Київський національний університет імені Тараса Шевченка

О.Г.Ганюшкін

ВСТУП
ДО АЛГЕБРИ

Навчальний посібник
для студентів механіко-математичного факультету

Київ
Видавничо–поліграфічний центр
“Київський університет“
2013

О.Г.Ганюшкін. Вступ до алгебри : навчальний посібник для студентів механіко–математичного факультету. – К. : ВПЦ "Київський університет", 2013. – 183 с.

Рецензенти: д-р фіз.-мат. наук, проф. М.Ф.Городній,
д-р фіз.-мат. наук, проф. А.П.Петравчук

Дисципліна "Вступ до алгебри" читається на механіко-математичному факультеті після загального курсу "Алгебра і теорія чисел" і має пропедевтичну мету — підготувати студента до слухання спеціальних курсів із різних областей алгебри. Посібник можна використовувати для різних варіантів читання такої дисципліни. Наявність великої кількості задач різної складності дозволяє використовувати посібник для проведення практичних задач і контрольних робіт.

Рекомендовано до друку вченою радою механіко-математичного факультету Київського національного університету імені Тараса Шевченка (протокол № 3 від 08.10.2012 року)

Зміст

Вступ

Книгу написано на основі кількох варіантів лекційної дисципліни "Вступ до алгебри", яку автор читав на механіко-математичному факультеті Київського національного університету імені Тараса Шевченка. Мета дисципліни — хоча б частково ліквідувати ті прогалини, що лишаються в загальній алгебричній освіті студента після вивчення нормативного курсу "Алгебра і теорія чисел", і закласти базу для подальшого більш поглибленого вивчення окремих розділів алгебри. Зрозуміло, що охопити хоча б початкові основи всіх розділів сучасної алгебри в підручнику такого обсягу просто неможливо. Тому вибір матеріалу та акцентів у його викладі робився як з огляду на його важливість (що є дуже суб'єктивною думкою автора), так і з огляду на наукові інтереси кафедри алгебри та математичної логіки Київського національного університету імені Тараса Шевченка (що є вже значно об'єктивнішою підставою для вибору). Зокрема, за межами посібника лишилися такі важливі розділи алгебри, як кільця та модулі над ними, групи та алгебри Лі, практично не розглянуто теорію зображень. Однак виклад основ кожного з цих розділів вимагає окремого спеціального курсу.

Припускається, що читач уже засвоїв стандартний нормативний курс алгебри. Тому елементарні властивості основних алгебричних структур — груп, кілець, полів, векторних просторів — вважаються відомими і зазвичай використовуються без посилань. Загальноприйняті позначення — як-от $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ і $\mathbb{C}$ для множин натуральних, цілих, раціональних, дійсних і комплексних чисел відповідно, $|M|$ для потужності множини M, і подібні — використовуються без пояснень. Список більш-менш усталених позначень, які студент не зобов'язаний знати після перших двох років навчання, наводиться в кінці книги.

Список літератури зовсім не претендує на повноту і містить лише кілька найбільш доступних (у прямому й переносному значеннях) книг, які можна використати для знайомства з іншими підходами до викладеного матеріалу і для його більш поглибленого вивчення.

Нечисленні вправи і задачі, які зустрічаються в основному тексті, є його невід'ємною частиною. Зокрема, на них можуть бути посилання у подальшому тексті.

1 Універсальні алгебри

1.1 Базові поняття

Означення 1.1. *Нехай M — непорожня множина, а $n \geq 0$ — ціле число. n-**арною дією** (або n-**арною операцією**) на непорожній множині M називається довільне відображення $\omega : M^n \to M$ n-го декартового степеня M^n у M. При $n = 1, 2, 3$ дія називається відповідно **унарною**, **бінарною**, **тернарною**. Арність операції ω позначаємо $n(\omega)$.*

При $n = 1$ це просто довільне перетворення множини M (тобто відображення M у себе). Оскільки зручно вважати, що $M^0 = \{\varnothing\}$, то 0-*арна дія* просто фіксує (виділяє) у множині M певний елемент. Тому 0-арні операції ще називають *константами*.

Результат застосування n-арної дії ω до елементів $a_1, \ldots, a_n \in M$ будемо зазвичай позначати через $\omega(a_1, \ldots, a_n)$. У випадку бінарних дій часто замість $\omega(a_1, a_2)$ пишуть $a_1 \omega a_2$.

Інколи буває зручно розглядати також дії *часткові* (тобто визначені на якійсь підмножині з M^n), *багатозначні* (значеннями є підмножини з M) або *нескінченноарні*. Однак далі дії будуть розумітися лише в сенсі означення 1.1, а щодо виняткiв робитимуться спеціальні застереження.

Операції арності, більшої ніж 2, з'являються в математиці нечасто. Прикладами таких операцій є:

a) тернарна операція знаходження четвертої вершини паралелограма за трьома відомими послідовними вершинами A_1, A_2, A_3;

b) n-арна операція знаходження центра ваги системи n точок одиничної ваги;

c) тернарна операція $(\varphi, \psi, \mu) := \varphi\psi^{-1}\mu$ у множині всіх бієкцій вигляду $A \to B$, де множини A і B — фіксовані.

