(x) < \deg g(x).$$

Многочлени $q(x)$ і $r(x)$ визначені однозначно.

Доведення. Існування. Нехай $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ і $b_m \neq 0$. Існування $q(x)$ і $r(x)$ будемо доводити індукцією за степенем многочлена $f(x)$.

Якщо $n < m$, то можна взяти $q(x) = 0$, $r = f(x)$.

Якщо $n \geq m$, то многочлен

$$f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = \Big(a_{n-1} - \frac{a_n}{b_m} b_{m-1} \Big) x^{n-1} + \cdots$$

має степінь менший, ніж $f(x)$, а тому за припущенням індукції існують такі многочлени $q_1(x)$ і $r_1(x)$, що $f_1(x) = q_1(x)g(x) + r_1(x)$ і $r_1(x) = 0$ або $45 r_1(x) < 45 g(x)$. Але тоді

$$f(x) = \frac{a_n}{b_m} x^{n-m} g(x) + f_1(x) = \frac{a_n}{b_m} x^{n-m} g(x) + q_1(x)g(x) + r_1(x) =$$

$$= \left(\frac{a_n}{b_m}x^{n-m} + q_1(x)\right)g(x) + r_1(x)$$

і многочлени $q(x) = \frac{a_n}{b_m}x^{n-m} + q_1(x)$, $r(x) = r_1(x)$ задовольняють умову теореми.

Однозначність. Нехай

$$f(x) = q(x)g(x) + r(x) = q_1(x)g(x) + r_1(x),$$

причому многочлени $r(x)$ і $r_1(x)$ задовольняють умову теореми. Тоді

$$(q(x) - q_1(x))g(x) = r_1(x) - r(x)\,. \tag{8.6}$$

Нагадаємо, що для многочленів із коефіцієнтами з поля степінь добутку дорівнює сумі степенів множників. Якщо $q(x) \neq q_1(x)$, то $q(x) - q_1(x) \neq 0$, і в рівності (8.6) степінь многочлена зліва $\geq 45g(x)$, у той час як степінь многочлена справа строго менший $45g(x)$. Оскільки це неможливо, то $q(x) = q_1(x)$. Але тоді $r_1(x) - r(x) = 0$ і $r_1(x) = r(x)$. □

Многочлени $q(x)$ і $r(x)$ із теореми 45 називаються відповідно *часткою* й *остачею* від ділення многочлена $f(x)$ на многочлен $g(x)$. Доведення теореми є конструктивним і дає метод обчислення частки й остачі (насправді це відомий ще зі школи метод ділення “ріжком”).

Зауваження. Для многочленів із коефіцієнтами з кільця теорема 45 перестає бути правильною: многочленів $q(x)$ і $r(x)$ може взагалі не існувати. Наприклад, у випадку кільця $\mathbb{Z}$ многочлен x^2 не ділиться з остачею на $2x + 1$. А в разі їх існування може бути багато різних пар $(q(x), r(x))$. Наприклад, над кільцем $\mathbb{Z}_4$

$$2x + 1 = 1 \cdot (2x + 1) + 0 = 3 \cdot (2x + 1) + 2.$$

Зазвичай ділення одного многочлена на інший виконують за допомогою відомого ще зі школи алгоритму ділення “ріжком” (фактично цей алгоритм використовується і в доведенні теореми 45). Однак ділення на двочлен $x - c$ (а ми пізніше пересвідчимось, що цей випадок є дуже важливим) можна організувати ліпшим чином. У цьому випадку остача від ділення має бути многочленом степеня < 1, тобто елементом поля P. Нехай

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x-c)(b_{n-1}x^{n-1} + \cdots + b_1x + b_0) + r. \tag{8.7}$$

Прирівняємо коефіцієнти при відповідних степенях x у лівій і правій частинах рівності (8.7):

$$\begin{aligned}
x^n: &\quad a_n &&= b_{n-1},\\
x^{n-1}: &\quad a_{n-1} &&= b_{n-2} - cb_{n-1},\\
x^{n-2}: &\quad a_{n-2} &&= b_{n-3} - cb_{n-2},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
x^1: &\quad a_1 &&= b_0 - cb_1,\\
x^0: &\quad a_0 &&= r - cb_0.
\end{aligned}$$

Із цих рівностей одержуємо прості рекурентні формули для знаходження коефіцієнтів частки $b_{n-1}x^{n-1} + \dots + b_1x + b_0$ й остачі r:

$$\begin{aligned}
b_{n-1} &= a_n,\\
b_{n-2} &= a_{n-1} + cb_{n-1},\\
b_{n-3} &= a_{n-2} + cb_{n-2},\\
&\dots\dots\dots\dots\dots\\
b_0 &= a_1 + cb_1,\\
r &= a_0 + cb_0.
\end{aligned} \tag{8.8}$$

Початкові дані й результати обчислень зручно записувати у вигляді таблиці, яка називається *схемою Горнера*:

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_1	a_0
c	b_{n-1}	b_{n-2}	b_{n-3}	$\dots$	b_0	r

. (8.9)

Із рівностей 8.8 випливає, що перший елемент b_{n-1} другого рядка просто зноситься з першого рядка, а кожен наступний елемент другого рядка обчислюється як сума числа, що стоїть над ним, і помноженого на c числа зліва від нього.

Приклад 18. Поділимо з остачею $2x^5 + 3x^4 - x^2 - 9x + 7$ на $x + 2$.

За схемою Горнера маємо

	2	3	0	−1	−9	7
−2	2	−1	2	−5	1	5

.

Отже,

$$2x^5 + 3x^4 - x^2 - 9x + 7 = (x + 2)(2x^4 - x^3 + 2x^2 - 5x + 1) + 5.$$

Говорять, що многочлен $f(x)$ *ділиться* на многочлен $g(x)$ або що $g(x)$ *ділить* $f(x)$ (і коротко позначають як $g(x) \mid f(x)$), якщо існує такий многочлен $h(x)$, що $f(x) = g(x)h(x)$. Якщо $g(x) \mid f(x)$), то $g(x)$ називається *дільником* $f(x)$, а $f(x)$ – *кратним* $g(x)$.

Твердження 50 (найпростіші властивості подільності многочленів)**.**

а) Відношення подільності є рефлексивним і транзитивним.

б) Якщо кожен із многочленів $f_1(x)$, …, $f_k(x)$ ділиться на $g(x)$, то для довільних многочленів $h_1(x)$, …, $h_k(x)$ сума $h_1f_1(x) + \cdots + h_kf_k(x)$ також ділиться на $g(x)$.

Доведення. а) рефлексивність випливає з рівності $f(x) = 1 \cdot f(x)$. Нехай тепер $g(x) \mid f(x)$ і $h(x) \mid g(x)$. Тоді існують такі многочлени $u(x)$ і $v(x)$, що $f(x) = g(x)u(x)$ і $g(x) = h(x)v(x)$. Але тоді $f(x) = h(x) \cdot v(x)u(x)$. Отже, $h(x) \mid f(x)$, що доводить транзитивність відношення подільності

б) Нехай $f_1(x) = g(x)u_1(x)$, …, $f_k(x) = g(x)u_k(x)$. Тоді

$$h_1f_1(x) + \cdots + h_kf_k(x) = h_1g(x)u_1(x) + \cdots + h_kg(x)u_k(x) =$$
$$= g(x)\big(h_1u_1(x) + \cdots + h_ku_k(x).\big)$$

Отже, сума $h_1f_1(x) + \cdots + h_kf_k(x)$ ділиться на $g(x)$. □

Многочлени $f(x)$ і $g(x)$ називають *асоційованими* (і записують $f(x) \sim g(x)$), якщо $g(x) \mid f(x)$ і $f(x) \mid g(x)$. Легко бачити, що відношення асоційованості є відношенням еквівалентності, причому нульовий многочлен утворює окремий клас еквівалентності.

Твердження 51. *У кільці $P[x]$ ненульові многочлени $f(x)$ і $g(x)$ будуть асоційованими тоді й лише тоді, коли вони розрізняються скалярними множниками.*

Доведення. Нехай $g(x) \mid f(x)$ і $f(x) \mid g(x)$. Тоді існують такі многочлени $u(x)$ і $v(x)$, що $f(x) = g(x)u(x)$ і $g(x) = f(x)v(x)$. Звідси випливає, що $f(x) = f(x)v(x)u(x)$. Позаяк степінь добутку дорівнює сумі степенів множників, то $45u(x) = 45v(x) = 0$. Але тоді $u(x)$ і $v(x)$ є скалярами.

Навпаки, нехай $f(x) = ag(x)$, де $a \in P$. Зрозуміло, що $a \neq 0$. У полі для кожного ненульового елемента є обернений, тому $g(x) = a^{-1}f(x)$. Отже, якщо $f(x)$ і $g(x)$ розрізняються скалярним множником, то $g(x) \mid f(x)$ і $f(x) \mid g(x)$. □

Наслідок 32. *Якщо многочлен $f(x)$ ділиться на $g(x)$, то*

а) кожен многочлен, асоційований з $f(x)$, ділиться на $g(x)$;

б) $f(x)$ ділиться на кожен многочлен, асоційований з $g(x)$.

Зауваження. Аналогічно вводиться поняття асоційованих чисел у кільці $\mathbb{Z}$: *a і b – асоційовані*, якщо $a \mid b$ і $b \mid a$. Легко зрозуміти, що асоційовані числа відрізняються щонайбільше знаком.

Многочлен $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ степеня n називається *нормованим*, якщо $a_n = 1$. Легко бачити, що в кожному класі асоційованих многочленів є рівно один нормований. Оскільки з наслідку 32 випливає, що асоційованість на подільність не впливає, то в багатьох питаннях подільності можна обмежитися лише нормованими многочленами.

Дільник $g(x)$ многочлена $f(x)$ називається *нетривіальним*, якщо $g(x)$ не є асоційованим ні з многочленом $f(x)$, ні з одиницею (тобто, якщо в розкладі $f(x) = g(x)h(x)$ обидва множники мають додатні степені).

Многочлен $f(x)$ ненульового степеня називається *незвідним*, якщо він не має нетривіальних дільників. У противному разі $f(x)$ називається *звідним*. Ці поняття є аналогами простих і складених чисел у кільці $\mathbb{Z}$.

Якщо поле P міститься в полі P_1, то многочлен $f(x)$ із $P[x]$ можна розглядати і як многочлен із $P_1[x]$. При переході до більшого поля незвідний многочлен може стати звідним. Тому часто говорять про незвідність многочлена $f(x)$ над даним полем P. Наприклад, многочлен $x^2 - 2$ є незвідним над $\mathbb{Q}$, але він буде звідним над $\mathbb{R}$: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. Многочлен $x^2 + 1$ є незвідним над $\mathbb{Q}$ і $\mathbb{R}$, але буде звідним над $\mathbb{C}$: $x^2 + 1 = (x + i)(x - i)$.

Кожне ціле число розкладається в добуток простих. Аналогічне твердження виконується і для многочленів:

Твердження 52. *Кожен ненульовий многочлен із коефіцієнтами з поля P розкладається в кільці $P[x]$ у добуток незвідних многочленів.*

Доведення. Зауважимо: зручно вважати, що добуток нульової кількості множників дорівнює 1. Тому з точністю до асоційованості кожен многочлен нульового степеня розкладається в добуток нульової кількості незвідних многочленів.

Нехай тепер $f(x)$ – многочлен степеня $n > 0$. Якщо він – незвідний, то його розклад у добуток незвідних містить один множник. Якщо ж $f(x)$ звідний, то його можна розкласти в добуток $f(x) = g(x)h(x)$ многочленів менших степенів. Якщо обидва множники $g(x)$ і $h(x)$ — незвідні, то процес розкладу $f(x)$ у добуток незвідних завершено. У противному разі ті із множників, які є звідними, розкладаємо далі. І так далі. Оскільки при множенні степені множників додаються, то розклад $f(x)$ у добуток многочленів ненульового степеня не може містити більше ніж n множників. Тому не пізніше ніж на n-му кроці ми одержимо розклад $f(x) = p_1(x) \cdots p_k(x)$ многочлена $f(x)$ у добуток незвідних многочленів $p_1(x), \ldots, p_k(x)$. □

Многочлен $d(x)$ називається *найбільшим спільним дільником* (скорочено: НСД) многочленів $f(x)$ і $g(x)$, якщо він задовольняє такі дві умови:

1) $d(x)$ є спільним дільником многочленів $f(x)$ і $g(x)$, тобто $d(x) \mid f(x)$ і $d(x) \mid g(x)$;

2) $d(x)$ ділиться на кожен спільний дільник многочленів $f(x)$ і $g(x)$, тобто із $c(x) \mid f(x)$ і $c(x) \mid g(x)$ випливає, що $c(x) \mid d(x)$.

Найбільший спільний дільник многочленів $f(x)$ і $g(x)$ позначається НСД $(f(x), g(x))$ або просто $(f(x), g(x))$. З умови 2) випливає, що коли НСД $(f(x), g(x))$ існує, то з точністю до асоційованості він єдиний. Справді, якщо $d_1(x)$ і $d_2(x)$ – два такі дільники, то вони повинні ділитися один на одного.

Теорема 46. *Якщо P — поле, то в кільці $P[x]$ для довільних многочленів $f(x)$ і $g(x)$ існує* НСД $(f(x), g(x))$.

Доведення. Очевидно, що, коли один із многочленів $f(x)$ і $g(x)$ є нульовим, то НСД$(f(x), g(x))$ збігається із другим із цих многочленів. Тому далі вважаємо, що кожен із многочленів $f(x)$ і $g(x)$ є ненульовим. Візьмемо у множині

$$I = \{u(x)f(x) + v(x)g(x) \mid u(x), v(x) \in P[x]\}$$

ненульовий многочлен $d(x) = u_1(x)f(x) + v_1(x)g(x)$ найменшого можливого степеня і покажемо, що $d(x)$ є найбільшим спільним дільником $f(x)$ і $g(x)$.

Для перевірки першої умови з означення НСД розділимо $f(x)$ на $d(x)$ з остачею: $f(x) = q(x)d(x) + r(x)$. Тоді

$$\begin{aligned} r(x) = f(x) - q(x)d(x) = f(x) - q(x)\big(u_1(x)f(x) + v_1(x)g(x)\big) = \\ = \big(1 - q(x)u_1(x)\big)f(x) - \big(q(x)v_1(x)\big)g(x). \end{aligned}$$

Отже, $r(x) \in I$. Якби $r(x)$ був ненульовим, то він би мав менший степінь, ніж $d(x)$. Але це суперечить вибору многочлена $d(x)$. Тому $r(x) = 0$ і $f(x)$ ділиться на $d(x)$. Аналогічно доводиться, що $g(x)$ ділиться на $d(x)$.

Виконання другої умови з означення НСД є очевидним: якщо $c(x) \mid f(x)$ і $c(x) \mid g(x)$, то із твердження 50 випливає, що $c(x) \mid d(x)$. □

Із доведення теореми 46 випливає важливий наслідок.

Наслідок 33. *Для довільних многочленів $f(x)$ і $g(x)$ існують такі многочлени $u(x)$ і $v(x)$, що*

$$\text{НСД}\,(f(x), g(x)) = u(x)f(x) + v(x)g(x).$$

Зображення $\text{НСД}\,(f(x), g(x)) = u(x)f(x) + v(x)g(x)$ визначене неоднозначно, але завжди можна зробити так, щоб степені $u(x)$ і $v(x)$ були меншими за степені $g(x)$ і $f(x)$ відповідно. Справді, розділимо $u(x)$ на $g(x)$ з остачею $u(x) = q(x)g(x) + r(x)$. Тоді

$$\text{НСД}\,(f(x), g(x)) = r(x)f(x) + \big(v(x) + f(x)q(x)\big)g(x)\,,$$

оскільки тепер степінь кожного із многочленів $\text{НСД}\,(f(x), g(x))$ і $r(x)f(x)$ менший ніж $45f(x) + 45g(x)$, то й степінь множника $v(x) + f(x)q(x)$ менший ніж $45f(x)$.

Недоліком доведення теореми 46 є те, що воно є чистим доведенням існування і не дає способу знаходження $\text{НСД}\,(f(x), g(x))$. Ефективний спосіб знаходження $\text{НСД}\,(f(x), g(x))$ базується на наступній лемі.

Лема 12. *Якщо $f(x) = q(x)g(x) + r(x)$, то*

$$\text{НСД}\,(f(x), g(x)) = \text{НСД}\,(g(x), r(x)).$$

Доведення. Досить показати, що пари $(f(x), g(x))$ і $(g(x), r(x))$ мають ту саму множину спільних дільників. Але це просто:

якщо $d(x)$ ділить кожен із многочленів $f(x)$ і $g(x)$, то за твердженням 50 $d(x)$ ділить і многочлен $r(x) = f(x) - q(x)g(x)$;

якщо ж $d(x)$ ділить кожен із многочленів $g(x)$ і $r(x)$, то за твердженням 50 $d(x)$ ділить і многочлен $f(x) = q(x)g(x) + r(x)$. □

Як уже зазначалося в доведенні теореми 46, якщо один із многочленів $f(x)$ і $g(x)$ є нульовим, то $\text{НСД}\,(f(x), g(x))$ збігається із другим із цих многочленів. Тому далі вважаємо, що кожен із многочленів $f(x)$ і $g(x)$ є ненульовим, причому $45f(x) \geq 45g(x)$. Поділимо $f(x)$ на $g(x)$ з остачею:

$$f(x) = q_1(x)g(x) + r_1(x). \tag{8.10}$$

Далі поділимо з остачею $g(x)$ на $r_1(x)$:

$$g(x) = q_2(x)r_1(x) + r_2(x). \tag{8.11}$$

Потім поділимо з остачею $r_1(x)$ на $r_2(x)$:

$$r_1(x) = q_3(x)r_2(x) + r_3(x). \tag{8.12}$$

І так далі. За теоремою про ділення з остачею степені остач спадатимуть:

$$45f(x) \geq 45g(x) > 45r_1(x) > 45r_2(x) > 45r_3(x) > \dots \tag{8.13}$$

Проте степені многочленів є невід'ємними цілими числами. Тому рано чи пізно ланцюжок має обірватися, тобто має відбутися ділення націло:

$$r_{k-3}(x) = q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x), \tag{8.14}$$
$$r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x), \tag{8.15}$$
$$r_{k-1}(x) = q_{k+1}(x)r_k(x). \tag{8.16}$$

Теорема 47. *Остання ненульова остача $r_k(x)$ у побудованому вище ланцюжку остач*

$$f(x),\ g(x),\ r_1(x),\ \dots,\ r_{k-3}(x),\ r_{k-2}(x),\ r_{k-1}(x),\ r_k(x) \tag{8.17}$$

є найбільшим спільним дільником многочленів $f(x)$ і $g(x)$.

Доведення. Оскільки $r_{k-1}(x)$ ділиться на $r_k(x)$, то

$$\text{НСД}\,(r_{k-1}(x), r_k(x)) = r_k(x).$$

Далі з рівностей (8.15), . . . , (8.12), (8.11), (8.10) і леми 12 випливає

$$r_k(x) = \text{НСД}\,(r_{k-1}(x), r_k(x)) = \text{НСД}\,(r_{k-2}(x), r_{k-1}(x)) = \cdots$$
$$\cdots = \text{НСД}\,(r_1(x), r_2(x)) = \text{НСД}\,(g(x), r_1(x)) = \text{НСД}\,(f(x), g(x)). \qquad \square$$

Описаний вище процес знаходження найбільшого спільного дільника двох многочленів називається *алгоритмом Евкліда*. Як бачимо, він дослівно повторює алгоритм Евкліда відшукання найбільшого спільного дільника двох цілих чисел[16].