Означення 1.2. ***Універсальною алгеброю*** (*або просто* ***алгеброю***) $\langle A; (\omega_i)_{i \in I} \rangle$ *називається непорожня множина A із заданою на ній системою $\Omega = (\omega_i)_{i \in I}$ дій. Множина A називається **носієм** алгебри. Множина Ω символів дій називається **сигнатурою** алгебри $\langle A; (\omega_i)_{i \in I} \rangle$, а родина $(n_i)_{i \in I}$ арностей дій із Ω — **типом** цієї алгебри.*

Алгебра з носієм A і сигнатурою Ω позначається $\langle A; \Omega \rangle$. Якщо сигнатура відома або не є важливою, то замість $\langle A; \Omega \rangle$ пишуть просто A. Якщо ж треба підкреслити, що йдеться не про носія алгебри, а про саму алгебру (тобто носій разом із операціями на ньому), то ми використовуватимемо каліграфічний шрифт і замість A писатимемо $\mathcal{A}$. Через $|A|$ позначатимемо *порядок* алгебри $\mathcal{A}$, тобто потужність множини A.

Приклади універсальних алгебр:

1) напівгрупи (одна бінарна операція — множення);

2) моноїди (одна бінарна операція — множення, одна константа — нейтральний елемент);

3) групи (одна бінарна операція — множення, одна унарна — взяття оберненого елемента, одна константа — нейтральний елемент);

4) кільця (дві бінарні операції — додавання і множення, одна константа — нейтральний елемент для додавання);

5) кільця з 1 (дві бінарні операції — додавання і множення, дві константи — нейтральні елементи для додавання і множення);

6) векторні простори (одна бінарна операція — додавання векторів, одна константа — нульовий вектор $\mathbf{0}$, і кожному елементу поля скалярів відповідає своя унарна операція — множення векторів на цей елемент).

Якщо $\mathcal{A}$ — універсальна алгебра сигнатури Ω, то множину $P(A)$ всіх непорожніх підмножин носія A також можна перетворити в алгебру $P(\mathcal{A})$ сигнатури Ω, якщо для кожної операції ω арності n і довільних множин $A_1, \ldots, A_n$ покласти:

$$\omega(A_1, \ldots, A_n) = \{\omega(a_1, \ldots, a_n) \mid a_1 \in A_1, \ \ldots, \ a_n \in A_n\}.$$

$P(\mathcal{A})$ називається *глобальною надалгеброю* алгебри $\mathcal{A}$. Походження назви зрозуміле: при природному ототожненні одноелементних множин зі своїми елементами $P(\mathcal{A})$ справді є надалгеброю алгебри $\mathcal{A}$.

Означення 1.3. *Підмножина $B \subseteq A$ алгебри $\langle A; \Omega\rangle$ називається* ***підалгеброю****, якщо вона замкнена відносно всіх операцій з Ω. Іншими словами, для довільних $\omega \in \Omega$ і $b_1, \ldots, b_n \in B$, де n — арність дії ω, має бути $\omega(b_1, \ldots, b_n) \in B$.*

Зауваження. Підалгебра $\mathcal{B}$ має бути замкненою і відносно нульарних дій, тобто вона повинна містити всі виділені елементи алгебри $\mathcal{A}$. Тому в алгебрі з виділеними елементами кожна підалгебра є непорожньою. Якщо ж $\mathcal{A}$ не містить виділених елементів, то зручно вважати підалгеброю і порожню множину.

Твердження 1.1. *Перетин довільної родини підалгебр алгебри $\langle A; \Omega\rangle$ також буде підалгеброю цієї алгебри.*

Доведення. Нехай $(\mathcal{B}_j)_{j\in J}$ — довільна родина підалгебр алгебри $\mathcal{A}$, а $B = \bigcap_{j\in J} B_j$. Припустимо, що $B \neq \varnothing$. Розглянемо довільні операцію $\omega \in \Omega$ і $b_1, \ldots, b_n \in B$, де $n = n(\omega)$. Позаяк кожна з множин B_j є підалгеброю і містить $b_1, \ldots, b_n$, то $\omega(b_1, \ldots, b_n) \in B_j$ для всіх $j \in J$, а

тому $\omega(b_1,\dots,b_n)\in\bigcap_{j\in J}B_j$. Отже, множина B замкнена відносно всіх операцій із Ω. $\square$

Наслідок 1.1. *Для довільної підмножини $M\subseteq A$ алгебри $\langle A;\Omega\rangle$ серед підалгебр, що містять M, існує найменша.*

Доведення. Родина тих підалгебр алгебри $\langle A;\Omega\rangle$, що містять M, не є порожньою — вона містить принаймні саму алгебру $\langle A;\Omega\rangle$. Очевидно, що перетин усіх таких підалгебр і буде шуканим. $\square$

Означення 1.4. *Найменша серед підалгебр, що містять M, позначається $\langle M\rangle$ і називається підалгеброю, **породженою** множиною M. Якщо $\langle M\rangle=\mathcal{A}$, то M називається **системою твірних** алгебри $\mathcal{A}$. Система твірних називається **незвідною**, якщо будь-яка її власна підмножина вже не є системою твірних.*

*Якщо алгебра має скінченну систему твірних, то вона називається **скінченнопородженою**.*

Очевидно, що кожна надмножина системи твірних сама є системою твірних. Тому алгебра може мати багато систем твірних. Навіть якщо обмежитися лише незвідними системами, то їх все одно може бути багато.

Задача 1.1. *Доведіть, що*

a) алгебра $\langle\mathbb{Z};+,-\rangle$ має незвідні системи твірних будь-якої скінченної потужності, але не має нескінченних незвідних систем твірних;

b) алгебра $\langle\mathbb{N};\cdot\rangle$ має єдину незвідну систему твірних, причому ця система є нескінченною.

Алгебри $\langle A;(\omega_i)_{i\in I}\rangle$ і $\langle B;(\tau_i)_{i\in I}\rangle$ називаються *однотипними* (або *подібними*), якщо множини їх операцій занумеровані однією й тією самою множиною індексів I і якщо відповідні операції мають одну й ту саму арність: $n(\omega_i)=n(\tau_i)$ для всіх $i\in I$.

Означення 1.5. ***Гомоморфізмом*** *алгебри $\langle A;(\omega_i)_{i\in I}\rangle$ в однотипну з нею алгебру $\langle B;(\tau_i)_{i\in I}\rangle$ називається таке відображення $\varphi:A\to B$, що для довільних $i\in I$ та $x_1,\dots,x_{n(\omega_i)}\in A$ виконується рівність*

$$\varphi\big(\omega_i(x_1,\dots,x_{n(\omega_i)})\big)=\tau_i\big(\varphi(x_1),\dots,\varphi(x_{n(\omega_i)})\big).$$

Наступне твердження пропонуємо читачеві довести самостійно.

Твердження 1.2. *Нехай $\varphi:\mathcal{A}\to\mathcal{B}$ — гомоморфізм алгебр. Тоді для довільної підалгебри $\mathcal{A}_1\subseteq\mathcal{A}$ її гомоморфний образ $\varphi(\mathcal{A}_1)$ буде підалгеброю алгебри $\mathcal{B}$, а для довільної підалгебри $\mathcal{B}_1\subseteq\mathcal{B}$ її повний прообраз $\varphi^{-1}(\mathcal{B}_1)$ буде підалгеброю алгебри $\mathcal{A}$.*

Для довільних двох гомоморфізмів вигляду $\varphi : \mathcal{A} \to \mathcal{B}$ і $\psi : \mathcal{B} \to \mathcal{C}$ можна визначити їхній добуток (як композицію відображень):

$$(\varphi \cdot \psi)(x) := \psi(\phi(x)).$$

Легко перевіряється, що добуток двох гомоморфізмів $\varphi : \mathcal{A} \to \mathcal{B}$ і $\psi : \mathcal{B} \to \mathcal{C}$ буде гомоморфізмом із $\mathcal{A}$ в $\mathcal{C}$. Позаяк композиція відображень є асоціативною, то асоціативним буде і множення гомоморфізмів.

Окремі класи гомоморфізмів отримали спеціальні назви. Так, ін'єктивні гомоморфізми називаються *мономорфізмами*, а сюр'єктивні — *епіморфізмами*. Гомоморфізми, які одночасно є ін'єктивними та сюр'єктивними, називаються *ізоморфізмами*. Гомоморфізм $\varphi : \mathcal{A} \to \mathcal{A}$ алгебри в себе називається *ендоморфізмом*, а ізоморфізм на себе — *автоморфізмом*.

Вправа 1.1. *Доведіть, що для скінченних алгебр поняття мономорфізму, епіморфізмів та ізоморфізму рівносильні.*

Вправа 1.2. *Доведіть, що відображення, обернене до ізоморфізму, і добуток двох ізоморфізмів також будуть ізоморфізмами.*

Теорія *алгебричних систем* (або *універсальних алгебр*) вивчає переважно лише ті властивості алгебричних систем, які зберігаються при ізоморфізмах і які, таким чином, однакові в усіх ізоморфних системах. Ці властивості часто називають *абстрактними* властивостями систем. Вважається, що абстрактні властивості системи — це властивості операцій системи, які не залежать від природи елементів, що складають систему.

Якщо M — непорожня множина, то *словом* в алфавіті M називається довільна послідовність $v = a_{i_1} a_{i_2} \dots a_{i_k}$ $(k \geq 0)$ елементів із M. Зокрема, при $k = 0$ одержуємо пусте слово Λ. Число k називається *довжиною* слова v.

Нехай тепер X — довільна непорожня множина, яка не має спільних елементів із сигнатурою Ω. Серед усіх слів в алфавіті $X \cup \Omega$ виділимо так звані Ω-*терми* (або *правильно побудовані слова*):

1) усі елементи з X і символи арності 0 з Ω є термами;

2) якщо ω — символ з Ω арності n, а $b_1, \dots, b_n$ — терми, то вираз $\omega(b_1, \dots, b_n)$ також є термом;

3) термами є тільки те, що можна одержати за допомогою пунктів 1 і 2.

Множина всіх Ω-*термів* над алфавітом X позначається $F(\Omega, X)$.

Інколи використовують так звані бездужкові способи запису Ω-термів — *префіксний* (тоді у п. 2 означення терма вираз $\omega(b_1, \ldots, b_n)$ треба замінити на $\omega b_1 \ldots b_n$) або *суфіксний* (тоді $\omega(b_1, \ldots, b_n)$ треба замінити на $b_1 \ldots b_n \omega$).