Алгоритм Евкліда (точніше, рівності (8.10)–(8.15), які з'являються у процесі роботи цього алгоритму) можна використати і для знаходження зображення найбільшого спільного дільника у вигляді

$$\text{НСД}\,(f(x), g(x)) = u(x)f(x) + v(x)g(x). \tag{8.18}$$

[16] Алгоритм Евкліда є найвідомішим з алгоритмів, що використовуються в сучасній математиці. Його дослідженню, модифікаціям і застосуванням присвячена величезна кількість літератури. Названий так тому, що вперше описаний у знаменитих "Початках" (або "Елементах") Евкліда. Там він фігурує навіть двічі: спочатку в чисто геометричній формі для знаходження *найбільшої спільної міри* двох відрізків, а потім для знаходження найбільшого спільного дільника двох натуральних чисел.

Позначимо для зручності $r_0(x) = g(x)$, $r_{-1}(x) = f(x)$. Щоб знайти зображення (8.18), будемо рухатися по рівностям (8.10)–(8.15) знизу вгору. Із рівності (8.15) маємо

$$\text{НСД}\,(f(x), g(x)) = r_k(x) = r_{k-2}(x) - q_k(x)r_{k-1}(x) = \\ = u_{k-2}(x)r_{k-2}(x) + v_{k-1}(x)r_{k-1}(x),$$

де $u_{k-2}(x) = 1$, $v_{k-1}(x) = -q_k(x)$. Підставляючи сюди значення $r_{k-1}(x)$ із рівності (8.14), отримуємо

$$\text{НСД}\,(f(x), g(x)) = u_{k-2}(x)r_{k-2}(x) + v_{k-1}(x)\big(r_{k-3}(x) - q_{k-1}(x)r_{k-2}(x)\big) = \\ = u_{k-3}(x)r_{k-3}(x) + v_{k-2}(x)r_{k-2}(x),$$

де $u_{k-3}(x) = v_{k-1}(x)$, $v_{k-2}(x) = u_{k-2}(x) - q_{k-1}(x)v_{k-1}(x)$. І так далі. Якщо ми вже знайшли зображення НСД

$$\text{НСД}\,(f(x), g(x)) = u_m(x)r_m(x) + v_{m+1}(x)r_{m+1}(x)$$

через остачі $r_m(x)$ і $r_{m+1}(x)$, то, використовуючи рівність

$$r_{m-1}(x) = q_{m+1}(x)r_m(x) + r_{m+1}(x),$$

знаходимо зображення НСД через остачі $r_{m-1}(x)$ і $r_m(x)$:

$$\text{НСД}(f(x), g(x)) = u_m(x)r_m(x) + v_{m+1}(x)\big(r_{m-1}(x) - q_{m+1}(x)r_m(x)\big) = \\ = u_{m-1}(x)r_{m-1}(x) + v_m(x)r_m(x),$$

де $u_{m-1}(x) = v_{m+1}(x)$, $v_m(x) = u_m(x) - q_{m+1}(x)v_{m+1}(x)$.

На останньому кроці, використовуючи рівність (8.10), одержимо потрібне зображення:

$$\text{НСД}(f(x), g(x)) = u_{-1}(x)r_{-1}(x) + v_0(x)r_0(x) = u_{-1}(x)f(x) + v_0(x)g(x).$$

Приклад 19. Знайдемо найбільший спільний дільник многочленів $f(x) = x^6 - 5x^4 - 2x^3 - x^2 - 4x + 26$ і $g(x) = x^5 - x^4 - 5x^3 + 7x^2 - 14x + 18$ та його зображення у вигляді (8.18).

Застосовуючи алгоритм Евкліда, дістаємо ланцюжок рівностей:

$$f(x) = (x+1)g(x) + (x^4 - 4x^3 + 6x^2 - 8x + 8) = (x+1)g(x) + r_1(x);$$

$$g(x) = (x+3)r_1(x) + (x^3 - 3x^2 + 2x - 6) = (x+3)r_1(x) + r_2(x);$$

$$r_1(x) = (x-1)r_2(x) + (x^2 + 2) = (x-1)r_2(x) + r_3(x);$$

$$r_2(x) = (x-3)r_3(x).$$

Таким чином,

$$\text{НСД}\,(f(x), g(x)) = r_3(x) = x^2 + 2.$$

Знайдемо тепер зображення НСД у вигляді (8.18). Для цього "розкручуємо" отримані рівності знизу вгору:

$$\begin{gathered} x^2 + 2 = r_1(x) - (x-1)r_2(x) = r_1(x) - (x-1)\big(g(x) - (x+3)r_1(x)\big) = \\ = -(x-1)(g(x) + (x^2 + 2x - 2)r_1(x) = \\ = -(x-1)(g(x) + (x^2 + 2x - 2)\big(f(x) - (x+1)g(x)\big) = \\ = (x^2 + 2x - 2)f(x) + (-x^3 - 3x^2 - x + 3)g(x). \end{gathered}$$

Многочлени $f(x)$ і $g(x)$ називаються *взаємно простими*, якщо 1 є їхнім найбільшим спільним дільником.

Твердження 53 (критерій взаємної простоти многочленів)**.** *Многочлени $f(x)$ і $g(x)$ будуть взаємно простими тоді й лише тоді, коли існують такі многочлени $u(x)$ і $v(x)$, що $u(x)f(x) + v(x)g(x) = 1$.*

Доведення. Якщо $f(x)$ і $g(x)$ взаємно прості, то їх найбільшим спільним дільником є 1. За наслідком 33 тоді існують такі многочлени $u(x)$ і $v(x)$, що $u(x)f(x) + v(x)g(x) = 1$.

Навпаки, нехай $u(x)f(x)+v(x)g(x) = 1$. Тоді за твердженням 50 кожен спільний дільник $d(x)$ многочленів $f(x)$ і $g(x)$ буде також і дільником суми $u(x)f(x) + v(x)g(x) = 1$. Отже, найбільший спільний дільник многочленів $f(x)$ і $g(x)$ дорівнює 1, а тому вони взаємно прості. □

Теорема 48 (властивості взаємно простих многочленів)**.**

а) **(лема Евкліда)** *Якщо $(f(x), g(x)) = 1$ і $f(x)|g(x)h(x)$, то $f(x)|h(x)$.*

б) Якщо $(f(x), g(x)) = 1$ і $f(x)|h(x)$, $g(x)|h(x)$, то $f(x)g(x)|h(x)$.

в) Якщо $(f(x), h(x)) = 1$ і $(g(x), h(x)) = 1$, то $(f(x)g(x), h(x)) = 1$.

Доведення. а) Нехай $(f(x), g(x)) = 1$. Тоді за твердженням 53 існують такі многочлени $u(x)$ і $v(x)$, що $u(x)f(x) + v(x)g(x) = 1$. Помножимо обидві частини останньої рівності на $h(x)$:

$$u(x)f(x)h(x) + v(x)g(x)h(x) = h(x). \tag{8.19}$$

Обидва доданки лівої частини діляться на $f(x)$. Тому й $h(x)$ ділиться на $f(x)$.

б) Знову можемо виписати рівність (8.19). Крім того, з умов $f(x)|h(x)$ та $g(x)|h(x)$ випливає існування таких многочленів $p(x)$ та $q(x)$, що $h(x) = f(x)p(x)$ і $h(x) = g(x)q(x)$. Тому рівність (8.19) можна переписати у вигляді

$$u(x)f(x)g(x)q(x) + v(x)g(x)f(x)p(x) = h(x).$$

Обидва доданки лівої частини діляться на $f(x)g(x)$. Тому й $h(x)$ ділиться на $f(x)g(x)$.

в) Нехай $(f(x), h(x)) = 1$ і $(g(x), h(x)) = 1$. Тоді існують такі многочлени $u_1(x)$, $v_1(x)$ та $u_2(x)$, $v_2(x)$, що

$$u_1(x)f(x) + v_1(x)h(x) = 1,$$
$$u_2(x)g(x) + v_2(x)h(x) = 1.$$

Перемножимо ці рівності. Одержимо

$$\big(u_1(x)u_2(x)\big) \cdot \big(f(x)g(x)\big) +$$
$$+\big(u_1(x)v_2(x)f(x) + v_1(x)u_2(x)g(x) + v_1(x)v_2(x)h(x)\big) \cdot h(x) = 1.$$

За твердженням 53 звідси випливає, що многочлени $f(x)g(x)$ та $h(x)$ — взаємно прості. □

Лема 13. *Якщо многочлени $f(x)$ і $g(x)$ — незвідні, то вони або взаємно прості, або асоційовані.*

Доведення. Припустимо, що многочлени $f(x)$ і $g(x)$ не є взаємно простими. Із точністю до асоційованості многочлен $f(x)$ має лише два дільники — $f(x)$ і 1. Тому в цьому випадку НСД $(f(x), g(x)) = f(x)$. Але тоді $f(x) \mid g(x)$. Аналогічно доводиться, що $g(x) \mid f(x)$. Отже, $f(x)$ і $g(x)$ — асоційовані. □

Теорема 49 (основна теорема арифметики кільця многочленів)**.** *Кожен ненульовий многочлен із коефіцієнтами з поля P розкладається в кільці $P[x]$ у добуток незвідних многочленів. Цей розклад є однозначним із точністю до порядку множників та їх асоційованості.*

Доведення. Без обмеження загальності можна вважати всі многочлени нормованими. Існування розкладу доведено вже раніше (твердження 52). Зауважимо, що кількість множників у розкладі не може перевищувати степеня многочлена. Тому завжди можна вибрати розклад із найбільшою кількістю множників.

Однозначність розкладу в добуток незвідних будемо доводити індукцією за кількістю множників у розкладі з найбільшою кількістю множників. Для многочленів нульового степеня та незвідних однозначність розкладу очевидна: у першому випадку маємо нуль множників, у другому – один множник, сам многочлен.

Припустимо тепер, що для многочленів, найдовший розклад яких містить менше ніж n множників, однозначність розкладу в добуток незвідних уже доведено. Розглянемо многочлен $f(x)$, найдовший розклад якого в добуток незвідних містить n множників:

$$f(x) = p_1(x)p_2(x)\cdots p_n(x). \tag{8.20}$$

Нехай

$$f(x) = q_1(x)q_2(x)\cdots q_m(x) \quad (m \le n) \tag{8.21}$$

— ще один розклад $f(x)$ у добуток незвідних многочленів. Многочлен $q_m(x)$ є незвідним і ділить $f(x)$. Тому він ділить добуток $p_1(x)p_2(x)\cdots p_n(x)$. Позаяк усі множники $p_i(x)$ також є незвідними, то з леми 13 випливає, що $q_m(x)$ або збігається з одним із цих множників, або взаємно простий із кожним із них. Але в другому випадку з леми Евкліда (теорема 48.а) випливає, що $q_m(x)$ взаємно простий із добутком $p_1(x)p_2(x)\cdots p_n(x)$. Отримана суперечність доводить, що $q_m(x)$ збігається з одним із множників $p_i(x)$. Без обмеження загальності можна вважати, що $q_m(x) = p_n(x)$.

Отже, маємо рівність

$$p_1(x)p_2(x)\cdots p_{n-1}(x)p_n(x) = q_1(x)q_2(x)\cdots q_{m-1}(x)q_m(x).$$

Враховуючи те, що кільці $P[x]$ можна скорочувати, звідси випливає рівність

$$p_1(x)p_2(x)\cdots p_{n-1}(x) = q_1(x)q_2(x)\cdots q_{m-1}(x).$$

Одержали два розклади многочлена $g(x) = p_1(x)p_2(x)\cdots p_{n-1}(x)$. Оскільки для многочлена $g(x)$ розклад $g(x) = p_1(x)p_2(x)\cdots p_{n-1}(x)$ є найдовшим (у противному разі розклад 8.20 не був би найдовшим для $f(x)$) і містить менше ніж n множників, то за припущенням індукції розклад $g(x)$ у добуток незвідних є однозначним. Тому $m-1 = n-1$ і, з точністю до порядку множників у розкладі 8.21,

$$q_1(x) = p_1(x), \;\; q_2(x) = p_2(x), \;\; \ldots, \;\; q_{n-1}(x) = p_{n-1}(x).$$

Отже, розклади 8.20 і 8.21 збігаються, а тому розклад многочлена в добуток незвідних є однозначним. □

Зауваження. **1.** На многочлени з коефіцієнтами з довільних комутативних кілець теорема 49, узагалі кажучи, не узагальнюється. Наприклад, для многочлена x^3 із $\mathbb{Z}_8[x]$ маємо кілька різних розкладів:

$$x^3 = x(x-4)^2 = (x-2)(x^2+2x+4) = (x+2)(x^2-2x+4)\,.$$

Теорема 49 не узагальнюється і на підкільця кільця $P[x]$. Наприклад, множина всіх многочленів вигляду $a_0 + a_2x^2 + \ldots$ (тобто з нульовим лінійним членом) із $\mathbb{R}[x]$ утворює підкільце кільця $\mathbb{R}[x]$. У цьому підкільці многочлени x^2 і x^3 є нерозкладними, що дає два різні розклади для x^6: $x^2 \cdot x^2 \cdot x^2$ і $x^3 \cdot x^3$.

2. Теорема 49 є повним аналогом **основної теореми арифметики**[17]:

У кільці $\mathbb{Z}$ кожне ненульове число розкладається в добуток простих чисел. Цей розклад є однозначним із точністю до порядку множників та їх асоційованості.

Доведення основної теореми арифметики повністю повторює доведення теореми 49.

Розклад многочлена $f(x)$ у добуток незвідних многочленів, записаний у вигляді

$$f(x) = p_1^{k_1}(x)p_2^{k_2}(x)\cdots p_m^{k_m}(x), \tag{8.22}$$

де $p_1(x)$, $p_2(x)$, …, $p_m(x)$ — попарно неасоційовані незвідні многочлени, називається *канонічним* розкладом многочлена $f(x)$.

Вправа 21. *Доведіть, що є рівно p^{n+1} многочленів степеня $\leq n$ із коефіцієнтами з поля $\mathbb{Z}_p$.*

Теорема 50 (Евклід)**.** *Для довільного поля P в кільці $P[x]$ є нескінченно багато попарно неасоційованих незвідних многочленів.*

Теорема є очевидною, якщо поле P — нескінченне: усі лінійні многочлени вигляду $x + a$ є незвідними і попарно неасоційованими. Однак

[17] Основна теорема арифметики має досить цікаву історію. У явному вигляді "Початки" Евкліда її не містять (можливо, тому, що для її доведення потрібен у тій чи іншій формі принцип математичної індукції). Однак деякі твердження з VII книги "Початків" фактично їй еквівалентні. До кінця XVIII ст. вона в явному вигляді так ніде і не формулюється. Її немає навіть у "Вступі до теорії чисел" Лежандра (1798) — найбільш повному на той час викладі теорії чисел. Перше точне формулювання, разом із доведенням, дав лише в 1801 році Гаусс (у своїх знаменитих "Арифметичних дослідженнях").

Можливо, саме через відсутність цієї теореми в Евкліда вона досі в шкільних підручниках подається як очевидний факт, без доведення. В одному з підручників вона навіть оголошена "законом мислення" (що, звичайно, є дурницею).

теорема зовсім не очевидна, якщо поле P є скінченним. Наступне доведення нескінченності множини незвідних многочленів від потужності поля P не залежить і фактично повторює доведення Евкліда нескінченності множини простих чисел.

Доведення теореми 50. Припустимо, що незвідних многочленів скінченна кількість. Нехай

$$p_1(x), \quad p_2(x), \quad \ldots, \quad p_m(x) \tag{8.23}$$

– їх повний список. Розглянемо многочлен

$$f(x) = p_1(x)p_2(x)\cdots p_m(x) + 1.$$

Тут $f(x)$ не ділиться на жоден із многочленів $p_1(x)$, $p_2(x)$, $\ldots$, $p_m(x)$, бо при діленні на кожен із них дає в остачі 1. Але за теоремою 49 $f(x)$ повинен ділитися на якийсь незвідний многочлен $p(x)$. Отже, $p(x)$ не зустрічається в списку (8.23). Таким чином, припущення про скінченність списку незвідних многочленів приводить до суперечності. □

Наслідок 34. *Над полем $\mathbb{Z}_p$ існують незвідні многочлени як завгодно великого степеня.*

Доведення. Над полем $\mathbb{Z}_p$ існує лише скінченна кількість многочленів степеня $\leq n$. Тому степені незвідних многочленів не обмежені згори жодним числом n. □

Зауваження. Насправді над полем $\mathbb{Z}_p$ є незвідні многочлени всіх додатних степенів. Але доведення цього є досить складним.

Двоїстим до поняття найбільшого спільного дільника є поняття найменшого спільного кратного. А саме, многочлен $m(x)$ називається *найменшим спільним кратним* (скорочено: НСК) многочленів $f(x)$ і $g(x)$, якщо він задовольняє такі дві умови:

1) $m(x)$ є спільним кратним многочленів $f(x)$ і $g(x)$, тобто $f(x) \mid m(x)$ і $g(x) \mid m(x)$;

2) $m(x)$ ділить кожне спільне кратне многочленів $f(x)$ і $g(x)$, тобто з $f(x) \mid c(x)$ і $g(x) \mid c(x)$ випливає, що $m(x) \mid c(x)$.

Найменше спільне кратне многочленів $f(x)$ і $g(x)$ позначається $\text{НСК}\,(f(x), g(x))$ або $[f(x), g(x)]$. З умови 2) випливає, що коли $\text{НСК}\,(f(x), g(x))$ існує, то з точністю до асоційованості воно єдине. Справді, якщо $m_1(x)$ і $m_2(x)$ – два такі кратні, то вони повинні ділитися одне на одне.

Твердження 54.

$$\text{НСК}\,(f(x),g(x)) = \frac{f(x)g(x)}{\text{НСД}\,(f(x),g(x))}\,. \tag{8.24}$$

Доведення. Нехай $\text{НСК}\,(f(x),g(x)) = d(x)$. Тоді існують такі многочлени $f_0(x)$ і $)g_0(x)$, що $f(x) = d(x)f_0(x)$, $g(x) = d(x)g_0(x)$. Розглянемо многочлен

$$m(x) = \frac{f(x)g(x)}{\text{НСД}\,(f(x),g(x))} = d(x)f_0(x)g_0(x).$$

Очевидно, що $f(x)|m(x)$ і $g(x)|m(x)$. Нехай тепер $f(x)|M(x)$ і $g(x)|M(x)$. Тоді існують такі многочлени $f_1(x)$ і $g_1(x)$, що $M(x) = f(x)f_1(x) = g(x)g_1(x)$. Оскільки $d(x)$ можна подати у вигляді $d(x) = u(x)f(x) + v(x)g(x)$, то

$$\frac{M(x)}{m(x)} = \frac{M(x)d(x)}{m(x)d(x)} = \frac{M(x)d(x)}{f(x)g(x)} = \frac{M(x)\big(u(x)f(x)+v(x)g(x)\big)}{f(x)g(x)} =$$

$$= \frac{M(x)u(x)f(x)}{f(x)g(x)} + \frac{M(x)v(x)g(x)}{f(x)g(x)} = u(x)\frac{M(x)}{g(x)} + v(x)\frac{M(x)}{f(x)} =$$

$$= u(x)\frac{g(x)g_1(x)}{g(x)} + v(x)\frac{f(x)f_1(x)}{f(x)} = u(x)g_1(x) + v(x)f_1(x)\,.$$

Отже, $M(x) = m(x)\big(u(x)g_1(x) + v(x)f_1(x)\big)$ і $m(x)|M(x)$. □

$\text{НСД}\,(f(x),g(x))$ і $\text{НСК}(f(x),g(x))$ особливо легко обчислюються, якщо відомі канонічні розклади

$$f(x) = p_1^{k_1}(x)p_2^{k_2}(x)\cdots p_m^{k_m}(x), \quad g(x) = p_1^{r_1}(x)p_2^{r_2}(x)\cdots p_m^{r_m}(x)$$

многочленів $f(x)$ і $g(x)$ (дозволивши нульові показники степенів, ми можемо вважати, що в розкладах обох многочленів зустрічаються ті самі незвідні многочлени). Справді, з означень НСД і НСК та теореми 49 одразу випливає, що

$$\text{НСД}\,(f(x),g(x)) = p_1^{\min(k_1,r_1)}(x)p_2^{\min(k_2,r_2)}(x)\cdots p_m^{\min(k_m,r_m)}(x),$$
$$\text{НСК}\,(f(x),g(x)) = p_1^{\max(k_1,r_1)}(x)p_2^{\max(k_2,r_2)}(x)\cdots p_m^{\max(k_m,r_m)}(x).$$

8.2. Корені многочленів

Нехай $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ — довільний многочлен із коефіцієнтами з кільця K. Якщо K_1 — довільне поле або кільце, яке містить K, то для довільного елемента $c \in K_1$ можна обчислити суму $a_0 + a_1c + a_2c^2 + \cdots + a_nc^n$. Значення цієї суми позначається $f(c)$ і називається *значенням многочлена $f(x)$ у точці c*. Зокрема, із кожним многочленом $f \in K[x]$ природно асоціюється функція $f : K \to K$.

Вправа 22. *Нехай $K \subseteq K_1$. Перевірте, що для довільних многочленів $f, g \in K[x]$ та елементів $a \in K$, $b \in K_1$ виконуються рівності*

$$(f + g)(b) = f(b) + g(b), \quad (af)(b) = af(b), \quad (fg)(b) = f(b)g(b).$$

Далі в цьому підрозділі, за винятком явно вказаних прикладів, розглядаються лише многочлени, коефіцієнти яких належать деякому полю P.

Теорема 51 (Безу)**.** *Нехай $f(x) \in P[x]$ і $c \in P$. Значення $f(c)$ многочлена $f(x)$ в точці c дорівнює остачі від ділення $f(x)$ на двочлен $x - c$.*

Доведення. Підставляючи $x = c$ у рівність $f(x) = (x - c)g(x) + r$, отримуємо: $f(c) = r$. □

Елемент c називається *коренем* многочлена $f(x)$, якщо $f(c) = 0$. Із теореми Безу одразу випливає наслідок.

Наслідок 35. *Елемент c буде коренем многочлена $f(x)$ тоді й лише тоді, коли $f(x)$ ділиться на $x - c$.*

Нехай c — корінь многочлена $f(x) \in P[x]$. Найбільше таке натуральне число k, що $f(x)$ ділиться на $(x-c)^k$, називається *кратністю* кореня c. Корені кратності 1 називаються *простими*, а корені більшої кратності — *кратними*. Зокрема, корені кратності 2 називають *подвійними*, кратності 3 — *потрійними* і т. д.

Наслідок із теореми Безу можна уточнити, якщо врахувати і кратність коренів.

Теорема 52. *Якщо $a_1, \ldots, a_m$ — корені многочлена $f(x) \in P[x]$ кратностей $k_1, \ldots, k_m$ відповідно, то $f(x)$ має вигляд*

$$f(x) = (x - a_1)^{k_1} \cdots (x - a_m)^{k_m} g(x)\,,$$

причому жоден з елементів $a_1, \ldots, a_m$ не є коренем многочлена $g(x)$.

Доведення. Якщо $a \neq b$, то многочлени $(x-a)^k$ і $(x-b)^m$ — взаємно прості. Тому перша частина твердження теореми одразу випливає з теореми 48.б і однозначності розкладу на незвідні множники в кільці многочленів. Якби якесь a_i було коренем многочлена $g(x)$, то за наслідком із теореми Безу $g(x)$ ділився б на $x - a_i$. Але тоді $f(x)$ ділився б на $(x - a_i)^{k_i+1}$, що суперечить означенню кратності кореня. □

Наслідок 36. *Кількість коренів многочлена (з урахуванням їх кратностей) не перевищує степеня многочлена, причому рівність досягається тоді й лише тоді, коли многочлен розкладається на лінійні множники. Зокрема, многочлен степеня n із коефіцієнтами з поля P має в цьому полі не більше ніж n різних коренів.*

Твердження 55. *Якщо степінь кожного із многочленів $f(x)$ і $g(x)$ не перевищує n і для попарно різних елементів $a_1, \ldots, a_{n+1}$ виконуються рівності $f(a_i) = g(a_i)$, то $f(x) = g(x)$.*

Доведення. Степінь многочлена $f(x) - g(x)$ не перевищує n, але він має $n + 1$ різних коренів $a_1, \ldots, a_{n+1}$. За наслідком 36 це можливе лише тоді, коли многочлен $f(x) - g(x)$ є нульовим, тобто, коли $f(x) = g(x)$. □

Наслідок 37. *Якщо поле P нескінченне, то різні многочлени визначають різні функції.*

Доведення. Із твердження 55 випливає, що два різні многочлени $f(x)$ і $g(x)$ степеня $\leq n$ можуть набувати однакових значень не більше ніж в n точках. □

Твердження 56. *Взаємно прості многочлени $f(x)$ і $g(x)$ із $P[x]$ не мають спільних коренів у жодному розширенні поля P.*

Доведення. Якщо многочлени $f(x)$ і $g(x)$ мають спільний корінь c в якомусь розширенні $P' \supseteq P$, то $x - c$ є їх спільним дільником у кільці $P'[x]$. Зокрема, у кільці $P'[x]$ НСД $(f(x), g(x))$ ділиться на $x - c$. При знаходженні НСД за допомогою алгоритму Евкліда використовуються лише арифметичні дії, тому при переході до більшого поля НСД $(f(x), g(x))$ не змінюється. Але за умовою в кільці $P[x]$ НСД $(f(x), g(x)) = 1$. □

Зауваження. У випадку многочленів із коефіцієнтами з довільного кільця теорема 52 і наслідок із неї перестають бути правильними. Наприклад, многочлени $x^3 \in \mathbb{Z}_8[x]$, $x^2 - 1 \in \mathbb{Z}_8[x]$ і $x^2 - 1 \in \mathbb{Z}_{15}[x]$ мають у відповідних кільцях по 4 корені.

Припустимо тепер, що многочлен $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ розкладається на лінійні множники:

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = a_n(x - c_1)(x - c_2)\cdots(x - c_n). \qquad (8.25)$$

Тоді $c_1, c_2, \ldots, c_n$ є його коренями, причому кожен із коренів зустрічається стільки разів, скільки становить його кратність. Якщо множники у правій частині рівності 8.25 перемножити, а потім прирівняти коефіцієнти при відповідних степенях x в обох частинах рівності, то одержимо

$$\begin{aligned}
x^n: &\quad a_n = a_n\,,\\
x^{n-1}: &\quad a_{n-1} = -a_n(c_1 + c_2 + \cdots + c_n)\,,\\
x^{n-2}: &\quad a_{n-2} = a_n(c_1c_2 + c_1c_3 + \cdots + c_{n-1}c_n),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
x^{n-k}: &\quad a_{n-k} = (-1)^k a_n \cdot \sum_{1\le i_1<i_2<\cdots<i_k\le n} c_{i_1}c_{i_2}\cdots c_{i_k}\,,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
x^0: &\quad a_0 = (-1)^n a_n \cdot c_1c_2\cdots c_n\,.
\end{aligned}$$

Звідси отримуємо формули

$$\begin{aligned}
c_1 + c_2 + \ldots + c_n &= -\frac{a_{n-1}}{a_n}\,,\\
c_1c_2 + c_1c_3 + \ldots + c_{n-1}c_n &= \frac{a_{n-2}}{a_n}\,,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\sum_{1\le i_1<i_2<\cdots<i_k\le n} c_{i_1}c_{i_2}\cdots c_{i_k} &= (-1)^k\,\frac{a_{n-k}}{a_n}\,,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
c_1c_2\cdots c_n &= (-1)^n\,\frac{a_0}{a_n}\,,
\end{aligned} \qquad (8.26)$$

які називається *формулами Вієта*. Вони встановлюють зв'язок між коренями многочлена та його коефіцієнтами.

Для дослідження властивостей кратних коренів дуже корисним є поняття похідної многочлена. Відоме з аналізу означення похідної спирається на поняття граничного переходу і є непридатним для многочленів з коефіцієнтами з довільного поля (наприклад, для многочленів з коефіцієнтами зі скінченного поля класів лишків $\mathbb{Z}_p$). Тому в алгебрі користуються таким означенням похідної многочлена, яке не вимагає граничного переходу.

Означення 19. ***Похідною*** *многочлена*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

називається многочлен

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1.$$

Твердження 57 (про властивості похідної)**.**
а) $(f(x) + g(x))' = f'(x) + g'(x)$;
б) $(cf(x))' = cf'(x)$;
в) $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$;
г) $(f^k(x))' = kf^{k-1}(x)f'(x)$.

Доведення. Перші дві властивості безпосередньо випливають з означення похідної.

в) Нехай $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$. Тоді

$$(f(x)g(x))' = \left(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j}\right)' = \sum_{i=0}^{n}\sum_{j=0}^{m}(i+j)a_i b_j x^{i+j-1} =$$

$$= \sum_{i=0}^{n}\sum_{j=0}^{m} i a_i b_j x^{i+j-1} + \sum_{i=0}^{n}\sum_{j=0}^{m} j a_i b_j x^{i+j-1} =$$

$$= \left(\sum_{i=1}^{n} i a_i x^{i-1}\right)\left(\sum_{j=0}^{m} b_j x^j\right) + \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=1}^{m} j b_j x^{j-1}\right) =$$

$$= f(x)g'(x) + f'(x)g(x)\,.$$

г) Твердження легко доводиться індукцією за k. Справді, для $k = 1$ воно тривіальне, а крок індукції легко обґрунтовується:

$$(f^k(x))' = (f^{k-1}(x)\cdot f(x))' = (f^{k-1}(x))'\cdot f(x) + f^{k-1}(x)\cdot f'(x) =$$
$$= (k-1)f^{k-2}(x)f'(x)\cdot f(x) + f^{k-1}(x)\cdot f'(x) = kf^{k-1}(x)f'(x). \qquad \square$$

Вправа 23. *Обчисліть* $[f(g(x))]'$.

Похідні вищих порядків визначаються так само, як і в аналізі — рекурентно: $f^{(k+1)}(x) = (f^{(k)}(x))'$.

Твердження 58. *Якщо* $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, *то*

$$f^{(k)}(x) = a_k \frac{k!}{0!} + a_{k+1} \frac{(k+1)!}{1!} x + \cdots + a_n \frac{n!}{(n-k)!} x^{n-k} =$$

$$= k! \left(a_k \binom{k}{0} + a_{k+1} \binom{k+1}{1} x + \cdots + a_n \binom{n}{n-k} x^{n-k} \right).$$

Доведення. Очевидно, що

$$(x^m)^{(k)} = m(x^{m-1})^{(k-1)} = m(m-1)(x^{m-2})^{(k-2)} = \ldots$$
$$\ldots = m(m-1)(m-2)\ldots(m-k+1)x^{m-k} =$$
$$= \frac{m!}{(m-k)!} \cdot x^{m-k} = k! \binom{m}{m-k} \cdot x^{m-k}.$$

Далі лишається лише розглянути $f(x)$ як суму одночленів і скористатися першими двома властивостями із твердження 57. □

Вправа 24. *Доведіть наступну формулу Тейлора* (*про розклад многочлена в ряд*) : *якщо* $\deg f(x) = n$, *то*

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!} (x-c)^k.$$

Твердження 59. *а) Якщо* c *— кратний корінь кратності* $k \geq 2$ *многочлена* $f(x)$, *то* c *є коренем кратності щонайменше* $k-1$ *його похідної* $f'(x)$.

б) Якщо c *— простий корінь многочлена* $f(x)$, *то* $f'(c) \neq 0$.

Зокрема, корінь c *многочлена* $f(x)$ *буде коренем його похідної* $f'(x)$ *тоді й лише тоді, коли він є кратним коренем.*

Доведення. а) Якщо c є коренем кратності k, то $f(x)$ можна записати у вигляді $f(x) = (x-c)^k g(x)$, де $g(c) \neq 0$. Тоді

$$f'(x) = k(x-c)^{k-1} g(x) + (x-c)^k g'(x) = \tag{8.27}$$
$$= (x-c)^{k-1}(kg(x) + (x-c)g'(x)).$$

Отже, для похідної $f'(x)$ c є коренем кратності щонайменше $k-1$.

б) Якщо c є простим коренем, то $f(x)$ має вигляд $f(x) = (x-c)g(x)$, де $g(c) \neq 0$. Тому $f'(x) = g(x) + (x-c)g'(x)$ і $f'(c) = g(c) \neq 0$. □

У твердженні 59.а дається лише нижня межа для кратності c як кореня похідної. Чи буде вона точною? У загальному випадку — ні. Наприклад, для многочлена $f(x) = (x+1)^2(x^3+x+1)$ із коефіцієнтами з поля $\mathbb{Z}_2$ маємо

$$f'(x) = 2(x+1)(x^3+x+1) + (x+1)^2(3x^2+1) = (x+1)^4 .$$

Щоб нижня межа стала точною, треба накласти додаткове обмеження на поле P. Будемо говорити, що поле P має *характеристику* 0, якщо для довільного додатного k виконується нерівність

$$\underbrace{1+1+\ldots+1}_{k \text{ доданків}} \neq 0.$$

Полями нульової характеристики будуть, наприклад, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. У той же час поле класів лишків $\mathbb{Z}_p$ таким не є.

Твердження 60. *Якщо характеристика поля P дорівнює 0 і c — корінь кратності $k \geq 2$ многочлена $f(x) \in P[x]$, то c є коренем кратності $k-1$ його похідної $f'(x)$.*

Доведення. Для доведення досить показати, що c не є коренем другого множника $kg(x) + (x-c)g'(x)$ із правої частини рівності (8.27). Але значення цього множника в точці c дорівнює $kg(c)$. Позаяк характеристика поля P дорівнює 0 і $g(c) \neq 0$, то $kg(c) \neq 0$. □

Наслідок 38. *Якщо характеристика поля P дорівнює 0, то кратність c як кореня многочлена $f(x) \in P[x]$ дорівнює найменшому порядку k похідної, для якої $f^{(k)}(c) \neq 0$.*

Останній наслідок може бути підставою “аналітичного” означення кратності кореня як “порядку” нульового значення многочлена в цій точці.

Твердження 61. *Якщо характеристика поля P дорівнює 0 і многочлен $p(x) \in P[x]$ — незвідний, то $p(x)$ не має кратних коренів у жодному розширенні $P_1 \supseteq P$ поля P.*

Доведення. Із точністю до асоційованості незвідний многочлен $p(x)$ має лише два дільники: 1 і $p(x)$. Похідна $p'(x)$ має менший степінь, ніж $p(x)$, тому не може ділитись на $p(x)$. Отже, НСД$(p(x), p'(x)) = 1$. Якби $p(x)$ мав кратні корені в якомусь розширенні $P_1 \supseteq P$, то із твердження 59 випливало б, що в кільці $P_1[x]$ многочлен $p(x)$ не є взаємно простий

зі своєю похідною. Але це суперечить рівності НСД $(p(x), p'(x)) = 1$, бо перехід до більшого поля не змінює ланцюжок рівностей в алгоритмі Евкліда, а тому не змінює і НСД многочленів $p(x)$ і $p'(x)$. □

Твердження 62. *Нехай характеристика поля P дорівнює 0 і $f(x) \in P[x]$. Якщо незвідний многочлен $p(x)$ входить у канонічний розклад многочлена $f(x)$ із показником $k > 0$, то він входить у канонічний розклад похідної $f'(x)$ із показником $k - 1$.*

Доведення. Нехай $f(x) = p^k(x)g(x)$, де многочлен $g(x)$ не ділиться на $p(x)$. Тоді

$$f'(x) = kp^{k-1}(x)p'(x)g(x) + p^k(x)g'(x) = p^{k-1}(x)\big(kp'(x)g(x) + p(x)g'(x)\big).$$

Розглянемо другий множник $kp'(x)g(x) + p(x)g'(x)$ у правій частині. Степінь $p'(x)$ менший за степінь $p(x)$, а $g(x)$ не ділиться на $p(x)$. Тому перший $kp'(x)g(x)$ доданок на $p(x)$ не ділиться. Оскільки другий доданок $p(x)g'(x)$ на $p(x)$ ділиться, то вся сума на $p(x)$ не ділиться. Отже, $p(x)$ входить у канонічний розклад похідної $f'(x)$ із показником $k - 1$. □

Наслідок 39. *Нехай P — поле характеристики 0 і многочлен $f(x) \in P[x]$ має канонічний розклад $f(x) = p_1^{k_1}(x)p_2^{k_2}(x) \cdots p_m^{k_m}(x)$. Тоді*

а) похідна $f'(x)$ має вигляд

$$f'(x) = p_1^{k_1-1}(x)p_2^{k_2-1}(x) \cdots p_m^{k_m-1}(x)g(x),$$

де $g(x)$ не ділиться на жоден із незвідних многочленів $p_1(x)$, $p_2(x)$, …, $p_m(x)$;

б) НСД $(f(x), f'(x)) = p_1^{k_1-1}(x)p_2^{k_2-1}(x) \cdots p_m^{k_m-1}(x)$;

в) многочлен $f(x)$ не має кратних множників тоді й лише тоді, коли він взаємно простий зі своєю похідною;

г) $\dfrac{f(x)}{\text{НСД}\,(f(x), f'(x))} = p_1(x)p_2(x) \cdots p_m(x).$

Доведення. а) Випливає із твердження 62 і однозначності канонічного розкладу.

б) Випливає з а).

в) Із б) випливає, що НСД $(p(x), p'(x)) = 1$ тоді й лише тоді, коли $k_1 - 1 = k_2 - 1 = \ldots = k_m - 1 = 0$, тобто, коли $k_1 = k_2 = \ldots = k_m = 1$.

г) Випливає з б). □

8.3. Многочлени над $\mathbb{R}$ і $\mathbb{C}$

Поле P називається *алгебрично замкненим*, якщо кожен многочлен ненульового степеня із $P[x]$ розкладається над полем P на лінійні множники.

Твердження 63. *Наведені умови рівносильні:*

а) Поле P – алгебрично замкнене.

б) Кожен многочлен $f(x) \in P[x]$ ненульового степеня має в полі P принаймні один корінь.

в) Многочлен $f(x) \in P[x]$ буде незвідним тоді й лише тоді, коли він лінійний.

Доведення. а) $\Rightarrow$ б). Нехай $f(x) = a_0 + a_1x + \ldots + a_nx^n$ — многочлен ненульового степеня. Він розкладається на лінійні множники:

$$f(x) = a_n(x - c_1)(x - c_2)\cdots(x - c_n).$$

Тоді $c_1, \ldots, c_n$ є коренями $f(x)$.

б) $\Rightarrow$ в). Лінійні многочлени завжди є незвідними. Нехай тепер $f(x)$ – многочлен степеня > 1. Він має якийсь корінь c. За наслідком із теореми Безу $f(x)$ ділиться на $x - c$: $f(x) = (x - c)g(x)$. Позаяк обидва множники ненульового степеня, то $f(x)$ – звідний.

в) $\Rightarrow$ а). За основною теоремою арифметики кільця $P[x]$ кожен многочлен розкладається в добуток незвідних. За припущенням незвідними є лише лінійні многочлени. Тому кожен многочлен ненульового степеня розкладається на лінійні множники. Отже, поле P – алгебрично замкнене. □

Вправа 25. *Доведіть, що, коли поле P — алгебрично замкнене, то кожен многочлен $f(x) \in P[x]$ додатного степеня набуває всіх значень із поля P.*

Теорема 53 (основна теорема алгебри)**.** *Кожен многочлен ненульового степеня з комплексними коефіцієнтами має в полі комплексних чисел принаймні один корінь.*

Гучний титул “основної теореми алгебри” ця теорема одержала у XVIII ст., коли поле $\mathbb{C}$ було найбільшим із відомих, а основною задачею алгебри вважалося розв’язування алгебричних рівнянь. Із того часу роль алгебри в математиці дуже змінилася і задача розв’язування алгебричних рівнянь відійшла на далеку периферію. Більше того, з нинішнього погляду ця теорема є і не зовсім теоремою алгебри: усі її доведення більшою чи меншою мірою використовують поняття неперервності, тобто

топологічну структуру полів $\mathbb{R}$ і $\mathbb{C}$. Деякі із цих доведень (зокрема, досить короткі) є зовсім неалгебричними. А ті доведення, які можна вважати "майже" алгебричними, використовують поняття, що виходять за межі нашого курсу.