Задача 1.2. *Нехай використовується префіксний бездужковий запис Ω-термів. Припишемо кожному символу з Ω арності n вагу $\nu = 1 - n$, а кожному символу з X — вагу $\nu = 1$. Доведіть, що слово $\alpha_1 \alpha_2 \ldots \alpha_k$ над алфавітом $X \cup \Omega$ буде Ω-термом тоді й тільки тоді, коли виконуються такі умови:*

$$\nu(\alpha_1) < 1, \quad \nu(\alpha_1) + \nu(\alpha_2) < 1, \quad \ldots, \quad \nu(\alpha_1) + \nu(\alpha_2) + \cdots + \nu(\alpha_{k-1}) < 1,$$
$$\nu(\alpha_1) + \nu(\alpha_2) + \cdots + \nu(\alpha_k) = 1.$$

Множина $F(\Omega, X)$ природним чином перетворюється в алгебру сигнатури Ω: результатом застосування операції ω арності n до термів $b_1, \ldots, b_n$ оголошуємо терм $\omega(b_1, \ldots, b_n)$. Зокрема, виділеними константами є самі символи нульарних операцій. Ця алгебра називається (*абсолютно*) *вільною алгеброю* сигнатури Ω із системою твірних X (або *алгеброю Ω-термів* над алфавітом X). Потужність множини X називається *рангом* вільної алгебри $F(\Omega, X)$.

Теорема 1.1 (Основна властивість вільної алгебри)**.** *Кожне відображення $\varphi_0 : X \to \mathcal{B}$ множини X твірних алгебри $F(\Omega, X)$ у довільну алгебру $\mathcal{B}$ сигнатури Ω можна продовжити, причому єдиним способом, до гомоморфізму алгебр $\varphi : F(\Omega, X) \to \mathcal{B}$.*

Доведення. Образи в алгебрі $\mathcal{B}$ символів арності 0 із Ω визначаються однозначно. Якщо ω — операція арності n і образи $\varphi(b_1)$, $\ldots$, $\varphi(b_n)$ термів b_1, $\ldots$, b_n вже визначені, то образом терму $\omega(b_1, \ldots, b_n)$ буде елемент $\omega(\varphi(b_1), \ldots, \varphi(b_n))$. Коректність такого визначення відображення $\varphi : F(\Omega, X) \to \mathcal{B}$ випливає з однозначності побудови терму. Те, що відображення φ є гомоморфізмом, безпосередньо випливає з побудови φ. □

Нехай $\varphi : \mathcal{A} \to \mathcal{B}$ — гомоморфізм однотипних алгебричних систем $\big(A; (\omega_i)_{i \in I}\big)$ і $\big(B; (\tau_i)_{i \in I}\big)$. Покладемо

$$a \sim_\varphi b :\Leftrightarrow \varphi(a) = \varphi(b)\ . \tag{1.1}$$

Відношення $\sim_\varphi$ називають *ядром* гомоморфізму $\varphi : \mathcal{A} \to \mathcal{B}$ і часто позначають $\operatorname{Ker} \varphi$. Очевидно, що $\sim_\varphi$ є відношенням еквівалентності. Тому з ним пов'язане розбиття множини A на класи еквівалентності, яке також називають ядром гомоморфізму φ.

Означення 1.6. *k-арне відношення Φ на множині A називається* ***стабільним*** *відносно n-арної операції ω на A, якщо з того, що відповідні аргументи пов'язані відношенням Φ, випливає, що й значення операції пов'язані цим відношенням. Більш строго: для довільних n наборів $(a_{11}, a_{21}, \ldots, a_{k1})$, $\ldots$, $(a_{1n}, a_{2n}, \ldots, a_{kn})$ із Φ має виконуватися умова*

$$\big(\omega(a_{11}, a_{12}, \ldots, a_{1n}), \ldots, \omega(a_{k1}, a_{k2}, \ldots, a_{kn})\big) \in \Phi. \tag{1.2}$$

Якщо відношення Φ є стабільним відносно кожної операції з Ω, то воно називається ***стабільним на алгебрі*** *$\langle A; \Omega\rangle$.*

Зазвичай нас будуть цікавити бінарні дії й бінарні відношення. У цьому випадку умова (1.2) набуває вигляду

$$(a, a') \in \Phi \ \text{ і } \ (b, b') \in \Phi \ \Rightarrow \ \big(\omega(a, b), \omega(a', b')\big) \in \Phi. \tag{1.3}$$

Означення 1.7. ***Конгруенцією*** *на алгебрі $\langle A; \Omega\rangle$ називається стабільне на цій алгебрі відношення еквівалентності.*

Множину всіх конгруенцій на алгебрі $\langle A; \Omega\rangle$ позначимо $\mathrm{Con}(\mathcal{A})$. Крім того, пов'язане з конгруенцією розбиття A на класи еквівалентності ми також називатимемо конгруенцією.