Перші точні формулювання і спроби доведення цієї теореми належать Д'Аламберу й Ойлеру. Перше відносно строге доведення дав Гаусс у 1799 році. Остаточну форму цьому доведенню, яке спирається лише на елементарні факти математичного аналізу й використовує ідеї Д'Аламбера, Ойлера, Гаусса, Коші, надав 1814 року Арган. Саме доведення Аргана наводиться нині в багатьох підручниках.

Із причини "неалгебричності" теореми 53 ми не будемо наводити її доведення. Це доведення можна знайти в багатьох підручниках. Назвемо лише кілька: [4, 9, 10, 14, 15, 17]. Зауважимо, що у [15] є навіть два різні доведення, друге з яких "майже" алгебричне.

Наслідок 40. *а) Кожен многочлен $f(x) \in \mathbb{C}[x]$ ненульового степеня розкладається над полем $\mathbb{C}$ на лінійні множники.*

б) Кожен многочлен $f(x) \in \mathbb{C}[x]$ степеня n має над полем $\mathbb{C}$, з урахуванням кратності, рівно n коренів.

Твердження 64. *а) Многочлен із дійсними коефіцієнтами буде незвідним над полем дійсних чисел тоді й лише тоді, коли він є лінійним або многочленом другого степеня з від'ємним дискримінантом.*

б) Кожен многочлен ненульового степеня з дійсними коефіцієнтами розкладається над полем $\mathbb{R}$ на множники першого і другого степеня.

в) Кожен многочлен непарного степеня з дійсними коефіцієнтами має принаймні один дійсний корінь.

Доведення. а) Зрозуміло, що лінійні многочлени і ті многочлени другого степеня з дійсними коефіцієнтами, які мають від'ємний дискримінант (а тому не мають дійсних коренів), є незвідними. Навпаки, якщо незвідний многочлен $f(x)$ із дійсними коефіцієнтами має дійсний корінь c, то він ділиться на $x - c$. А тому буде відрізнятися від $x - c$ лише числовим множником. Якщо ж дійсних коренів нема, то він має комплексний корінь z. За наслідком 2 спряжене число $\overline{z}$ також буде коренем многочлена $f(x)$. Але тоді $f(x)$ ділиться на многочлен другого степеня $g(x) = (x - z)(x - \overline{z}) = x^2 - 2\mathrm{Re}\, z \cdot x + |z|^2$, який має дійсні коефіцієнти і від'ємний дискримінант. Із незвідності $f(x)$ випливає, що він відрізняється від $g(x)$ лише числовим множником.

б) Випливає з а).

в) Випливає з б). □

8.4. Многочлени над $\mathbb{Z}$ і $\mathbb{Q}$

Теорема 54. *Нехай нескоротний дріб p/q є коренем многочлена $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$ із цілими коефіцієнтами. Тоді $q \mid a_n$ і для довільного цілого числа m $(p - qm) \mid f(m)$. Зокрема, $p \mid a_0$.*

Доведення. Оскільки

$$f\left(\frac{p}{q}\right) = a_0 + a_1\frac{p}{q} + \ldots + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + a_n\frac{p^n}{q^n} = 0, \tag{8.28}$$

то

$$a_0q^n + a_1pq^{n-1} + \cdots + a_2p^{n-1}q + a_np^n = 0.$$

У лівій частині всі доданки, крім останнього, діляться на q. Тому й останній доданок повинен ділитися на q. Оскільки p і q взаємно прості, то на q ділиться a_n.

Віднімемо тепер від рівності

$$f(m) = a_0 + a_1m + \ldots + a_{n-1}m^{n-1} + a_mx^n$$

рівність (8.28). Одержимо:

$$f(m) - 0 = a_1\left(m - \frac{p}{q}\right) + \ldots + a_{n-1}\left(m^{n-1} - \frac{p^{n-1}}{q^{n-1}}\right) + a_n\left(m^n - \frac{p^n}{q^n}\right),$$

звідки

$$q^nf(m) = a_1q^{n-1}(qm - p) + \ldots + a_{n-1}q(q^{n-1}m^{n-1} - p^{n-1}) + a_m(q^nm^n - p^n).$$

Позаяк для кожного натурального k число $a^k - b^k$ ділиться на $a - b$, то всі доданки у правій частині діляться на $qm - p$. Тому $q^nf(m)$ також ділиться на $qm - p$. Кожне просте число, яке ділить q^n і $qm - p$, буде ділити і числа q та p. Але q і p взаємно прості, тому q^n і $qm - p$ також взаємно прості. Отже, на $qm - p$ ділиться $f(m)$.

Зокрема, при $m = 0$ одержуємо, що $f(0) = a_0$ ділиться на p. □

Наслідок 41. *а) Цілі корені многочлена із цілими коефіцієнтами є дільниками його вільного члена.*

б) Якщо старший коефіцієнт a_n многочлена $f(x) \in \mathbb{Z}[x]$ дорівнює 1, то всі раціональні корені многочлена $f(x)$ є цілими.

в) Для довільних попарно різних простих чисел $p_1, \ldots, p_k$ число $a = \sqrt[n]{p_1^{m_1} \cdots p_k^{m_k}}$ буде раціональним тоді й лише тоді, коли всі показники $m_1, \ldots, m_k$ діляться на n (і в цьому випадку число a буде цілим).

Доведення. а) Якщо записати цілий корінь у вигляді $p/1$, то за теоремою 54 $p \mid a_0$.

б) У цьому випадку знаменник q раціонального кореня p/q повинен бути дільником 1. Тому $q = 1$.

в) Число $a = \sqrt[n]{p_1^{m_1} \cdots p_k^{m_k}}$ є коренем многочлена $x^n - p_1^{m_1} \cdots p_k^{m_k}$ із цілими коефіцієнтами і старшим коефіцієнтом 1. Нехай число a – раціональне. Тоді за твердженням б) воно повинне бути цілим числом і, за твердженням а), дільником вільного члена $p_1^{m_1} \cdots p_k^{m_k}$. Звідси випливає, що число a має вигляд $a = p_1^{r_1} \cdots p_k^{r_k}$. Оскільки $a^n = p_1^{m_1} \cdots p_k^{m_k}$, то $m_1 = nr_1, \ldots, m_k = nr_k$.

Обернене твердження очевидне. □

З останнього твердження цього наслідку випливає, зокрема, що корінь цілого степеня із цілого числа буде або цілим числом, або ірраціональним.

Приклад 20. Знайдемо раціональні корені многочлена

$$f(x) = 6x^5 + 13x^4 - 2x^3 + 2x^2 + 17x - 6.$$

Нехай нескоротний дріб p/q є коренем. Тоді за твердженням 54 чисельник p повинен бути дільником вільного члена -6, а знаменник q — дільником старшого коефіцієнта 6. Це дає такі "кандидати в корені":

$$\frac{\pm 6}{1},\ \frac{\pm 3}{1},\ \frac{\pm 2}{1},\ \frac{\pm 1}{1},\ \frac{\pm 3}{2},\ \frac{\pm 1}{2},\ \frac{\pm 2}{3},\ \frac{\pm 1}{3},\ \frac{\pm 1}{6}. \tag{8.29}$$

$f(1) = 30$ і $f(-1) = 12$. Тому за твердженням 54 сума $p + q$ повинна бути дільником числа 12, а різниця $p - q$ — дільником числа 30. Після перевірки цих умов зі списку (8.29) залишається лише 7 "кандидатів у корені":

$$\frac{\pm 2}{1},\ \frac{-3}{2},\ \frac{\pm 1}{2},\ \frac{-2}{3},\ \frac{1}{3}.$$

$f(2) = 420$. Перевірка умови $(p - 2q) \mid 420$ відкидає ще число $\frac{-2}{3}$. Крім того, $f(-2) = 0$, отже, число -2 є коренем. Після цього лишається лише 4 "кандидати":

$$\frac{-3}{2},\ \frac{-1}{2},\ \frac{1}{2},\ \frac{1}{3}.$$

Безпосередня перевірка показує, що перше й останнє із цих чисел є коренями, а друге та третє – ні. Таким чином, многочлен $f(x)$ має три раціональні корені: -2, $\frac{-3}{2}$ і $\frac{1}{3}$.

При дослідженні звідності многочленів із цілими коефіцієнтами часто буває корисною наступна конструкція. Нехай

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$$

– многочлен із цілими коефіцієнтами. *Редукцією $f(x)$ за модулем* простого числа p називається многочлен

$$[f(x)]_p = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_{n-1}}x^{n-1} + \overline{a_n}x^n \in \mathbb{Z}_p[x],$$

коефіцієнтами якого є лишки за модулем p відповідних коефіцієнтів многочлена $f(x)$. З означень дій із многочленами і дій із лишками випливає, що

$$[f(x) + g(x)]_p = [f(x)]_p + [g(x)]_p, \qquad [f(x)g(x)]_p = [f(x)]_p[g(x)]_p. \quad (8.30)$$

Із другої з рівностей (8.30) випливає, що, коли многочлен $f(x)$ є звідним над кільцем $\mathbb{Z}$, то редукований многочлен буде звідним над полем $\mathbb{Z}_p$. Зворотне твердження, взагалі кажучи, неправильне: многочлен x^2+x+2 не має цілих коренів, а тому незвідний над $\mathbb{Z}$, але редукований за модулем 2 многочлен є звідним:

$$[x^2 + x + 2]_2 = x^2 + x = x(x + 1).$$

Очевидно, що, коли многочлен із цілими коефіцієнтами є звідним над $\mathbb{Z}$, то він буде звідним і над $\mathbb{Q}$. Зворотна ж імплікація зовсім не є очевидною. Для її доведення нам знадобиться одне допоміжне поняття.

Многочлен із цілими коефіцієнтами називається *примітивним*, якщо його коефіцієнти в сукупності взаємно прості.

Лема 14 (Гаусс)**.** *Добуток двох примітивних многочленів також є примітивним многочленом.*

Доведення. Нехай $g(x) = a_0 + a_1x + \ldots + a_nx^n$ і $h(x) = b_0 + b_1x + \ldots + b_mx^m$ – такі примітивні многочлени, що їх добуток $f(x) = g(x)h(x)$ не є примітивним. Нехай $d > 1$ – НСД коефіцієнтів многочлена $f(x)$ і p – якийсь із простих дільників числа d. Застосовуючи до рівності $f(x) = g(x)h(x)$ редукцію за модулем p, одержимо

$$0 = [g(x)]_p[h(x)]_p.$$

Але із примітивності многочленів $g(x)$ і $h(x)$ випливає, що не всі їхні коефіцієнти діляться на p. Тому $[g(x)]_p \neq 0$, $[h(x)]_p \neq 0$ і $[g(x)]_p[h(x)]_p \neq 0$. Отже, припущення про непримітивність многочлена $f(x)$ приводить до суперечності. □

Теорема 55 (Гаусс)**.** *Якщо многочлен $f(x)$ із цілими коефіцієнтами є незвідним над кільцем $\mathbb{Z}$ цілих чисел, то він лишається незвідним і над полем $\mathbb{Q}$ раціональних чисел.*

Доведення. Досить довести, що, коли многочлен $f(x)$ розкладається над полем $\mathbb{Q}$, то він розкладається і над кільцем $\mathbb{Z}$.

Нехай $f(x) = g(x)h(x)$ — розклад многочлена $f(x)$ над полем $\mathbb{Q}$. Зведемо коефіцієнти множників $g(x)$ і $h(x)$ до спільних знаменників m_1 і m_2 відповідно: $f(x) = \dfrac{g_1(x)}{m_1} \cdot \dfrac{h_1(x)}{m_2}$. Многочлени $g_1(x)$ і $h_1(x)$ мають цілі коефіцієнти, тому в кожному з них ми можемо виділити найбільший спільний дільник коефіцієнтів: $f(x) = \dfrac{d_1 g_2(x)}{m_1} \cdot \dfrac{d_2 h_2(x)}{m_2}$, де $g_2(x)$ і $h_2(x)$ – примітивні многочлени. Останню рівність перепишемо у вигляді

$$m_1 m_2 f(x) = d_1 d_2 g_2(x) h_2(x)\,. \tag{8.31}$$

За лемою Гаусса добуток примітивних многочленів $g_2(x)$ і $h_2(x)$ знову є примітивним многочленом, тому НСД коефіцієнтів многочлена у правій частині рівності (8.31) дорівнює $d_1 d_2$. З іншого боку, усі коефіцієнти многочлена у лівій частині рівності (8.31) діляться на $m_1 m_2$. Тому $m_1 m_2 \mid d_1 d_2$ і дріб $\dfrac{d_1 d_2}{m_1 m_2}$ є цілим числом. Це дає нам розклад $f(x)$ над кільцем $\mathbb{Z}$:

$$f(x) = \frac{d_1 d_2}{m_1 m_2} g_2(x) \cdot h_2(x)\,. \qquad \square$$

Є проста ознака, яка в багатьох випадках дозволяє з'ясувати, чи буде многочлен із цілими коефіцієнтами незвідним над $\mathbb{Z}$.

Теорема 56 (ознака Айзенштайна)**.** *Нехай $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ – многочлен із цілими коефіцієнтами. Якщо існує просте число p, яке задовольняє такі умови:*

(1) *старший коефіцієнт a_n не ділиться на p;*

(2) *усі інші коефіцієнти діляться p;*

(3) *вільний член a_0 не ділиться на p^2,*

то многочлен $f(x)$ є незвідним над кільцем $\mathbb{Z}$ цілих чисел.

Доведення. Нехай

$$f(x) = (b_m x^m + \ldots + b_1 x + b_0)(c_k x^k + \ldots + c_1 x + c_0),$$

де $k, m > 0$ і $k + m = n$. Застосовуючи редукцію за модулем числа p, одержимо

$$[f(x)]_p = \overline{a_n}x^n = (\overline{b_m}x^m + \ldots + \overline{b_1}x + \overline{b_0})(\overline{c_k}x^k + \ldots + \overline{c_1}x + \overline{c_0})\,.$$

Оскільки над полем $\mathbb{Z}_p$ розклад многочлена на незвідні множники однозначний, то кожен дільник многочлена $\overline{a_n}x^n$ має вигляд $\overline{a}x^l$. Тому

$$\overline{b_{m-1}} = \ldots = \overline{b_1} = \overline{b_0} = \overline{0} = \overline{c_{k-1}} = \ldots = \overline{c_1} = \overline{c_0}\,.$$

Отже, b_0 і c_0 діляться на p. Але тоді коефіцієнт $a_0 = b_0c_0$ ділиться на p^2, що суперечить умові. □

Звертаємо увагу на те, що ознака Айзенштайна дає лише достатні умови незвідності многочлена $f(x) \in \mathbb{Z}[x]$. Наприклад, многочлен $x^2 + x + 3$ є незвідним над кільцем $\mathbb{Z}$, але не існує простого числа p, яке б для цього многочлена задовольняло умови ознаки Айзенштайна.

Приклад 21. 1. Многочлен $2x^5 - 3x^4 + 6x^3 - 9x + 12$ буде незвідним над $\mathbb{Z}$, бо для цього многочлена число 3 задовольняє умови ознаки Айзенштайна.

2. Для кожного простого числа p многочлен

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \tag{8.32}$$

буде незвідним над $\mathbb{Z}$.

В останньому випадку безпосередньо застосувати ознаку Айзенштайна не вдається. Але є один прийом, який дозволяє значно розширити межі застосування цієї ознаки. Ґрунтується він на простому зауваженні: для довільної лінійної заміни $x = ay + b$, $a, b \in \mathbb{Z}$, $a \neq 0$, многочлени $f(x)$ і $g(y) = f(ay + b)$ або обидва звідні, або обидва незвідні. Справді, якщо $f(x) = u_1(x)u_2(x)$, то $g(y) = u_1(ay + b)u_2(ay + b)$, а якщо $g(y) = v_1(y)v_2(y)$, то $f(x) = v_1(\frac{1}{x}x - \frac{b}{a})v_2(\frac{1}{x}x - \frac{b}{a})$.

У нашому випадку перепишемо многочлен $f(x)$ так: $f(x) = \dfrac{x^p - 1}{x - 1}$. Тоді легко помітити, що заміною $x = y + 1$ він зводиться до многочлена

$$y^{p-1} + \binom{p}{1}y^{p-2} + \ldots + \binom{p}{p-2}y + \binom{p}{p-1},$$

який задовольняє умови ознаки Айзенштайна для числа p.

8.5. Інтерполяція

Нехай $x_0, x_1, \ldots, x_n$ — попарно різні елементи поля P. Часто, особливо в застосуваннях, виникає задача відшукання такого многочлена $f(x) \in P[x]$, який у точках $x_0, x_1, \ldots, x_n$ набуває відповідно наперед заданих значень $b_0, b_1, \ldots, b_n$. Ця задача називається *задачею інтерполяції*, а сам многочлен – $f(x)$ *інтерполяційним многочленом*. Одразу виникає кілька питань:
1) чи завжди інтерполяційний многочлен існує?
2) якщо такі многочлени існують, то скільки їх?
3) як шукати інтерполяційний многочлен?

Теорема 57. *Для довільних попарно різних точок $x_0, x_1, \ldots, x_n$ і довільних значень $b_0, b_1, \ldots, b_n$ існує єдиний інтерполяційний многочлен $f(x)$ степеня $\leq n$.*

Доведення. Запишемо шуканий многочлен із невизначеними коефіцієнтами: $f(x) = a_0 + a_1x + \ldots + a_nx^n$ (*увага*: коефіцієнти $a_0, a_1, \ldots, a_n$ є невідомими!). Тоді мають виконуватися рівності:

$$\begin{array}{ccccccccc} a_0 & + & a_1x_0 & + & \ldots & + & a_nx_0^n & = & b_0, \\ a_0 & + & a_1x_1 & + & \ldots & + & a_nx_1^n & = & b_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_0 & + & a_1x_n & + & \ldots & + & a_nx_n^n & = & b_n. \end{array} \tag{8.33}$$

Ця СЛР є квадратною, а її визначник

$$\Delta = \begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ 1 & x_2 & x_2^2 & \ldots & x_2^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{vmatrix}$$

є визначником Вандермонда. Оскільки точки $x_0, x_1, x_2, \ldots, x_n$ є попарно різними, то $\Delta \neq 0$. Із теореми Крамера тепер випливає, що система (8.33) має єдиний розв'язок. □

Зауваження. **1.** Якщо не накладати обмеження на степінь, то інтерполяційних многочленів існує нескінченно багато. Справді, якщо $f(x)$ – інтерполяційний многочлен із теореми 57, то для довільного многочлена $g(x)$ многочлен $f(x) + (x - x_0)(x - x_1) \cdots (x - x_n)g(x)$ також буде інтерполяційним.

2. Із теореми 57 випливає досить несподіваний факт: дійсний чи комплексний многочлен повністю визначається своєю поведінкою в будь–якому околі будь–якої точки (позаяк цей окіл містить нескінченно багато точок). Іншими словами, локальна поведінка многочлена повністю визначає його глобальну поведінку. Пізніше у курсі теорії функцій комплексної змінної ви познайомитеся зі значно ширшим класом функцій з аналогічною властивістю – так званими *аналітичними функціями*, які можна вважати дуже широким узагальненням поняття многочлена.

Вправа 26. *Доведіть, що для довільної точки a і довільних значень b_0, b_1, b_2, …, b_n існує єдиний многочлен $f(x)$ степеня $\leq n$, який задовольняє умови $f(a) = b_0$, $f'(a) = b_1$, …, $f^{(n)}(a) = b_n$.*

Шукати інтерполяційний многочлен можна, розв'язуючи систему (8.33). Однак частіше користуються іншими методами. Основними з них є такі.

I. *Метод Лагранжа* ("компонування із заготовок" або "метод дитячого конструктора").

У цьому методі ми спочатку робимо "заготовки", тобто для кожного k $(0 \leq k \leq n)$ будуємо такий многочлен $f_k(x)$, який в усіх точках множини $\{x_0, x_1, x_2, \ldots, x_n\}$, крім точки x_k, набуває значення 0, а в точці x_k він дорівнює 1. Очевидно, що першу умову задовольняє кожний многочлен вигляду

$$g(x) = a(x - x_0)(x - x_1) \cdots (x - x_{k-1})(x - x_{k+1}) \cdots (x - x_n)\,.$$

Знайшовши числовий множник a з умови $g(x_k) = 1$, остаточно одержуємо

$$f_k(x) = \frac{(x - x_0)(x - x_1) \cdots (x - x_{k-1})(x - x_{k+1}) \cdots (x - x_n)}{(x_k - x_0)(x_k - x_1) \cdots (x_k - x_{k-1})(x_k - x_{k+1}) \cdots (x_k - x_n)}\,.$$

Інтерполяційний многочлен тепер будуємо дуже легко:

$$f(x) = b_0 f_0(x) + b_1 f_1(x) + b_2 f_2(x) + \cdots + b_n f_n(x)\,. \tag{8.34}$$

II. *Метод Ньютона* (метод послідовного уточнення).

У цьому випадку інтерполяційний многочлен шукаємо у вигляді

$$f(x) = c_0 + c_1(x - x_0) + \ldots + c_k(x - x_0)(x - x_1) \cdots (x - x_{k-1}) + \ldots$$

$$\ldots + c_n(x - x_0)(x - x_1)\cdots(x - x_{n-1})\,.$$

Суму $g_k(x) = c_0 + c_1(x - x_0) + \ldots + c_k(x - x_0)(x - x_1)\cdots(x - x_{k-1})$ будемо називати k-м наближенням многочлена $f(x)$. Коефіцієнти $c_0, c_1, \ldots, c_n$ вибиратимемо таким чином, щоб наближення $g_k(x)$ набувало значень $b_0, b_1, b_2, \ldots, b_k$ у точках $x_0, x_1, x_2, \ldots, x_k$ відповідно.

Очевидно, що $c_0 = b_0$. Наступні коефіцієнти знаходимо послідовно. Позаяк

$$g_k(x) = g_{k-1}(x) + c_k(x - x_0)(x - x_1)\cdots(x - x_{k-1})$$

і "доважок" $c_k(x - x_0)(x - x_1)\cdots(x - x_{k-1})$ не змінює значень многочлена $g_{k-1}(x)$ у точках $x_0, x_1, x_2, \ldots, x_{k-1}$, то коефіцієнт c_k знаходимо з умови

$$b_k = g_k(x_k) = g_{k-1}(x_k) + c_k(x_k - x_0)(x_k - x_1)\cdots(x_k - x_{k-1})\,.$$

Отже,

$$c_k = \frac{b_k - g_{k-1}(x_k)}{(x_k - x_0)(x_k - x_1)\cdots(x_k - x_{k-1})}\,.$$

Кожен із цих методів має свої переваги і недоліки. Метод Лагранжа вимагає громіздких обчислень на стадії "виробництва заготовок". Однак ці зусилля виправдані, якщо набір точок $x_0, x_1, x_2, \ldots, x_n$ фіксований і потрібно будувати багато інтерполяційних многочленів для різних наборів значень $b_0, b_1, b_2, \ldots, b_n$ (наприклад, коли проводиться серія дослідів, в яких вимірювання одного параметра виконуються при фіксованих значеннях $x_0, x_1, x_2, \ldots, x_n$ іншого; інша подібна ситуація наведена трохи нижче в описі алгоритму Кронекера). У методі Ньютона при заміні одного набору значень $b_0, b_1, b_2, \ldots, b_n$ іншим ми повинні всі обчислення робити заново.

Протилежна ситуація виникає, коли ми хочемо "покращити" наш інтерполяційний многочлен, розширюючи набір точок, в яких він повинен набувати заданих значень. Якщо додається нова точка x_{n+1}, в якій значення многочлена має дорівнювати b_{n+1}, то в методі Ньютона потрібно обчислити лише черговий "доважок" $c_{n+1}(x - x_0)(x - x_1)\cdots(x - x_n)$. У той же час метод Лагранжа вимагає перерахунку всіх "заготовок" заново.

Інтерполяційні многочлени використовуються в *алгоритмі Кронекера* розкладу на множники многочленів із цілими коефіцієнтами. Цей алгоритм ґрунтується на простому зауваженні, що для кожного цілого числа m будуть правильними такі імплікації:

$$f(x) = g(x)h(x) \;\Rightarrow\; f(m) = g(m)h(m) \;\Rightarrow\; g(m)|f(m)\,.$$

Нехай степінь многочлена $f(x)$ дорівнює $2k$ або $2k+1$. Якщо многочлен є звідним, то він має дільник $g(x)$, степінь якого не перевищує k. Виберемо довільні цілі точки $x_0, x_1, \ldots, x_k$ (наприклад, $0, 1, \ldots, k$). Тоді $g(x_0)|f(x_0), \ldots, g(x_k)|f(x_k)$. Для побудови дільника $g(x)$ послідовно перебираємо всі можливі набори $d_0, d_1, \ldots, d_k$, де $d_0|f(x_0), \ldots, d_k|f(x_k)$. Таких наборів скінченна кількість. Для кожного набору будуємо інтерполяційний многочлен $g(x)$, який у точках $x_0, x_1, \ldots, x_k$ набуває відповідно значень $d_0, d_1, \ldots, d_k$, і перевіряємо умови:

$$g(x) \in \mathbb{Z}[x] \quad \text{і} \quad g(x)|f(x)\,.$$

Зрозуміло, що або на певному кроці ми натрапимо на многочлен $g(x)$, який задовольняє ці умови (і тоді матимемо цілочисловий дільник многочлена $f(x)$), або $f(x)$ є незвідним над $\mathbb{Z}$.

8.6. Локалізація коренів

Для практичного знаходження коренів многочлена $f(x)$ бажано знати хоча б їх кількість. Крім того, важливо *локалізувати* корені, тобто обмежити кожен корінь певною областю, причому ці області не повинні перетинатися. У задачі локалізації коренів ми обмежимося лише многочленами з дійсними коефіцієнтами (для многочленів із комплексними коефіцієнтами ця задача є значно складнішою).

Якщо для дійсного многочлена $f(x)$ відомо, що даний інтервал (a, b) містить рівно один його корінь c і цей корінь є простим, то існує багато різних ефективних способів наближеного обчислення c. Найпримітивніший із них базується на тому, що при переході через такий корінь c многочлен міняє знак, а тому на кінцях інтервалу $f(x)$ набуває значень різних знаків. Тому можна інтервал поділити навпіл і з'ясувати, в яку з половинок потрапляє корінь. Потім знову інтервал із коренем поділити навпіл і т. д.

Але такий метод не спрацьовує, якщо c, наприклад, є коренем кратності 2, бо в цьому випадку $f(x)$ при переході через точку c знаку не змінює. Тому для локалізації коренів насамперед треба позбутися кратних коренів.

Твердження 65. *Нехай $f(x) \in \mathbb{R}[x]$. Тоді многочлен $g(x) = \dfrac{f(x)}{(f(x), f'(x))}$ взаємно простий зі своєю похідною і має ті самі дійсні корені, що й $f(x)$, причому всі корені $g(x)$ є простими.*

Доведення. Нехай многочлен $f(x)$ має канонічний розклад

$$f(x) = a(x - c_1)^{r_1} \cdots (x - c_k)^{r_k} p_1^{k_1}(x) \cdots p_m^{k_m}(x),$$

де $p_1(x), \ldots, p_m(x)$ — попарно неасоційовані квадратні тричлени з від'ємним дискримінантом. Тоді $c_1, \ldots, c_k$ — це всі попарно різні дійсні корені многочлена $f(x)$. За наслідком 39.г

$$g(x) = \frac{f(x)}{(f(x), f'(x))} = (x - c_1) \cdots (x - c_k) p_1(x) \cdots p_m(x).$$

Отже, многочлен $g(x)$ має ті самі дійсні корені, що й $f(x)$, тільки тепер вони стали простими. Крім того, із наслідку 39 випливає, що $g(x)$ взаємно простий зі своєю похідною. □

Наступне твердження дозволяє просто (хоча й доволі грубо) оцінити межі, в яких лежать корені многочлена.

Твердження 66. *Якщо многочлен* $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ *має корінь* a, *то*

$$|a| \leq 1 + \max_{1 \leq i \leq n} |a_i| . \tag{8.35}$$

Доведення. Нехай $A = \max\limits_{1 \leq i \leq n} |a_i|$. Припустимо, що $a > 1 + A$. Тоді

$$f(a) \geq a^n - A(a^{n-1} + \ldots + 1) = a^n - A\frac{a^n - 1}{a - 1} >$$
$$> a^n - A\frac{a^n - 1}{A} = a^n - (a^n - 1) = 1 .$$

Отже, припущення хибне.

Щоб довести нерівність (8.35) для від'ємних коренів, треба розглянути $f(-x)$. □

Задачу знаходження точної кількості коренів многочлена $f(x)$ на даному проміжку (a, b) уперше розв'язав у 1829 році Штурм. Для формулювання його результату нам буде потрібно кілька нових понять.

Нехай $S = (c_1, c_2, \ldots, c_m)$ — набір дійсних ненульових чисел. Кількість Zm таких індексів i, $1 \leq i < m$, що $c_i c_{i+1} < 0$ (тобто числа c_i і c_{i+1} мають протилежні знаки), називається *числом змін знаку* в наборі S. Це поняття переноситься і на довільні набори дійсних чисел: якщо набір S містить нулі, то під числом змін знаку в S розуміється число змін знаку

в укороченому наборі S', який одержується із S викреслюванням нулів. Наприклад, число змін знаку в наборі $(3, -1, 0, -2, 1, 3, 0, -1, -2, 3)$ дорівнює 4.

Рядом Штурма для многочлена $f(x)$ без кратних коренів називається набір многочленів

$$f_0(x) = f(x), \quad f_1(x), \quad \ldots, \quad f_k(x)\,, \tag{8.36}$$

який задовольняє умови:

(1) многочлен $f_k(x)$ не має дійсних коренів;

(2) при переході через корінь многочлена $f(x)$ добуток $f(x)f_1(x)$ змінює знак із „−“ на „+“;

(3) якщо $f_i(a) = 0$ для деякого i, $0 < i < k$, то $f_{i-1}(a)f_{i+1}(a) < 0$.

Причому з умови (3) випливає, що сусідні многочлени ряду (8.36) не мають спільних коренів.

Для ряду Штурма (8.36) і для кожного дійсного числа c через $\mathrm{Zm}(c)$ позначимо число змін знаку в наборі $(f_0(c), f_1(c), \ldots, f_k(c))$. Як випливає з теореми 58, функція $\mathrm{Zm}(x)$ є своєрідним “лічильником коренів” многочлена $f(x)$.

Теорема 58 (Штурм). *Нехай многочлен $f(x) \in \mathbb{R}[x]$ взаємно простий зі своєю похідною і для нього існує ряд Штурма* (8.36). *Якщо $a < b$ і $f(a) \neq 0 \neq f(b)$, то число коренів многочлена $f(x)$ на інтервалі (a, b) дорівнює $\mathrm{Zm}(a) - \mathrm{Zm}(b)$.*

Доведення. Якщо многочлен $g(x)$ не має на інтервалі (a, b) коренів, то він зберігає на цьому інтервалі знак. Отже, функція $\mathrm{Zm}(x)$ може змінюватися лише при переході через корінь якогось $f_m(x)$. Лишилося з’ясувати, як змінюється $\mathrm{Zm}(x)$ при переході через корінь многочлена $f_0(x) = f(x)$ і при переході через корінь $f_i(x)$, $i > 0$.

а) Нехай c – корінь многочлена $f(x)$. Оскільки $f(x)$ і $f_1(x)$ не мають спільних коренів, то в деякому околі точки c многочлен $f_1(x)$ зберігає знак. Але при переході через c добуток $f(x)f_1(x)$ змінює знак із „−“ на „+“. Отже, зліва від c числа $f(x)$ і $f_1(x)$ були різних знаків, а справа від c – одного. Тому в послідовності $f(x)$, $f_1(x)$ число змін знаку зменшується на 1.

б) Нехай c – корінь многочлена $f_i(x)$, $i > 0$. У деякому околі точки c многочлени $f_{i-1}(x)$ і $f_{i+1}(x)$ зберігають знак. Крім того, числа $f_{i-1}(c)$ і $f_{i+1}(c)$ мають протилежні знаки. Тому по обидва боки від точки c фрагмент $f_{i-1}(x)$, $f_i(x)$, $f_{i+1}(x)$ послідовності ряду Штурма має або знаки

$+, \varepsilon, -$, або знаки $-, \varepsilon, +$, де ε – знак числа $f_i(x)$. В обох випадках цей фрагмент містить рівно одну зміну знаку, а число змін знаку при переході через точку c не змінюється.

Таким чином, функція $\mathrm{Zm}(x)$ змінюється лише при переході через корінь многочлена $f(x)$, причому кожного разу зменшується на 1. □

Насправді для теореми Штурма, як видно з доведення, виконання умов (1)–(3) для ряду Штурма досить вимагати лише на проміжку $[a, b]$. Якщо ці умови виконуються на всій числові осі, то загальна кількість дійсних коренів многочлена $f(x)$ дорівнює $\mathrm{Zm}(-\infty) - \mathrm{Zm}(\infty)$.

Зрозуміло, що теорема Штурма може бути корисною лише в тому разі, якщо ми навчимося будувати ряд Штурма. Один зі способів побудови такого ряду виглядає так: покладемо $f_0(x) = f(x)$, $f_1(x) = f'(x)$, а далі для $i > 0$ члени ряду визначаємо рекурентно:

$$f_{i-1}(x) = q_i(x)f_i(x) - f_{i+1}(x). \tag{8.37}$$

Позаяк $f(x)$ і $f'(x)$ взаємно прості, то на якомусь кроці одержимо $f_k(x) = a \neq 0$.

Перевіримо виконання умов (1)–(3) з означення ряду Штурма.

(1) Виконання цієї умови є очевидним

(2) Якщо при переході через корінь x_0 многочлен $f(x)$ змінює знак із „+“ на „−“, то $f'(x_0) < 0$; якщо ж він змінює знак із „−“ на „+“, то $f'(x_0) > 0$. В обох випадках добуток $f(x)f'(x)$ змінює знак із „−“ на „+“.

(3) Якщо $f_i(x_0) = 0$, то із (8.37) випливає, що $f_{i-1}(x_0) = -f_{i+1}(x_0)$. Тому $f_{i-1}(x_0)f_{i+1}(x_0) = -f_{i+1}^2(x_0)$. Якщо $f_{i+1}(x_0) = 0$, то із правила побудови ряду випливає, що $f_{i+2}(x_0) = f_{i+3}(x_0) = \cdots = f_k(x_0) = 0$. Але остання рівність суперечить тому, що $f_k(x) = a \neq 0$. Отже, $f_{i+1}(x_0) \neq 0$ і $f_{i-1}(x_0)f_{i+1}(x_0) < 0$.

Приклад 22. Розглянемо дійсний многочлен $f(x) = x^3 + px + q$ степеня 3. Його ряд Штурма має вигляд

$$f_0(x) = f(x), \quad f_1(x) = f'(x) = 3x^2 + p,$$
$$f_3(x) = -4p^3 - 27q^2, \quad f_3(x) = -4p^3 - 27q^2.$$

Число $f_3 = -4p^3 - 27q^2$ називається **дискримінантом** многочлена $f(x)$ і позначається $D(f)$. Із побудови ряду Штурма для $f(x)$ й алгоритму Евкліда випливає, що $f(x)$ має кратні корені тоді й лише тоді, коли $D(f) = 0$.

Нехай тепер $D(f) \neq 0$. Тоді $f(x)$ має або один дійсний корінь, або три. Розглянемо таблицю знаків для ряду Штурма:

	f_0	f_1	f_2	f_3
$-\infty$	$-$	$+$	$\operatorname{sign} p$	$\operatorname{sign} D(f)$
∞	$+$	$+$	$-\operatorname{sign} p$	$\operatorname{sign} D(f)$

.

Зауважимо, що, коли $D(f) > 0$, то $p < 0$. Із таблиці знаків тепер легко бачити, що при $D(f) < 0$ многочлен $f(x)$ має один дійсний корінь, а при $D(f) > 0$ — три.

Перед наступним прикладом зробимо одне зауваження, яке трохи полегшує обчислення: якщо члени ряду Штурма (8.36) помножити на довільні додатні числа, то він залишиться рядом Штурма.

Приклад 23. Локалізуємо корені многочлена $f(x) = x^4 - 12x^2 - 16x - 4$.

Покладемо $f_0(x) = f(x)$. Оскільки $f'(x) = 4x^3 - 24x - 16$, то можна взяти $f_1(x) = x^3 - 6x - 4$. Щоб знайти $f_2(x)$, ділимо $f_0(x)$ на $f_1(x)$ з остачею:

$$f_0(x) = x \cdot f_1(x) - 6x^2 - 12x - 4.$$

Міняємо в остачі знак і ділимо на 2: $f_2(x) = 3x^2 + 6x + 2$. Далі шукаємо $f_3(x)$:

$$f_1(x) = \left(\frac{1}{3}x - \frac{2}{3}\right) \cdot f_2(x) - \frac{8}{3}x - \frac{8}{3}.$$

Міняємо в остачі знак і множимо на $3/8$: $f_3(x) = x + 1$. Нарешті, з рівності $f_2(x) = (3x + 3) \cdot f_3(x) - 1$ випливає, що $f_4(x) = 1$. Таким чином, ряд Штурма для $f(x)$ має вигляд

$$f_0 = x^4 - 12x^2 - 16x - 4, \quad f_1(x) = x^3 - 6x - 4,$$
$$f_2(x) = 3x^2 + 6x + 2, \quad f_3(x) = x + 1, \quad f_4(x) = 1.$$

Складаємо таблицю знаків для ряду Штурма:

x	f_0	f_1	f_2	f_3	f_4	$\operatorname{Zm}(x)$
$-\infty$	$+$	$-$	$+$	$-$	$+$	4
∞	$+$	$+$	$+$	$+$	$+$	0
0	$-$	$-$	$+$	$+$	$+$	1
-2	$-$	0	$+$	$-$	$+$	3
-1	$+$	$+$	$-$	0	$+$	2

.

Таким чином, многочлен має $\mathrm{Zm}(-\infty) - \mathrm{Zm}(\infty) = 4$ дійсні корені, з яких $\mathrm{Zm}(-\infty) - \mathrm{Zm}(0) = 3$ будуть від'ємними і $\mathrm{Zm}(0) - \mathrm{Zm}(\infty) = 1$ – додатним. Оскільки $\mathrm{Zm}(-\infty) - \mathrm{Zm}(-2) = \mathrm{Zm}(-2) - \mathrm{Zm}(-1) = \mathrm{Zm}(-1) - \mathrm{Zm}(0) = 1$, то від'ємні корені локалізовані в інтервалах $(-\infty, -2)$, $(-2, -1)$ і $(-1, 0)$ відповідно. Враховуючи твердження 66, перший із від'ємних коренів можемо локалізувати в інтервалі $(-17, -2)$, а додатний корінь – в інтервалі $(0, 17)$.