Твердження 1.3. *Якщо $\varphi : \mathcal{A} \to \mathcal{B}$ — гомоморфізм однотипних алгебричних систем $\big(A; (\omega_i)_{i\in I}\big)$ і $\big(B; (\tau_i)_{i\in I}\big)$, то ядро $\sim_\varphi$ гомоморфізму φ є конгруенцією на алгебричній системі $\mathcal{A}$.*

Доведення. Доведемо, наприклад, узгодженість відношення $\sim_\varphi$ із визначеною на A дією ω_i арності n. Справді, якщо $a_1 \sim_\varphi b_1$, $\ldots$, $a_n \sim_\varphi b_n$ для a_1, $\ldots$, a_n, b_1, $\ldots$, $b_n \in A$, то

$$\varphi(\omega_i(a_1, \ldots, a_n)) = \tau_i(\varphi(a_1), \ldots, \varphi(a_n)) =$$

$$= \tau_i(\varphi(b_1), \ldots, \varphi(b_n)) = \varphi(\omega_i(b_1, \ldots, b_n)).$$

Отже, $\omega_i(a_1, \ldots, a_n) \sim_\varphi \omega_i(b_1, \ldots, b_n)$, тобто відношення $\sim_\varphi$ узгоджене з дією ω_i. □

Вправа 1.3. *Доведіть, що перетин довільної родини конгруенцій на алгебрі $\mathcal{A}$ також буде конгруенцією на $\mathcal{A}$.*

Позаяк конгруенція є відношенням еквівалентності, то далі ми позначатимемо її символом $\sim$ і замість $(a, b) \in \sim$ писатимемо $a \sim b$.

Приклади. **1**. *Нульова* конгруенція $\mathbf{o}_A = \{(a, a) \mid a \in A\}$ (= відношення рівності).

2. *Одинична* (або *тотальна*) конгруенція $\mathbf{i}_A = A \times A$.

Про задовільний опис усіх конгруенцій для довільних алгебричних систем можна лише мріяти. Але конгруенції на групах влаштовані відносно просто.

Теорема 1.2. *Відношення еквівалентності на групі G буде конгруенцією тоді й лише тоді, коли класи еквівалентності цього відношення є класами суміжності за деякою нормальною підгрупою.*

Доведення. Необхідність. Нехай $\sim$ — конгруенція на групі G. Позначимо символом $\cdot$ дію на G і розглянемо той клас еквівалентності H, який містить одиницю e. Тоді для довільних $a, b \in H$ маємо: $a \sim e$, $b \sim e$, звідки $a \cdot b \sim e \cdot e = e$, тобто $ab \in H$. Крім того, з $a^{-1} \sim a^{-1}$ випливає, що $a \cdot a^{-1} \sim e \cdot a^{-1}$, тобто $e \sim a^{-1}$. Отже, H є підгрупою.

Далі, для довільних $g_1, g_2 \in G$ із $g_2^{-1} \sim g_2^{-1}$ випливає, що

$$g_1 \sim g_2 \quad \Leftrightarrow \quad g_1 \cdot g_2^{-1} \sim g_2 \cdot g_2^{-1} = e \,,$$

Отже, $g_1 \sim g_2$ тоді й тільки тоді, коли $g_1 \cdot g_2^{-1} \in H$, тобто коли g_1 і g_2 належать одному правому класові суміжності за підгрупою H.

Аналогічно доводиться, що $g_1 \sim g_2$ тоді й лише тоді, коли $g_2^{-1} \cdot g_1 \in H$, тобто коли g_1 і g_2 належать одному лівому класові суміжності за підгрупою H.

Таким чином, класи еквівалентності конгруенції $\sim$ є класами суміжності за підгрупою H, причому ліві та праві класи збігаються, тобто підгрупа H є нормальною.

Достатність. Навпаки, нехай H є нормальною підгрупою групи G. Розглянемо відношення еквівалентності $\sim$, класами еквівалентності якого є класи суміжності за підгрупою H. Нехай $a \sim a_1$ і $b \sim b_1$. Тоді існують такі $h_1 \in H$ і $h_2 \in H$, що $a_1 = ah_1$ і $b_1 = bh_2$. Тому $a_1 b_1 = ah_1 \cdot bh_2 = ab \cdot b^{-1} h_1 b h_2$. Із нормальності H випливає, що $b^{-1} h_1 b h_2 \in H$. Але тоді $a_1 b_1 \in abH$ і $a_1 b_1 \sim ab$. Отже, відношення $\sim$ узгоджене з діями на G, а тому є конгруенцією. $\square$

Якщо $\sim$ — відношення еквівалентності на множині A, то множина $\{\overline{a} \mid a \in A\}$ усіх класів еквівалентності називається *фактормножиною* множини A за відношенням $\sim$ і позначається $A/\!\sim$. Відображення $A \to A/\!\sim$, $a \mapsto \overline{a}$, є, очевидно, сюр'єктивним. Його називають *відображенням факторизації* або *канонічним відображенням* множини A на фактормножину $A/\!\sim$.

Для кожної конгруенції $\sim$ на алгебрі $\big(A; (\omega_i)_{i \in I}\big)$ усі визначені в $\mathcal{A}$ операції природно переносяться на фактормножину $A/\!\sim$:

якщо ω — операція арності n, то

$$\omega(\overline{a_1},\dots,\overline{a_n}) := \overline{\omega(a_1,\dots,a_n)}\,. \tag{1.4}$$

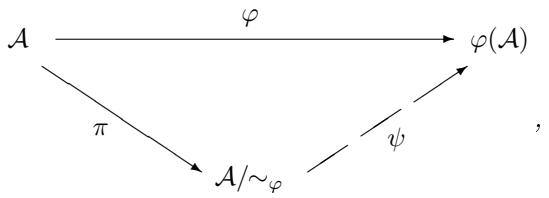
У результаті одержуємо нову алгебру $\big(A/\!\sim;(\omega_i)_{i\in I}\big)$ цієї самої сигнатури, яка називається *факторалгеброю* алгебри $\mathcal{A}$ за конгруенцією $\sim$.

Твердження 1.4. *Нехай відношення $\sim$ є конгруенцією на алгебрі $\big(A;(\omega_i)_{i\in I}\big)$. Тоді відображення $\pi : a \mapsto \overline{a}$ є епіморфізмом алгебри $\mathcal{A}$ на алгебру $\big(A/\!\sim;(\omega_i)_{i\in I}\big)$.*

Доведення. Сюр'єктивність відображення π очевидна, а гомоморфність випливає з означення дій на факторалгебрі. □

Епіморфізм π із твердження 1.4 називається *канонічним* (або *природним*). Легко бачити, що ядром цього гомоморфізму є конгруенція $\sim$. Таким чином, кожна конгруенція є ядром деякого гомоморфізму. З урахуванням твердження 1.3 бачимо, що множина всіх конгруенцій на алгебрі $\mathcal{A}$ збігається з множиною ядер гомоморфізмів із $\mathcal{A}$ в однотипні алгебри.

Теорема 1.3 (Основна теорема про гомоморфізми)**.** *Нехай $\varphi{:}\mathcal{A}\to\mathcal{B}$ — гомоморфізм однотипних алгебр $\big(A;(\omega_i)_{i\in I}\big)$ та $\big(B;(\tau_i)_{i\in I}\big)$, а $\sim_\varphi$ — ядро гомоморфізму φ. Тоді відображення $\psi : \mathcal{A}/\!\sim_\varphi \longrightarrow \varphi(\mathcal{A})$, $\overline{a}\mapsto\varphi(a)$, є ізоморфізмом факторалгебри $\mathcal{A}/\!\sim_\varphi$ на образ $\varphi(\mathcal{A})$ алгебри $\mathcal{A}$ при гомоморфізмі φ, а діаграма*



де $\pi : \mathcal{A} \to \mathcal{A}/\!\sim_\varphi$ — канонічний епіморфізм, є комутативною.

Доведення. 1. *Коректність* визначення ψ. Виберемо довільного представника $b \in \overline{a}$. Тоді $\overline{b} = \overline{a}$ і $\varphi(b) = \varphi(a)$. А тому $\psi(\overline{b}) = \varphi(a)$. Отже, образ $\psi(\overline{a})$ елемента $\overline{a}$ при відображенні ψ визначений однозначно.

2. *Ін'єктивність ψ*:

$$\psi(\overline{a}) = \psi(\overline{b}) \Rightarrow \varphi(a) = \varphi(b) \Rightarrow a \sim_\varphi b \Rightarrow \overline{a} = \overline{b}\,.$$

3. *Сюр'єктивність ψ*. Якщо $b \in \varphi(A)$, то існує таке $a \in A$, що $\varphi(a) = b$. Але тоді $\psi(\overline{a}) = \varphi(a) = b$.

4. *Гомоморфність* ψ. Якщо ω_i — якась дія на A арності n, то для довільних $a_1, \ldots, a_n \in A$ маємо

$$\psi(\omega_i(\overline{a}_1, \ldots, \overline{a}_n)) = \psi(\overline{\omega_i(a_1, \ldots, a_n)}) = \varphi(\omega_i(a_1, \ldots, a_n)) =$$

$$= \tau_i(\varphi(a_1), \ldots, \varphi(a_n)) = \tau_i(\psi(\overline{a}_1), \ldots, \psi(\overline{a}_n)),$$

тобто відображення ψ узгоджене з діями на A.

5. *Комутативність* діаграми. Для довільного $a \in A$ маємо $\varphi(a) = \psi(\overline{a}) = \psi(\pi(a))$, тому $\varphi = \pi\psi$. □

Наслідок 1.2. *Кожна універсальна алгебра ізоморфна факторалгебрі деякої однотипної вільної алгебри.*

Доведення. Це випливає з теорем 1.1 і 1.3. □

Задача 1.3 (Перша теорема про ізоморфізм)**.** *Якщо ρ — конгруенція на алгебрі $\mathcal{A}$ і $\mathcal{B} \subseteq \mathcal{A}$ — підалгебра, то $\rho \cap B^2$ є конгруенцією на $\mathcal{B}$, причому образ $\mathcal{B}$ при канонічному епіморфізмі $\pi : \mathcal{A} \to \mathcal{A}/\rho$ ізоморфний факторалгебрі $\mathcal{B}/(\rho \cap B^2)$.*

Задача 1.4 (Друга теорема про ізоморфізм)**.** *Нехай ρ і τ — конгруенції на алгебрі $\mathcal{A}$, причому $\rho \subseteq \tau$. Тоді відношення*

$$\tau^* = \{(\overline{a_\rho}, \overline{b_\rho}) \in A/\rho \times A/\rho \mid (a, b) \in \tau\}$$

є конгруенцією на факторалгебрі $\mathcal{A}/\rho$, причому $\mathcal{A}/\tau \simeq (\mathcal{A}/\rho)/\tau^*$.