8.7. Раціональні дроби

Описана на початку розділу 1 конструкція, за допомогою якої з кільця $\mathbb{Z}$ цілих чисел будується поле $\mathbb{Q}$ раціональних чисел, насправді узагальнюється на дуже широкий клас кілець. Детально вона буде вивчатися пізніше, а зараз ми розглянемо, як ця конструкція працює у випадку кільця многочленів.

Нехай $P[x]$ – кільце многочленів із коефіцієнтами з поля P. Розглянемо множину $R = P[x]\times(P[x]\setminus\{0\})$, елементами якої є впорядковані пари вигляду $(f(x), g(x))$, де многочлен $f(x)$ – довільний, а $g(x)$ – ненульовий. Пару $(f(x), g(x))$ будемо записувати у вигляді $\dfrac{f(x)}{g(x)}$ і називати *раціональним дробом* із *чисельником* $f(x)$ та *знаменником* $g(x)$. На множині R раціональних дробів визначимо відношення:

$$\frac{f(x)}{g(x)} \sim \frac{p(x)}{q(x)} \quad \text{тоді й лише тоді, коли} \quad f(x)g(x) = n(x)p(x).$$

Вправа 27. *Перевірте, що відношення $\sim$ є відношенням еквівалентності.*

Фактор-множина $P(x) = R/\!\sim$ називається множиною *раціональних функцій* із коефіцієнтами з поля P, а її елементи (тобто класи еквівалентності раціональних дробів) — *раціональними функціями*.

Клас еквівалентності раціональних дробів (тобто раціональну функцію), який містить дріб $\dfrac{f(x)}{g(x)}$, будемо позначати $\left[\dfrac{f(x)}{g(x)}\right]$ (згодом, коли з контексту буде зрозуміло, чи йдеться про дріб, чи про відповідну раціональну функцію, квадратні дужки ми опускатимемо).

Додавання і множення раціональних функцій визначимо такими

правилами:

$$\left[\frac{f_1(x)}{g_1(x)}\right] + \left[\frac{f_2(x)}{g_2(x)}\right] := \left[\frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)}\right], \tag{8.38}$$

$$\left[\frac{f_1(x)}{g_1(x)}\right] \cdot \left[\frac{f_2(x)}{g_2(x)}\right] := \left[\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}\right]. \tag{8.39}$$

Теорема 59. *Множина $P(x)$ раціональних функцій відносно дій, визначених правилами* (8.38) *і* (8.39)*, утворює поле.*

Доведення. Спочатку переконаємося, що дії у множині $P(x)$ визначено коректно, тобто, що результат не залежить від вибору конкретних представників із класів еквівалентності. Справді, нехай

$$\frac{f_1(x)}{g_1(x)} \sim \frac{f_1^*(x)}{g_1^*(x)}, \quad \frac{f_2(x)}{g_2(x)} \sim \frac{f_2^*(x)}{g_2^*(x)}.$$

Тоді $f_1(x)g_1^*(x) = f_1^*(x)g_1(x)$ і $f_2(x)g_2^*(x) = f_2^*(x)g_2(x)$. Із цих рівностей випливає, що

$$\begin{gathered}\big(f_1(x)g_2(x) + f_2(x)g_1(x)\big)g_1^*(x)g_2^*(x) = \\ = f_1(x)g_2(x)g_1^*(x)g_2^*(x) + f_2(x)g_1(x)g_1^*(x)g_2^*(x) = \\ = f_1^*(x)g_2(x)g_1(x)g_2^*(x) + f_2^*(x)g_1(x)g_1^*(x)g_2(x) = \\ = \big(f_1^*(x)g_2^*(x) + f_2^*(x)g_1^*(x)\big)g_1(x)g_2(x).\end{gathered}$$

Отже,

$$\frac{f_1(x)g_2(x) + f_2(x)g_1(x)}{g_1(x)g_2(x)} = \frac{f_1^*(x)g_2^*(x) + f_2^*(x)g_1^*(x)}{g_1^*(x)g_2^*(x)}.$$

Коректність правила для множення перевіряється аналогічно.

Легко переконатися, що нейтральним елементом для додавання – нулем – буде раціональна функція $\left[\frac{0}{g(x)}\right]$; нейтральним елементом для множення – одиницею – раціональна функція $\left[\frac{g(x)}{g(x)}\right]$; протилежною до функції $\left[\frac{f(x)}{g(x)}\right]$ – функція $\left[\frac{-f(x)}{g(x)}\right]$, а оберненою до ненульової функції $\left[\frac{f(x)}{g(x)}\right]$ – функція $\left[\frac{g(x)}{f(x)}\right]$. Решта аксіом поля перевіряється прямим обчисленням. □

Якщо многочлен $f(x)$ ототожнити з раціональною функцією $\dfrac{f(x)}{1}$, то одержимо занурення $P[x] \hookrightarrow P(x)$.

Раціональний дріб $\dfrac{f(x)}{g(x)}$ називається *правильним*, якщо $45f(x) < 45g(x)$. Із правил (8.38) і (8.39) випливає, що сума і добуток правильних дробів також є правильними дробами[18].

Теорема 60. *Кожен раціональний дріб* $r(x)$ *розкладається в суму*

$$r(x) = p(x) + \frac{u(x)}{v(x)}$$

многочлена і правильного дробу, причому єдиним чином.

Доведення. Нехай $r(x) = \dfrac{f(x)}{g(x)}$. Поділимо чисельник на знаменник з остачею:

$$f(x) = q(x)g(x) + r(x) \quad \text{і} \quad r(x) = 0 \ \text{ або } \ 45r(x) < 45g(x).$$

Тоді

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

причому дріб $\dfrac{r(x)}{g(x)}$ є правильним.

Нехай тепер

$$r(x) = p(x) + \frac{u(x)}{v(x)} = q(x) + \frac{r(x)}{g(x)}$$

– два різні розклади дробу $r(x)$. Тоді

$$p(x) - q(x) = \frac{r(x)}{g(x)} - \frac{u(x)}{v(x)},$$

причому зліва стоїть многочлен, а справа — правильний дріб. Оскільки многочлен не може дорівнювати правильному дробу, то припущення про існування двох різних розкладів є хибним. □

[18] Зауважимо, що для правильних дробів із $\mathbb{Q}$ лише добуток завжди буде правильним дробом.

Раціональний дріб $\dfrac{f(x)}{g(x)}$ називається *елементарним* або *найпростішим*, якщо знаменник $g(x)$ є степенем деякого незвідного многочлена $p(x)$ і $45f(x) < 45p(x)$.

Теорема 61. *Кожен правильний дріб можна подати у вигляді суми елементарних дробів.*

Нам знадобляться дві леми.

Лема 15. *Нехай правильний дріб має вигляд* $\dfrac{f(x)}{g_1(x)g_2(x)\dots g_k(x)}$, *де многочлени* $g_1(x)$, $g_2(x)$, $\cdots$, $g_k(x)$ *попарно взаємно прості. Тоді його можна розкласти в суму правильних дробів зі знаменниками* $g_1(x), g_2(x), \dots, g_k(x)$.

Доведення. Будемо доводити це індукцією за кількістю k взаємно простих множників. Нехай $k = 2$. За критерієм взаємної простоти многочленів (твердження 53) існують такі многочлени u_1 і u_2, що

$$u_1(x)g_1(x) + u_2(x)g_2(x) = 1.$$

Тоді

$$\frac{f(x)}{g_1(x)g_2(x)} = \frac{f(x)(u_1(x)g_1(x) + u_2(x)g_2(x))}{g_1(x)g_2(x)} = \frac{f(x)u_1(x)}{g_2(x)} + \frac{f(x)u_2(x)}{g_1(x)}.$$

Запишемо кожен із доданків із правої частини у вигляді суми многочлена і правильного дробу:

$$\frac{f(x)u_1(x)}{g_2(x)} = p_1(x) + \frac{q_1(x)}{g_2(x)}, \qquad \frac{f(x)u_2(x)}{g_1(x)} = p_2(x) + \frac{q_2(x)}{g_1(x)}.$$

Тоді

$$\frac{f(x)}{g_1(x)g_2(x)} = (p_1(x) + p_2(x)) + \frac{q_1(x)}{g_2(x)} + \frac{q_2(x)}{g_1(x)}. \tag{8.40}$$

Сума $p_1(x) + p_2(x)$ многочленів має бути правильним дробом, тому $p_1(x) + p_2(x) = 0$ і у правій частині рівності (8.40) лишаються лише правильні дроби з потрібними знаменниками.

Нехай тепер $k > 2$. Множники $g_1(x)\cdots g_{k-1}(x)$ і $g_k(x)$ є взаємно простими. Тому за доведеним вище дріб $\dfrac{f(x)}{g_1(x)g_2(x)\cdots g_k(x)}$ розкладається в суму правильних дробів зі знаменниками $g_1(x)\cdots g_{k-1}(x)$ і $g_k(x)$. У свою чергу за припущенням індукції правильний дріб зі знаменником

$g_1(x)\cdots g_{k-1}(x)$ розкладається в суму правильних дробів зі знаменниками $g_1(x)$, …, $g_{k-1}(x)$. Тому $\dfrac{f(x)}{g_1(x)g_2(x)\cdots g_k(x)}$ розкладається в суму правильних дробів зі знаменниками $g_1(x)$, $g_2(x)$, …, $g_k(x)$. □

Лема 16. *Кожен правильний дріб вигляду* $\dfrac{f(x)}{p^k(x)}$, *де* $p(x)$ *– незвідний многочлен, розкладається в суму елементарних.*

Доведення. Доведемо це індукцією за показником k. Твердження тривіальне, якщо $k = 1$. Нехай тепер $k > 1$. Поділимо $f(x)$ на $p(x)$ з остачею:

$$f(x) = q(x)p(x) + r(x).$$

Тоді

$$\frac{f(x)}{p^k(x)} = \frac{q(x)p(x) + r(x)}{p^k(x)} = \frac{q(x)}{p^{k-1}(x)} + \frac{r(x)}{p^k(x)}. \tag{8.41}$$

У правій частині рівності (8.41) обидва доданки є правильними дробами, причому другий доданок є навіть елементарним дробом. За припущенням індукції перший доданок також розкладається в суму елементарних дробів. □

Доведення теореми 61. Нехай $t(x) = \dfrac{f(x)}{g(x)}$ – правильний дріб і $g(x) = p_1^{m_1}(x)p_2^{m_2}(x)\cdots p_k^{m_k}(x)$ – канонічний розклад знаменника. За лемою 15 $t(x)$ можна розкласти в суму правильних дробів зі знаменниками $p_1^{m_1}(x)$, $p_2^{m_2}(x)$, …, $p_k^{m_k}(x)$, а за лемою 16 кожен правильний дріб зі знаменником $p_i^{m_i}(x)$ можна розкласти в суму елементарних дробів. □

Наслідок 42. *а) Над полем* $\mathbb{C}$ *кожен раціональний дріб розкладається в суму дробів вигляду* $\dfrac{a}{(x-c)^k}$.

б) Над полем $\mathbb{R}$ *кожен раціональний дріб розкладається в суму дробів вигляду* $\dfrac{a}{(x-c)^k}$ *або* $\dfrac{ax+b}{(x^2+px+q)^k}$, *де квадратний тричлен* x^2+px+q *має від'ємний дискримінант.*

Доведення. Над полем $\mathbb{C}$ незвідними є лише лінійні многочлени, а над $\mathbb{R}$ – лінійні і квадратні з від'ємним дискримінантом. □

Теорема 61 використовується в математичному аналізі при інтегруванні раціональних функцій.

Доведення теореми 61 є конструктивним і дає алгоритм розкладу дробу в суму елементарних. Однак із практичного погляду зручнішим є *метод невизначених коефіцієнтів*. Суть цього методу буде зрозумілою з прикладу 24.

Приклад 24. Розкладемо в суму елементарних дробів над полем $\mathbb{R}$ раціональний дріб $\dfrac{1}{x^3(x^2+1)^2}$.

На підставі наслідку 42 цей дріб можна записати у вигляді

$$\frac{1}{x^3(x^2+1)^2} = \frac{a}{x} + \frac{b}{x^2} + \frac{c}{x^3} + \frac{d+ex}{x^2+1} + \frac{f+gx}{(x^2+1)^2},$$

де a, b, c, d, e, f, g – якісь дійсні числа. Помножимо обидві частини цієї рівності на $x^3(x^2+1)^2$:

$$1 = ax^2(x^2+1)^2 + bx(x^2+1)^2 + c(x^2+1)^2 +$$
$$+(d+ex)x^3(x^2+1) + (f+gx)x^3. \tag{8.42}$$

Спочатку підставляємо в це рівняння корені знаменника. Підставляючи $x = 0$, знаходимо $c = 1$. Підставляючи $x = i$, одержуємо $1 = (f + gi)i^3$, звідки $g = 1$, $f = 0$. Щоб знайти решту коефіцієнтів a, b, d, e, підставляємо в рівняння (8.42) послідовно $x = 1$, $x = -1$, $x = 2$, $x = -2$. Одержуємо систему лінійних рівнянь

$$\begin{array}{rcrcrcrcr} 4a & + & 4b & + & 2d & + & 2e & = & -4\,, \\ 4a & - & 4b & - & 2d & + & 2e & = & -4\,, \\ 100a & + & 50b & + & 40d & + & 80e & = & -40\,, \\ 100a & - & 50b & - & 40d & + & 80e & = & -40\,. \end{array} \tag{8.43}$$

Розв'язуючи цю систему, знаходимо: $a = -2$, $b = d = 0$, $e = 2$. Отже, шуканий розклад має вигляд

$$\frac{1}{x^3(x^2+1)^2} = \frac{-2}{x} + \frac{1}{x^3} + \frac{2x}{x^2+1} + \frac{x}{(x^2+1)^2}.$$

8.8. Задачі

8.1. Нехай P – поле. З'ясуйте, чи для довільних многочлена $g(x) \in P[x]$ і степеневого ряду $f(x) \in P[[x]]$ існують такі многочлен $r(x) \in P[x]$ і степеневий ряд $h(x) \in P[[x]]$, що $f(x) = h(x)g(x) + r(x)$ і або $r(x) = 0$, або $45r(x) < 45g(x)$.

8.2. Доведіть, що, коли многочлен $f(x^n)$ ділиться на $x-1$, то він ділиться і на $x^n - 1$.

8.3.° Доведіть, що для кожного многочлена $f(x)$ із коефіцієнтами з поля P існує такий многочлен $h(x,y) \in P[x,y]$, що $f(x+y) = f(x) + yf'(x) + y^2h(x,y)$.

8.4. Для рекурентного співвідношення

$$f_{n+k} = a_0f_n + a_1f_{n+1} + \ldots + a_{k-1}f_{n+k-1},\ k \neq 0,\ a_0 \neq 0\ , \qquad (8.44)$$

із комплексними коефіцієнтами $a_0, a_1, \ldots, a_{k-1}$ запишемо многочлен $f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_0$. Доведіть, що

а)* послідовність $f_n = n^r a^n$, $r \geq 0$, $a \neq 0$, буде задовольняти рекурентне співвідношення (8.44) тоді й лише тоді, коли a буде коренем кратності $\geq r+1$ многочлена $f(x)$;

б)** якщо $\beta_1, \ldots, \beta_m$ — усі комплексні корені многочлена $f(x)$ кратностей $s_1, \ldots, s_m$ відповідно, то кожна послідовність f_n, яка задовольняє рекурентне співвідношення (8.44), має вигляд

$$f_n = \sum_{i=1}^{m} g_i(n)\beta_i^n,$$

де $g_i(x)$ – многочлен степеня не більшого за $s_i - 1$, $i = 1, \ldots, m$.

8.5.* Доведіть, що для довільних a, b і c $(c \neq 0)$ многочлен

$$f(x) = x^5 + ax^4 + bx^3 + c \in \mathbb{R}[x]$$

не розкладається над $\mathbb{R}$ на лінійні множники.

8.6.* Нехай $f(x)$ і $g(x)$ — взаємно прості многочлени з дійсними коефіцієнтами. Доведіть, що корені многочленів $f(x)$ і $g(x)$ дійсні й розділяються тоді й лише тоді, коли для довільних дійсних чисел a і b всі корені многочлена $af(x) + bg(x)$ – дійсні.

8.7. Доведіть, що, коли всі корені многочлена $f(x) \in \mathbb{R}[x]$ є дійсними, то для довільного $a \in \mathbb{R}$ всі корені многочлена $f(x) + af'(x)$ також є дійсними.

8.8. Нехай $f(x)$ і $g(x)$ – взаємно прості многочлени з дійсними коефіцієнтами. Доведіть, що, коли всі корені многочленів $f(x)$ і $g(x)$ дійсні й попарно розділяються, то корені їх похідних також розділяються.

8.9*. Доведіть, що, коли всі корені дійсних многочленів $f(x)$ і $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ є дійсними, то всі корені многочлена $F(x) = a_n f(x) + a_{n-1}f'(x) + \cdots + a_0 f^{(n)}(x)$ також є дійсними.

8.10*. Доведіть, що для кожного многочлена $f(x) \in \mathbb{Z}[x]$ додатного степеня існує нескінченно багато таких простих чисел p, що $f(x)$ має корінь у полі $\mathbb{Z}_p$.

8.11. Розкладіть на лінійні множники многочлен $x^p - x$ із коефіцієнтами з поля $\mathbb{Z}_p$.

8.12. Доведіть *теорему Вільсона*: для кожного простого числа p виконується конгруенція $(p-1)! \equiv -1 \pmod{p}$.

8.13. Нехай $g(x) = (x - c_0)(x - c_1)\cdots(x - c_n)$, де $c_0, c_1, \ldots, c_n$ — попарно різні елементи поля P. Доведіть, що многочлен

$$f(x) = g(x) \cdot \sum_{k=0}^{n} \frac{b_k}{g'(c_k)(x - c_k)} \tag{8.45}$$

набуває в точках $c_0, c_1, \ldots, c_n$ значень $b_0, b_1, \ldots, b_n$ відповідно (формула (8.45) називається *інтерполяційною формулою Лагранжа*).

8.14. Доведіть, що для довільного многочлена $f(z) = a_0 + a_1 z + \ldots + a_n z^n$ із комплексними коефіцієнтами середнє арифметичне значень цього многочлена у вершинах довільного правильного m-кутника $(m > n)$ дорівнює значенню $f(z)$ у центрі цього m-кутника.

8.15. Розкладіть у суму елементарних дробів над полем $\mathbb{C}$ дріб $\dfrac{1}{x^n - 1}$.

8.16*. Розкладіть у суму елементарних дробів над полем $\mathbb{Z}_p$ дріб $\dfrac{1}{x^p - x}$.

8.17. *Оцінка Маклорена.* Нехай m – номер першого від'ємного коефіцієнта многочлена $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $A = \max\limits_{a_i<0} |a_i|$. Доведіть, що кожен корінь c многочлена $f(x)$ задовольняє нерівність $c \le 1 + \sqrt[m]{A}$.

8.18. *Многочлени Лежандра* $P_0(x) = 1$, $P_1(x) = x$, …, $P_n(x)$, … визначаються рекурентно:

$$nP_n(x) - (2n-1)xP_{n-1}(x) + (n-1)P_{n-2}(x) = 0\,.$$

Доведіть, що а) $P_n(1) = 1$, $P_n(-1) = -1$;

б) на відрізку $[-1, 1]$ набір $P_n(x), P_{n-1}(x), \ldots, P_0(x)$ є рядом Штурма для многочлена $P_n(x)$;

в) на проміжку $[-1, 1]$ многочлен $P_n(x)$ має n різних коренів.

8.19. Доведіть, що

а)** для $n \geq 2$ многочлен $x^n - x - 1$ є незвідним над $\mathbb{Q}$;

б) для $n \equiv 2 \pmod 3$ многочлен $x^n + x + 1$ ділиться над $\mathbb{Z}$ на $x^2 + x + 1$;

в)** для $n \not\equiv 2 \pmod 3$ многочлен $x^n + x + 1$ є незвідним над $\mathbb{Q}$.