Крім того, відображення $\tau \mapsto \tau^*$ є бієкцією між множиною тих конгруенцій на алгебрі $\mathcal{A}$, які містять ρ, і множиною конгруенцій на факторалгебрі $\mathcal{A}/\rho$, причому відображення $\tau \mapsto \tau^*$ зберігає відношення включення (тобто є ізоморфізмом упорядкованих за включенням множин $\mathrm{Con}(\mathcal{A}/\rho)$ *і* $\{\tau \in \mathrm{Con}(\mathcal{A}) \mid \rho \subseteq \tau\}$ *).*

1.2 Прямі та підпрямі добутки

Означення 1.8. *Нехай $(\mathcal{A}_i)_{i\in I}$ — родина алгебр фіксованої сигнатури $\Omega = (\omega_j)_{j\in J}$. Кожну операцію з Ω можна визначити і на декартовому добутковій $\prod\limits_{i\in I} A_i$ носіїв цих алгебр, якщо її виконувати покомпонентно:*

$$\omega\big((a_i)_{i\in I}, (b_i)_{i\in I}, \ldots, (c_i)_{i\in I}\big) := (\omega(a_i, b_i, \ldots, c_i))_{i\in I}. \qquad (1.5)$$

Визначена таким чином алгебра $\langle \prod_{i\in I} A_i; \Omega\rangle$ називається ***декартовим*** *або (****повним****) **прямим добутком** родини алгебр $(\mathcal{A}_i)_{i\in I}$.*

У випадку скінченної кількості множників $\mathcal{A}_1, \ldots, \mathcal{A}_n$ використовують також позначення $\mathcal{A}_1 \times \cdots \times \mathcal{A}_n$. Якщо всі множники $\mathcal{A}_i$ є копіями алгебри $\mathcal{B}$, то декартів добуток $\prod_{i\in I} \mathcal{B}$ часто позначають $\mathcal{B}^I$ і називають *декартовим* або (*повним*) *прямим степенем* алгебри $\mathcal{B}$.

Вправа 1.4. *Нехай $\mathcal{A}, \mathcal{B}, \mathcal{C}$ — довільні алгебри даної сигнатури Ω. Доведіть, що* *а)* $\mathcal{A} \times \mathcal{B} \simeq \mathcal{B} \times \mathcal{A}$; *б)* $(\mathcal{A} \times \mathcal{B}) \times \mathcal{C} \simeq \mathcal{A} \times (\mathcal{B} \times \mathcal{C})$.

Для кожного $i \in I$ відображення $\pi_i : \prod_{i\in I} \mathcal{A}_i \to \mathcal{A}_i$, $(a_i)_{i\in I} \mapsto a_i$, називається *канонічною проекцією* добутку $\prod_{i\in I} \mathcal{A}_i$ на i-й множник $\mathcal{A}_i$. Очевидно, що π_i є епіморфізмом.

Означення 1.9. *Підалгебра $\mathcal{A}$ прямого добутку $\prod_{i\in I} \mathcal{A}_i$ називається* ***підпрямим добутком*** *алгебр $\mathcal{A}_i$, $i \in I$, якщо проекція $\mathcal{A}$ на кожен множник $\mathcal{A}_i$ збігається із самим множником. Кажуть також, що $\mathcal{A}$* ***розкладається*** *в підпрямий добуток алгебр $\mathcal{A}_i$, $i \in I$. Якщо проекція алгебри $\mathcal{A}$ на якийсь множник $\mathcal{A}_i$ є ізоморфізмом, то підпрямий розклад називається* ***тривіальним****.*

Приклади підпрямих добутків.

1. Повний добуток $\prod_{i\in I} \mathcal{A}_i$.

2. Діагональ $\{(a)_{i\in I} \mid a \in \mathcal{A}\} \subseteq \prod_{i\in I} \mathcal{A}$ алгебри $\mathcal{A}$.

3. Кожна конгруенція на алгебрі $\mathcal{A}$ є підпрямим квадратом алгебри $\mathcal{A}$.

Вправа 1.5. *Чи правильно, що кожен підпрямий квадрат алгебри $\mathcal{A}$ є конгруенцією на алгебрі $\mathcal{A}$?*

Приклади підпрямих розкладів.

1. Тривіальні розклади, коли один із множників збігається з $\mathcal{A}$, а решта — одноелементні.

2. Діагональне занурення $\mathcal{A} \hookrightarrow \prod_{i\in I} A$, $a \mapsto (a)_{i\in I}$.

Вправа 1.6. *Нехай $K = \mathbb{R}[x_1, x_2, x_3, \ldots]$ — кільце дійсних многочленів від зліченної кількості змінних x_1, x_2, x_3, … , I_n — головний ідеал, породжений многочленом x_n, $\psi_n : K \to K/I_n$ — канонічний епіморфізм. Доведіть, що*

а) відображення $K \to \prod_{n\in\mathbb{N}} K/I_n$, $f \mapsto (\psi_n(f))_{n\in\mathbb{N}}$, є мономорфізмом, а тому визначає підпрямий розклад кільця K;

б) підпрямий розклад кільця K із а) є нетривіальним, хоча кожен із множників K/I_n ізоморфний кільцю K.

Приклади груп, які розкладаються в нетривіальний підпрямий добуток, але не розкладаються у прямий.