8.20.*** Нехай многочлени $f(x)$ і $g(x)$ із $\mathbb{C}[x]$ — взаємно прості. Доведіть, що число $\max(\deg f, \deg g)$ завжди менше за кількість різних коренів многочлена $f(x)g(x)(f(x) + g(x))$.

8.21.*** Нехай $f(x)$, $g(x)$ і $h(x)$ із $\mathbb{C}[x]$ — такі попарно взаємно прості многочлени, що $f^n(x) + g^n(x) = h^n(x)$. Доведіть, що $n \leq 2$.

Відповіді та вказівки до вправ

Розділ 1. 5. Застосуйте індукцію.

Розділ 4. 11. kmn. **12.** Ні. **13.** *Вказ*. Використайте наслідок 17 про ранг добутку двох матриць. **14.** Ні.

Розділ 6. 17. Наприклад, $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Розділ 5. 15. Наприклад, $A = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$, $C = \left(\begin{smallmatrix} 0 & -2 \\ -1 & 5 \end{smallmatrix}\right)$. **16**. Оберненою до $\pi = (a_1 a_2 \dots a_k) \cdots (c_1 c_2 \dots c_m)$ є підстановка $\pi^{-1} = (a_k a_{k-1} \dots a_1) \cdots (c_m c_{m-1} \dots c_1)$.

Розділ 8. 23. $[f'(g(x))]' \cdot g'(x)$. **25.** *Вказ.* Для довільного $a \in P$ многочлен $f(x) - a$ має корінь.

Розділ 7. 20. *Вказ.* При розкритті дужок у добуткові $(x_1 + x_2 + \dots + x_k)^n$ доданок $x_1^\alpha x_2^\beta \cdots x_k^\gamma$ можна одержати $\binom{n}{\alpha}\binom{n-\alpha}{\beta}\cdots\binom{\gamma}{\gamma}$ способами.

Відповіді та вказівки до задач

Розділ 1. 1.3. *Вказ*. Нехай $z = a + bi \neq 0$. Обчислення $\sqrt{z}$ зводиться до розв'язання рівняння $(x + iy)^2 = a + bi$ з дійсними невідомими x і y, тобто до дійсної системи $x^2 - y^2 = a$, $2xy = b$. Якщо $b = 0$, то маємо $x = \pm\sqrt{a}$, $y = 0$ (при $a > 0$) або $x = 0$, $y = \pm i\sqrt{-a}$ (при $a < 0$). Якщо ж $b \neq 0$, то, виключаючи за допомогою другого рівняння y, зводимо задачу до біквадратного рівняння $4x^4 - 4ax^2 - b^2 = 0$, яке має рівно 2 дійсні розв'язки. **1.4.** *Вказ*. У цьому випадку існують такі цілі числа a і b, що $am + bn = 1$. Тому $z^1 = z^{am+bn} = 1$. **1.5.** *Вказ*. Скористайтесь розв'язанням задачі 1.4. **1.6.** *Вказ*. Досить показати, що коли $\mu_1, \mu_2 \in \mathbb{C}_m$, $\nu_1, \nu_2 \in \mathbb{C}_n$ і $\mu_1\nu_1 = \mu_2\nu_2$, то $\mu_1 = \mu_2$ і $\nu_1 = \nu_2$. Але з рівності $\mu_1\nu_1 = \mu_2\nu_2$ випливає, що $\nu_1^m = \nu_2^m$, а тому $\frac{\nu_1}{\nu_2} \in \mathbb{C}_n \cap \mathbb{C}_m$. Далі використайте задачу 1.4. **1.7.** *Вказ*. Якщо μ не є первісним коренем степеня m або ν не є первісним коренем степеня n, то добуток $\mu \cdot \nu$ не є первісним коренем степеня mn. Далі використайте задачу 1.6 і мультиплікативність функції Ойлера. **1.8**. Так. *Вказ*. Напр., для $n = 36$ корені ε_1, ε_7, ε_{13}, ε_{19}, ε_{25}, ε_{31} є первісними і кожен із них є сумою двох сусідніх. **1.9**. *Вказ*. Якщо рівність виконується, то $(2 + i)^n = (2 - i + 2i)^n = (2 - i)^n + \binom{n}{1}(2-i)^{n-1}2i + \binom{n}{2}(2-i)^{n-2}(2i)^2 + \ldots + \binom{n}{n-1}(2-i)(2i)^{n-1} + (2i)^n = (2-i)^n$, звідки $(2 - i)(A + Bi) = (2i)^n$, де A і B – цілі числа. Для квадратів модулів одержимо: $5(A^2 + B^2) = 4^n$. **1.10.** *Вказ*. Запишіть z у тригонометричній формі. **1.12.** *Вказ*. Подвійне відношення буде дійсним числом тоді й лише тоді, числа $\frac{z_1-z_2}{z_1-z_4}$ і $\frac{z_3-z_2}{z_3-z_4}$ мають однакові аргументи (з точністю до кута, кратного 2π). Але аргумент числа $\frac{z-z_2}{z-z_4}$ – це кут, під яким із точки z видно відрізок із кінцями z_2 і z_4. **1.14.** $a_n = 2^{n/2}\cos\frac{n\pi}{4}$. *Вказ*. Геометрична прогресія $b_n = cq^n$ задовольняє рекурентне співвідношення $b_{n+1} = 2b_n - 2b_{n-1}$ тоді й лише тоді, коли її знаменник q є коренем рівняння $q^2 = 2q + 2$, тобто коли $q = 1 \pm i$. Запишіть a_n у вигляді $a_n = c_1(1 + i)^n + c_2(1 - i)^n$, знайдіть з умови $a_0 = a_1 = 1$ коефіцієнти c_1 і c_2 і перейдіть до тригонометричної форми. **1.15.** *Вказ*. а) Точки z_1, z_2, z_3, z_4 є чотирма послідовними вершинами квадрата (при обході квадрата проти руху годинникової стрілки) тоді й лише тоді, коли $|z_2 - z_1| = |z_3 - z_2| = |z_4 - z_3|$, $\frac{z_3-z_2}{z_2-z_1} = \frac{z_4-z_3}{z_3-z_2} = i$. Поворот на кут φ вектора, що відповідає числу z, відповідає множенню z на число $\cos\varphi + i\sin\varphi$. **1.16.** *Вказ*. Для довільного автоморфізму $\varphi(0) = 0$, $\varphi(1) = 1$ і $\varphi(i) = \pm i$. Тому для довільних $p, q \in \mathbb{Q}$ буде $\varphi(p + qi) = p + q\varphi(i)$. Нехай тепер автоморфізм $\varphi : \mathbb{C} \to \mathbb{C}$ – неперервний і $(p_n)_{n>0}$, $(q_n)_{n>0}$ – послідовності раціональних чисел, які збігаються до p і q відповідно. Тоді $p_n + q_n i \to a + bi$ і $\varphi(p_n +$

$+ q_n i) = p_n + q_n\varphi(i) \longrightarrow a + b\varphi(i) = \varphi(a + bi)$. **1.17.** $(a^2 + b^2 + c^2 + d^2)(k^2 + + l^2 + m^2 + n^2) = (ak - bl - cm - dn)^2 + (al + bk + cn - dm)^2 + (am - bn + + ck + dl)^2 + (an + bm - cl + dk)^2$.

Розділ 2. 2.1. $x = \frac{1}{3}(a+b+c), y = \frac{1}{3}(a-b+\varepsilon(c-b)), z = \frac{1}{3}(a-c+\varepsilon(b-c))$. *Вказ.* Покажіть, що $\varepsilon^2 + \varepsilon + 1 = 0$. **2.2.** *Вказ.* Позначимо через $\|X\|$ максимум модулів компонент стовпця X, а через q – максимум сум модулів елементів рядків матриці $E + A$. Тоді $0 \leq q < 1$. Доведіть, що для довільних натуральних чисел m і k виконується нерівність $\|X_{m+1} - X_{k+1}\| \leq q\|X_m - X_k\|$. **2.3.** *Вказ.* Перестановкою стовпців та рядків можна зробити так, щоб елемент a_{11} став найменшим за модулем серед ненульових елементів. Далі, віднімаючи від усіх рядків (стовпців) відповідні кратні першого рядка (стовпця), можна замінити всі відмінні від a_{11} елементи першого рядка і першого стовпця їх остачами від ділення на a_{11}. Якщо серед цих остач є ненульові, то найменшу з них ставимо на місце a_{11} і повторюємо процес. Урешті-решт отримаємо матрицю, в якій усі елементи першого рядка і першого стовпця, крім a_{11}, дорівнюють нулю. Далі застосуйте індукцію.

Розділ 3. 3.1. б) Так. **3.2**. *Вказ.* Так, якщо $n \leq 2$; не обов'язково, якщо $n > 2$. **3.3**. *Вказ.* Застосуйте теореми Кронекера – Капеллі. **3.4.** *Вказ.* Із теореми Кронекера – Капеллі про сумісність випливає, що СЛР буде сумісною для кожного стовпця $\boldsymbol{b}$ вільних членів тоді й лише тоді, коли рядки її основної матриці лінійно незалежні. У противному разі її рядки є лінійно залежними. Але тоді лінійно залежними будуть і стовпці. Тому, за теоремою Кронекера – Капеллі про визначеність, відповідна однорідна СЛР буде невизначеною. **3.5**. Матриці $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}$ та $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$ мають однаковий ранг. *Вказ.* Застосуйте теорему Кронекера – Капеллі. **3.6**. *Вказ. Необхідність*. Якщо M_1, M_2, M_3, M_4 лежать на одній прямій, то існують такі k і b, що $y_i = kx_i + b$ $(i = 1, 2, 3, 4)$. Легко перевіряється, що відповідні рівняння – лінійно залежні. *Достатність*. Нехай п'яте рівняння є лінійною комбінацією решти рівнянь. Тоді кожна крива другого порядку, що проходить через M_1, M_2, M_3, M_4, проходить і через M_5. Зокрема, кожна пара прямих M_1, M_2, M_3, M_4 і M_1, M_2, M_3, M_4 містить точку M_5. Це можливо лише тоді, коли принаймні дві із цих чотирьох прямих збігаються, тобто, коли три з точок M_1, M_2, M_3, M_4 лежать на одній прямій. Але тоді й точка M_5 лежить на цій прямій.

Розділ 4. 4.1. $[\varphi_\alpha] = \left(\begin{smallmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{smallmatrix}\right)$; $[\varphi_\alpha] \cdot [\varphi_\beta] = [\varphi_{\alpha+\beta}]$. **13.** *Вказ.* а) Нехай $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ – база підпростору $V \subseteq P^n$, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k, \ldots, \boldsymbol{v}_n$ – її поповнення до бази P^n, $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m$ – база P^m. Розгляньте лінійне відображення $\varphi : P^n \longrightarrow P^m$, при якому $\varphi(\boldsymbol{v}_i) = \boldsymbol{0}$ $(i = 1, \ldots, k)$, $\varphi(\boldsymbol{v}_j) = \boldsymbol{e}_j$

$(j = k+1, \ldots, n)$. б) Нехай $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ – база P^n, $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ – база підпростору $U \subseteq P^m$. Розгляньте лінійне відображення $\varphi : P^n \to P^m$, при якому $\varphi(\boldsymbol{e}_i) = \boldsymbol{u}_i$ $(i = 1, \ldots, k)$, $\varphi(\boldsymbol{e}_j) = \boldsymbol{0}$ $(j = k+1, \ldots, n)$. **4.3.** а) Наприклад, $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$; б) Напр., $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$. **4.4.** *Вказ*. Використайте задачу 4.2. **4.5.** а) Система стовпців матриці B повинна лінійно виражатися через систему стовпців матриці A. б) Система рядків матриці B повинна лінійно виражатися через систему рядків матриці A. *Вказ.* Застосуйте теорему 26. **4.6.** *Вказ.* Якщо A – квадратна матриця порядку n, то матриці $A^{n^2}, A^{n^2-1}, \ldots, A, E$ лінійно залежні. **4.7.** *Вказ.* Елементарними перетвореннями рядків розширеної матриці $(A|B)$ зведіть матрицю A у лівій частині до ступінчастого вигляду. **4.8.** Так. *Вказ.* Використайте твердження 31. **4.9.** *Вказ.* Використовуючи елементарні перетворення рядків та елементарні матриці, доведіть існування розкладу $A = B_1 C_1$, в якому лише перші r рядків матриці C_1 є ненульовими. **4.11**. *Вказ.* Із задачі 4.10 випливає, що $\operatorname{rank} A + \operatorname{rank} B + \operatorname{rank} C \leq \operatorname{rank}(AB) + n + \operatorname{rank} C \leq \operatorname{rank}(ABC) + 2n$. **4.12.** *Вказ.* Розгляньте пов'язане з матрицею A лінійне відображення $\varphi : P^n \to P^m$. **4.15.** *Вказ.* $A^2 = A$ тоді й лише тоді, коли A є матрицею проектування на певний підпростір в $\mathbb{R}^2$. **4.17.** *Вказ.* Із задачі 4.16.д випливає, що $(A \times B) \cdot (A^{-1} \times B^{-1}) = E_{mn}$. **4.19.** б) Для комплексних матриць можна гарантувати лише симетричність матриць $AA^\top$ і $A^\top A$. Контрприклад до другої частини твердження: $\left(\begin{smallmatrix} 1 & i \\ 1 & i \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ i & i \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. *Вказ.* а) Оскільки $\operatorname{rank} A = \operatorname{rank} A^\top$ і $AA^\top = (A^\top)^\top A^\top$, то досить лише розглянути випадок $A^\top A$. Для довільної матриці $B \in M_{m\times n}(\mathbb{R})$ простір розв'язків СЛР $Bx = 0$ має розмірність $n - \operatorname{rank} B$. Якщо $A \in M_{m\times n}(\mathbb{R})$, то $A^\top A \in M_{n\times n}(\mathbb{R})$. Тому досить показати еквівалентність СЛР $A\boldsymbol{x} = 0$ і $A^\top A\boldsymbol{x} = 0$. Нехай $A^\top A\boldsymbol{x} = 0$ і $A\boldsymbol{x} = (x_1, \ldots, x_n)^\top$. Тоді $\boldsymbol{x}^\top A^\top \cdot A\boldsymbol{x} = 0$, звідки $x_1^2 + \ldots + x_n^2 = 0$ і $A\boldsymbol{x} = 0$. **4.20.** *Вказ.* Нехай $A\boldsymbol{x} = \boldsymbol{b}$ і $A^\top \boldsymbol{y} = \boldsymbol{0}$. Тоді $\boldsymbol{b}^\top \cdot \boldsymbol{y} = \boldsymbol{x}^\top A^\top \cdot \boldsymbol{y} = \boldsymbol{0}$. Навпаки, якщо $\boldsymbol{b}^\top \cdot \boldsymbol{y} = \boldsymbol{0}$ для всіх розв'язків СЛР $A^\top \boldsymbol{y} = \boldsymbol{0}$, то $\boldsymbol{b}^\top$ є лінійною комбінацією рядків матриці $A^\top$. Але тоді $\boldsymbol{b}$ є лінійною комбінацією стовпців матриці A, а тому СЛР $A\boldsymbol{x} = \boldsymbol{b}$ має розв'язок. **4.21**. *Вказ.* Елементарні перетворення стовпців рівносильні множенню справа на елементарні матриці. Тому матриця B, як добуток елементарних матриць, є невиродженою і $C = AB$. Те, що продовження нульових стовпців матриці AB є розв'язками ОСЛР $A\boldsymbol{x} = \boldsymbol{0}$, випливає з того, що в добуткові AB відповідні стовпці є нульовими. Їх кількість дорівнює $n - \operatorname{rank} A$, тобто збігається з розмірністю простору розв'язків ОСЛР, а їх лінійна незалежність випливає з невиродженості матриці B.

Розділ 5. 5.2. $\frac{n!}{1^{l_1} 2^{l_2} \cdots n^{l_n} l_1! l_2! \cdots l_n!}$. **5.4.** *Вказ.* Нехай s – кількість тих чисел, які стоять перед k і які менші за k. Тоді k утворює $j - 1 - s$ ін-

версій із числами, які стоять перед k, і $k-1-s$ інверсій із числами, які стоять після k. Тому $m = m' + (j+k) - 2(1+s)$. **5.5.** *Вказ.* а) Цикл довжини k має знак $(-1)^{k-1}$; б) цикл довжини k можна розкласти в добуток $k-1$ транспозицій; в) цикл довжини k не можна розкласти в добуток менше ніж $k-1$ транспозицій. **5.7.** *Вказ.* Кожна підстановка із S_n розкладається в добуток транспозицій із даної множини транспозицій тоді й лише тоді, коли граф, що відповідає цій множині, є зв'язним. **5.8.** *Вказ.* Кількість способів розкладу для всіх циклів довжини n однакова, а всього є $(n-1)!$ циклів довжини n. Добуток $n-1$ транспозицій є циклом довжини n тоді й лише тоді, коли ці транспозиції відповідають дереву. За теоремою Келі кількість дерев із вершинами $\{1, 2, \ldots, n\}$ дорівнює n^{n-2}, а ребра такого дерева можна впорядкувати $(n-1)!$ способами. **5.9.** *Вказ.* Розбийте підстановки на 2 класи залежно від довжини циклу, в який входить число $n+1$: або довжина такого циклу > 2, або дорівнює 2. **5.10**. *Вказ*. б) Перестановку одержуємо, послідовно заповнюючи місця в таблиці довжини n. Число i ставимо на (b_i+1)-е вільне місце (позаяк $b_i \leq n-i$, а вже заповнених місць $i-1$, то це можливо). **5.11**. $a_n, a_{n-1}, \ldots, a_2, a_1$. **5.12**. $1 + 1/2 + 1/3 + \ldots + 1/n$. *Вказ*. k є правостороннім максимумом тоді й лише тоді, коли в таблиці інверсій (див. задачу 5.10) $b_k = n-k$. Різні компоненти таблиці інверсій набувають своїх значень незалежно, а b_k набуває кожного зі своїх значень $0, 1, \ldots, n-k$ однакову кількість разів. **5.13.** Нехай $\pi_1, \pi_2, \ldots, \pi_{n!}$ – потрібне впорядкування перестановок з S_n. Позначимо через π'_i перестановку, яка одержується з π_i дописуванням справа числа $n+1$. Тоді $\tau_1, \tau_2, \ldots, \tau_{(n+1)!}$, де $\tau_{k\cdot n!+i}$ $(1 \leq i \leq n!)$ одержується з π'_i циклічним зсувом на k позицій, буде потрібним упорядкуванням перестановок з S_{n+1}. **5.14.** $\frac{1}{n}\binom{2n-2}{n-1}$. *Вказ.* Нехай C_n – кількість таких способів. Покладіть $C_1 = 1$ і покажіть, що $C_{n+1} = C_1C_n + C_2C_{n-1} + \cdots + C_nC_1$.

Розділ 6. 6.1. а) 4; б) 2. *Вказ.* б) Якщо $\det A > 0$, то в A є принаймні 2 нулі. Але тоді розклад $\det A$ містить не більше 2 додатних доданків. Тому $\det A \leq 2$. З іншого боку, $\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 2$. **6.2.** *Вказ.* б) Використайте а). **6.3.** $\begin{vmatrix} f_1 & f_2 & \cdots & f_n \\ f'_1 & f'_2 & \cdots & f'_n \\ \cdots & \cdots & \cdots & \cdots \\ f_1^{(n-2)} & f_2^{(n-2)} & \cdots & f_n^{(n-2)} \\ f_1^{(n)} & f_2^{(n)} & \cdots & f_n^{(n)} \end{vmatrix}$. *Вказ.* Використайте за-

дачу 6.2.а. **6.4.** *Вказ.* Якщо $P \neq 0$, то можна взяти $A = \begin{pmatrix} P & 0 & -R \\ 0 & 1 & Q/P \end{pmatrix}$.
6.5. *Вказ.* Якщо при фіксованому j усі мінори $M_{\{i,i_1,\ldots,i_k\}}^{\{j,j_1,\ldots,j_k\}}$ дорівнюють нулю, то розкрийте ці мінори за i-м рядком і покажіть, що j-й стовпець є лінійною комбінацією стовпців $j_1, \ldots, j_k$. **6.6.** *Вказ.* Використайте задачу 6.5. **6.7.** *Вказ.* Мінор $M_{\{i_1,\ldots,i_k\}}^{\{j_1,\ldots,j_k\}}(AB)$ має вигляд

$$\begin{vmatrix} a_{i_1 1}b_{1j_1} + \ldots + a_{i_1 n}b_{nj_1} & \ldots & a_{i_1 1}b_{1j_k} + \ldots + a_{i_1 n}b_{nj_k} \\ a_{i_2 1}b_{1j_1} + \ldots + a_{i_2 n}b_{nj_1} & \ldots & a_{i_2 1}b_{1j_k} + \ldots + a_{i_j n}b_{nj_k} \\ \ldots & \ldots & \ldots \\ a_{i_k 1}b_{1j_1} + \ldots + a_{i_k n}b_{nj_1} & \ldots & a_{i_k 1}b_{1j_k} + \ldots + a_{i_k n}b_{nj_k} \end{vmatrix}.$$

Кожен його стовпець записується у вигляді лінійної комбінації k стовпців. Враховуючи це, розкладіть $M_{\{i_1,\ldots,i_k\}}^{\{j_1,\ldots,j_k\}}(AB)$ у суму k^k доданків. **6.8.** *Вказ.* Використайте задачу 6.7. **6.9.** *Вказ.* Використайте теорему про розклад визначника за своїм (чужим) рядком. **6.10.** *Вказ.* Нехай $A = (a_{ij})$ і $A^{-1} = (b_{ij})$. Використайте рівність

$$\begin{vmatrix} b_{11} & \ldots & b_{1k} & b_{1,k+1} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ b_{k1} & \ldots & b_{kk} & b_{k,k+1} & \ldots & b_{kn} \\ 0 & \ldots & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & \ldots & 1 \end{vmatrix} \cdot A = \begin{vmatrix} 1 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 1 & 0 & \ldots & 0 \\ a_{k+1,1} & \ldots & a_{k+1,k} & a_{k+1,k+1} & \ldots & a_{k+1,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nk} & a_{n,k+1} & \ldots & a_{nn} \end{vmatrix}$$

і теорему Коші. **6.11.** *Вказ.* Розгляньте ті доданки з розкладу $\det A$, які містять k множників, що лежать на перетині рядків із номерами $i_1, \ldots, i_k$ та стовпців із номерами $j_1, \ldots, j_k$. **6.12.** *Вказ.* Використайте задачу 6.11. **6.13.** *Вказ.* A можна звести до верхнього трикутного вигляду, використовуючи лише додавання до рядків лінійних комбінацій попередніх рядків. Перейшовши від елементарних перетворень рядків до множення зліва на елементарні матриці, одержимо розклад $A = UB$. Якщо $U_1B_1 = U_2B_2$, то $U_2^{-1}U_1 = B_2B_1^{-1}$, де $U_2^{-1}U_1$ є нижньою трикутною матрицею з одиницями на діагоналі, а $B_2B_1^{-1}$ – верхньою трикутною. **6.14.** *Вказ.* а) Доповняльні мінори матриць $A^\top$ і A пов'язані співвідношенням $\overline{M}_i^j(A^\top) = \overline{M}_j^i(A)$. в) Використайте формулу Біне – Коші (задача 6.7). **6.15.** *Вказ.* Якщо A – невироджена, то це випливає з рівності $A \cdot A^* = |A|^n \cdot E$. Якщо ж A – вироджена, то A^* також є виродженою (це очевидно, якщо $r < n - 1$; якщо ж $r = n - 1$,

то використайте задачу 6.9). **6.16.** *Вказ.* Використайте задачу 6.14.а. **6.17.** *Вказ.* а) Використайте рівність $A \cdot A^* = |A|^n \cdot E$. б) Нехай невироджена матриця A з першим рядком $(a_1, a_2, \ldots, a_n)$ є асоційованою з матрицею B. Тоді матриця $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix}$ буде асоційованою з матрицею C, яка одержується з B заміною елементів першого стовпця нулями. Далі використайте задачу 6.14 і те, що кожну квадратну матрицю рангу 1 можна розкласти в добуток $\begin{pmatrix} b_1 & 0 & \ldots & 0 \\ b_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ b_n & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \end{pmatrix}$.

6.18. *Вказ.* $\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} - \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ тоді й лише тоді, коли $\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix} = a$, $\begin{vmatrix} x_2 & x_4 - x_1 \\ y_2 & y_4 - y_1 \end{vmatrix} = b$, $\begin{vmatrix} x_4 - x_1 & x_3 \\ y_4 - y_1 & y_3 \end{vmatrix} = c$. Далі використайте задачу 6.4. **6.19.** *Вказ.* Позначимо визначник через $D(k, r, n)$. Використовуючи рівність $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$, можна винести з першого рядка k, із другого рядка – $k+1$, і т. д., а потім із першого стовпця $\frac{1}{r}$, із другого стовпця – $\frac{1}{r+1}$, і т. д. Це дає рекурентне співвідношення

$$D(k, r, n) = \frac{k(k+1)\cdots(k+n-1)}{r(r+1)\cdots(r+n-1)} D(k-1, r-1, n) = \frac{\binom{n+k-1}{n}}{\binom{n+r-1}{n}} D(k-1, r-1, n).$$

Нарешті, якщо у визначнику $D(m, 0, n)$ із кожного рядка відняти попередній, а потім отриманий визначник розкрити за першим стовпцем і скористатися рівністю $\binom{i}{j} - \binom{i-1}{j} = \binom{i-1}{j-1}$, то одержимо рекурентне співвідношення $D(m, 0, n) = D(m-1, 0, n-1)$, з якого випливає, що $D(k-r, 0, n) = 1$.

6.20. *Вказ.* Якщо матрицю $\begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}$ помножити на матрицю $A = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \varepsilon & \varepsilon^2 & \ldots & \varepsilon^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \varepsilon^{n-1} & \varepsilon^{2(n-1)} & \ldots & \varepsilon^{(n-1)(n-1)} \end{pmatrix}$, то в добутку вийде матриця, яка одержується з A множенням першого стовпця на $a_0 + a_1 + a_2 + \ldots + a_{n-1}$, другого стовпця – на $a_0 + \varepsilon a_1 + \varepsilon^2 a_2 + \ldots + \varepsilon^{(n-1)} a_{n-1}$, ..., останнього

стовпця – на $a_0 + \varepsilon^{n-1}a_1 + \varepsilon^{2(n-1)}a_2 + \ldots + \varepsilon^{(n-1)(n-1)}a_{n-1}$. Далі використайте теорему про визначник добутку двох матриць. **6.21.** *Вказ.* $\det\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\det\left(\begin{smallmatrix} D & 0 \\ 0 & C \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} AD & BC \\ CD & DC \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} AD & BC \\ CD & CD \end{smallmatrix}\right) = \det\left(\begin{smallmatrix} AD-BC & BC \\ 0 & CD \end{smallmatrix}\right) = \det(AD-BC)\det(CD)$.

Розділ 7. **7.1.** *Вказ.* Поділіть a, b і n на d. **7.2.** *Вказ.* Якщо $x^2 \equiv a$, то $(8x)^2 \equiv -a$. **7.3.** *Вказ.* Від нетривіальної лінійної комбінації з раціональними коефіцієнтами, яка дорівнює $\mathbf{0}$, перейдіть до лінійної комбінації із цілими коефіцієнтами, з яких принаймні один не ділиться на p. **7.4.** *Вказ.* Якщо система з k векторів лінійно незалежна, то в матриці, утвореній із координат цих векторів, є ненульовий мінор порядку k. Цей мінор ділиться лише на скінченну кількість простих чисел. **7.5**. б) Ні. *Вказ.* б) Конгруенція $4x \equiv 2 \pmod p$ сумісна для всіх простих p, однак рівняння $4x = 2$ не має цілих розв'язків. **7.6.** У загальному випадку – ні; якщо хоча б один з елементів є оборотним – так. **7.7**. *Вказ.* Визначник матриці A є оборотним елементом кільця $\mathbb{Z}_m$, а тому систему $A\boldsymbol{x} = \boldsymbol{b}$ можна розв'язувати за правилом Крамера. **7.8.** а) 8; б) 184.

Розділ 8. **8.1.** Так. *Вказ.* Нехай $g(x) = x^k(c_0 + \ldots + c_m x^m)$, де $c_0 \neq 0$. Покажіть, що для довільного ряду $\widehat{f}(x) = a_k x^k + \cdots + a_n x^n + \cdots$ по індукції можна знайти коефіцієнти такого ряду $h(x) = b_0 + b_1 x + \ldots + b_n x^n + \ldots$, що $\widehat{f}(x) = h(x)g(x)$. **8.2.** *Вказ.* Якщо $f(x^n)$ ділиться на $x - 1$, то $f(1) = 0$. Але тоді $f(x)$ ділиться на $x - 1$. Тому $f(x^n)$ ділиться на $x^n - 1$. **8.3.** *Вказ.* Розкладіть $f(x + y)$ за степенями y. **8.4.** *Вказ.* а) Розгляньте многочлен $xf'(x)$ і застосуйте індукцію. б) Запишіть многочлени $g_i(x)$ із невизначеними коефіцієнтами і спочатку покажіть, що кожна послідовність $f_n = \sum_{i=1}^m g_i(n)\beta_i^n$ задовольняє рекурентне співвідношення (8.44). Потім покажіть, що для довільних $f_1, f_2, \ldots, f_k$ СЛР $\sum_{i=1}^m g_i(1)\beta_i^1 = 1, \ldots, \sum_{i=1}^m g_i(k)\beta_i^k = k$ буде сумісною. **8.5.** *Вказ.* Якщо $f(x)$ розкладається над $\mathbb{R}$ на лінійні множники, то $g(x) = x^5 f(\frac{1}{c}) = cx^5 + bx^2 + ax + 1$ також розкладається на лінійні множники. Нехай x_1, x_2, x_3, x_4, x_5 – його корені. За допомогою формул Вієта обчисліть $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$. **8.6.** *Вказ.* Нехай корені многочленів $f(x)$ і $g(x)$ дійсні і розділяються. Можна вважати, що $f(x)$ і $g(x)$ нормовані і що $\deg f(x) \geq \deg g(x)$. Можливі два випадки: I. $\deg f(x) = \deg g(x)$; II. $\deg f(x) = \deg g(x) + 1$. Розглянемо перший випадок. Нехай $x_1 < x_2 < \ldots < x_n$ – корені $f(x)$, $y_1 < y_2 < \ldots < y_n$ – корені $g(x)$. Можна вважати, що $x_1 < y_1 < x_2 < \ldots < y_{n-1} < x_n < y_n$. При $a = 0$ твердження очевидне, тому рівняння $af(x) + bg(x) = 0$ можна переписати у вигляді $\frac{f(x)}{g(x)} = -\frac{b}{a}$. Розглянемо поведінку функції $\varphi(x) = \frac{f(x)}{g(x)}$. Ця функція неперервна на кожному з інтервалів $(-\infty, y_1)$, (y_1, y_2), $\ldots$, (y_{n-1}, y_n), (y_n, ∞), і змінюється на кожному із цих інтервалів відповідно від 1 до

$-\infty$, від ∞ до $-\infty$, ..., від ∞ до $-\infty$, від ∞ до 1. Таким чином, якщо $\frac{b}{a} = -1$, то рівняння $\varphi(x) = -\frac{b}{a}$ має не менше ніж $n-1$ корінь, а якщо $\frac{b}{a} \neq -1$ – то не менше ніж n коренів. Тому кількість дійсних коренів многочлена $af(x)+bg(x)$ збігається з його степенем. Випадок II аналізується аналогічно. Навпаки, нехай для довільних дійсних чисел a і b многочлен $af(x)+bg(x)$ має дійсні корені. Тоді корені кожного із многочленів $f(x)$ і $g(x)$ будуть дійсними. Припустимо, що між сусідніми коренями x_1 і x_2 многочлена $f(x)$ немає коренів многочлена $g(x)$. Тоді функція $\varphi(x) = \frac{f(x)}{g(x)}$ буде диференційовною на $[x_1, x_2]$ і $\varphi(x_1) = \varphi(x_2) = 0$. Отже, існує така точка $c \in (x_1, x_2)$, що $\varphi'(c) = 0$. Для многочлена $g'(c)f(x) - f'(c)g(x)$ і для функції $\varphi(x) - \varphi(c)$ ця точка c буде кратним коренем. Тому існує таке мале α, що для функції $\varphi(x) - \varphi(c) + \alpha$ точка c вже не буде коренем, а в околі c, можливо, з'явиться простий корінь цієї функції. Але тоді при переході від $g'(c)f(x) - f'(c)g(x)$ до многочлена $g'(c)f(x) - (f'(c) + \alpha g'(c))g(x)$ також зникне кратний корінь, замість якого з'явиться щонайбільше один простий. Тому в останньому многочлені не всі корені будуть дійсними. **8.7.** *Вказ.* Якщо НСД $(f(x), f'(x)) = 1$, то це частковий випадок задачі 8.6. Якщо ж НСД $(f(x), f'(x)) = d(x)$, то твердження буде правильним для многочлена $\frac{f(x)}{d(x)} + a\frac{f'(x)}{d(x)}$, до якого лишається приєднати корені $d(x)$. **8.8.** *Вказ.* Відповідно до задачі 8.6 для довільних дійсних чисел a і b всі корені многочлена $af(x) + bg(x)$ – дійсні. Але тоді всі корені похідної $af'(x) + bg'(x)$ також будуть дійсними. Далі знову скористайтеся задачею 8.6. **8.9.** *Вказ.* Нехай $g(x) = a_n(x + c_1)(x + c_2)\cdots(x + c_n)$. Покладемо $h_0(x) = a_n f(x)$, $h_1(x) = h_0(x) + c_1 h_0'(x) = a_n f(x) + a_n c_1 f'(x)$, $h_2(x) = h_1(x) + c_2 h_1'(x) = a_n f(x) + a_n(c_1 + c_2)f'(x) + a_n c_1 c_2 f''(x)$ і т. д. Тоді $h_n(x) = h_{n-1}(x) + c_n h_{n-1}'(x) = a_n f(x) + a_{n-1} f'(x) + \ldots + a_0 f^{(n)}(x) = F(x)$. Згідно із задачею 8.7 усі корені кожного із многочленів $h_0(x)$, $h_1(x)$, ..., $h_n(x)$ будуть дійсними. **8.10.** *Вказ.* Нехай $f(x) = a_n x^n + \cdots + a_0$ і нехай кількість таких p скінченна. Тоді $a_0 \neq 0$. Візьмемо b, яке ділиться на всі такі p. Тоді $f(a_0 b) = a_0(a_n a_0^{n-1} b^n + \ldots + a_1 b + 1) = a_0 c$, причому $c \equiv 1 \pmod{b}$. Позаяк існує лише скінченна кількість таких b, що $f(a_0 b) = \pm a_0$, то можна вважати, що $c \neq \pm 1$. Але тоді для кожного простого дільника $q|c$ буде $f(a_0 b) \equiv 0 \pmod{q}$, що суперечить вибору b. **8.11.** $x^p - x = x(x-1)(x-2)\cdots(x-p+1)$. *Вказ.* Використайте малу теорему Ферма. **8.12.** *Вказ.* Використайте результат задачі 8.11. **8.13.** *Вказ.* $g'(x) = \sum_{k=0}^{n}(x - c_0)\cdots(x - c_{k-1})(x - c_{k+1})\cdots(x - c_n)$. **8.14.** *Вказ.* Нехай u – центр правильного m-кутника, w – одна з його вершин, $v = w - u$. Тоді вершини m-кутника мають вигляд $u + v\varepsilon^k$ $(k = 0, 1, \ldots, m-1)$, де ε – первісний корінь степеня m з 1. Якщо $0 < j < m$, то $\sum_{k=0}^{m-1} \varepsilon^{kj} = 0$.

Тому для $r < m$ маємо $\frac{1}{m}\sum_{k=0}^{m-1}(u+v\varepsilon^k)^r = \frac{1}{m}\sum_{k=0}^{m-1}\left(\sum_{j=0}^{r}\binom{r}{j}u^{r-j}(v\varepsilon^k)^j\right) =$
$= \frac{1}{m}\sum_{j=0}^{r}\binom{r}{j}u^{r-j}v^j\left(\sum_{k=0}^{m-1}\varepsilon^{kj}\right) = \frac{1}{m}u^r v^0\sum_{k=0}^{m-1}\varepsilon^0 = u^r$. **8.15.** $\frac{1}{n}\sum_{k=0}^{n-1}\frac{\varepsilon_k}{x-\varepsilon_k}$, де $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ – усі комплексні корені степеня n з одиниці. **8.16.** $\sum_{k=0}^{p-1}\frac{p-1}{x-k}$. *Вказ.* Над полем $\mathbb{Z}_p$ $x^p - x = \prod_{k=0}^{-1}(x-k)$. Далі скористайтесь методом невизначених коефіцієнтів і теоремою Вільсона: $(p-1)! \equiv -1 \pmod{p}$. **8.17.** *Вказ.* Якщо $c > 1 + \sqrt[m]{A}$, то $f(c) \geq c^n - A(c^{n-m} + c^{n-m-1} + \cdots + 1) =$
$= c^n - A\cdot\frac{c^{n-m+1}-1}{c-1} > \frac{c^{n-m+1}}{c-1}\big((c-1)c^{m-1} - A\big) > \frac{c^{n-m+1}}{c-1}\big((c-1)^m - A\big) > 0$.

Література

[1] 1. Безущак О.О. Елементи теорії чисел / О. О. Безущак, О. Г. Ганюшкін. – К. : ВПЦ «Київський університет», 2003.

[2] 2. Безущак О.О. Завдання до практичних занять з лінійної алгебри / О. О. Безущак, О. Г. Ганюшкін, Кочубінська Є. А. – К. : ВПЦ «Київський університет», 2015.

[3] *Боднарчук Ю.В., Олійник Б.В.* Лінійна алгебра та аналітична геометрія.

[4] *Винберг Э.Б.* Курс алгебры. М., 2002, 544 с.

[5] Виноградов И. М. Основы теории чисел / И. М. Виноградов. – СПб. : Лань, 2009.

[6] Гаусс К. Ф. Труды по истории чисел / К. Ф. Гаусс. – М. : Изд-во АН СССР, 1959.

[7] Гельфанд И. М. Лекции по линейной алгебре / И. М. Гельфанд. – М. : Наука, 1971

[8] Даан-Дальмедико А. / А. Даан-Дальмедико, Ж. Пфейффер. Пути и лабиринты. Очерки по истории математики. – М. : Мир, 1986.

[9] *Завало С.Т.* Курс алгебри. К., 1985, 503 с.

[10] *Завало С.Т., Костарчук В.М., Хацет Б.І.* Алгебра і теорія чисел. Ч. 1,2. К., 1976.

[11] *Калужнін Л.А., Вишенський В.А., Шуб Ц.О.* Лінійні простори. К., 1971, 343 с.

[12] Клейн Ф. Лекции о развитии математики в XIX столетии / Ф. Клейн. – М. : Наука, 1989.

[13] *Кострикин А.И.* Введение в алгебру. М., 1977, 495 с.

[14] *Кострикин А.И.* Введение в алгебру. Основные структуры. М., 1994, 318 с.

[15] *Курош А.Г.* Курс высшей алгебры. М., 1968, 431 с.

[16] Мальцев А.И. Основы линейной алгебры / А. И. Мальцев. – М. : Наука, 1970

[17] *Фаддеев Д.К.* Лекции по алгебре. М., 1984, 416 с.

[18] Фаддеев Д. К. Сборник задач по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. – М. : Наука, 1968.

Предметний покажчик