1. Розглянемо в $S_3 \times S_3$ підгрупу

$$H = \{(\pi, \tau) \mid \pi \text{ і } \tau \text{ мають однакову парність}\}.$$

Тоді H має порядок 18 і є нетривіальним підпрямим квадратом групи S_3. Крім того, H не є абелевою. Тому H не може розкладатися у прямий добуток груп порядків 2 і 9, бо такі групи є абелевими. Отже, якщо H розкладається у прямий добуток, то множники мають порядки 3 і 6. Серед груп порядку 6 неабелевою є тільки S_3. Тому лишається тільки варіант $H \simeq C_3 \times S_3$. Але він також неможливий, бо H має 9 елементів порядку 2, а $C_3 \times S_3$ — лише 3.

2. Занурення $\mathbb{Z} \hookrightarrow \prod_{k\in\mathbb{N}} \mathbb{Z}_k$, $n \mapsto (n \bmod k)_{k\in\mathbb{N}}$ є, очевидно, підпрямим. Але будь-які дві ненульові підгрупи із $\mathbb{Z}$ мають ненульовий перетин. Тому група $\mathbb{Z}$ у нетривіальний прямий добуток не розкладається. (Одночасно отримуємо і приклад кільця, яке розкладається в нетривіальний підпрямий добуток, але не розкладається у прямий.)

Теорема 1.4 (Кляйн–Фрікке)**.** *Нехай $\varphi : A \to F$ і $\psi : B \to F$ — епіморфізми груп. Тоді множина*

$$A \underset{F}{\times} B = \{(a, b) \in A \times B \mid \varphi(a) = \psi(b)\}$$

буде підпрямим добутком груп A і B. Із іншого боку, кожен підпрямий добуток груп A і B має вигляд $A \underset{F}{\times} B$ для відповідно вибраних групи F та епіморфізмів $\varphi : A \to F$ і $\psi : B \to F$.

Доведення. Очевидно, що коли $\varphi(a_1) = \psi(b_1)$ і $\varphi(a_2) = \psi(b_2)$, то маємо $\varphi(a_1 a_2) = \psi(b_1 b_2)$ і $\varphi(a_1^{-1}) = \psi(b_1^{-1})$. Тому множина $A \underset{F}{\times} B$ є підгрупою в $A \times B$. Крім того, позаяк φ і ψ — епіморфізми, то для кожного $a \in A$ існує такий $b \in B$, що $\varphi(a) = \psi(b)$, і навпаки. Тому проекція $A \underset{F}{\times} B$ на кожен множник збігається із самим множником. Це завершує доведення першого твердження теореми.

На рис. 1, де $A_1 = \operatorname{Ker}\varphi$, $B_1 = \operatorname{Ker}\psi$, підпрямий добуток $A \underset{F}{\times} B$ зображено заштрихованими клітинками:

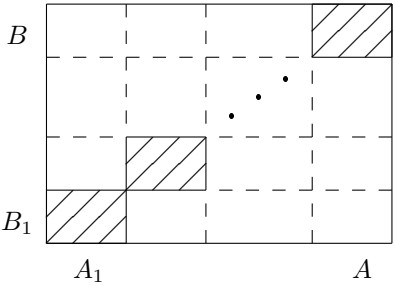


Рис. 1

Нехай тепер $H \leq A \times B$ — підпрямий добуток груп A і B. Ототожнимо елемент $(a, e) \in A \times B$ з елементом $a \in A$ і, аналогічно, елементи (e, b) і $b \in B$. Позначимо $A_1 = H \cap A$, $B_1 = H \cap B$. Позаяк H — підпрямий добуток, то для довільного $a \in A$ знайдеться такий $b \in B$, що $(a, b) \in H$. Але тоді для кожного $a_1 \in A_1$ маємо

$$(a, b)^{-1}(a_1, e)(a, b) = (a^{-1}a_1a, e) \in A_1 .$$

Це означає, що A_1 є нормальною підгрупою в A. Аналогічно доводиться, що B_1 є нормальною підгрупою в B. Тому добуток $A_1 \times B_1$ буде нормальною підгрупою у групі $A \times B$, а тим самим і в підгрупі H, бо $A_1 \times B_1 \leq H$. Канонічний епіморфізм групи H на факторгрупу $H/(A_1 \times B_1)$ позначимо через π.

Для кожного $a \in A$ виберемо такий $b \in B$, що $(a, b) \in H$, і покладемо $\varphi(a) = \pi((a, b))$. Покажемо, що визначене таким чином відображення $\varphi : A \to F$ є епіморфізмом.

Коректність φ: якщо $(a, b_1) \in H$ і $(a, b_2) \in H$, то елемент $(a, b_1)^{-1}(a, b_2) = (e, b_1^{-1}b_2)$ також належить підгрупі H, а тому

$$\pi((a, b_2)) = \pi((a, b_1) \cdot (e, b_1^{-1}b_2)) = \pi((a, b_1)) \cdot \pi((e, b_1^{-1}b_2)) = \pi((a, b_1)) .$$

Отже, $\varphi(a)$ не залежить від вибору елемента $(a, b) \in H$.

Сюр'єктивність φ випливає з того, що $\operatorname{Im}\varphi = \operatorname{Im}\pi$.

Гомоморфність φ також очевидна:

$$\varphi(a_1) \cdot \varphi(a_2) = \pi((a_1, b_1)) \cdot \pi((a_2, b_2)) = \pi((a_1a_2, b_1b_2)) = \varphi(a_1a_2).$$

Аналогічно доводиться, що коли для кожного $b \in B$ вибрати такий $a \in A$, що $(a, b) \in H$, і покласти $\psi(b) = \pi((a, b))$, то відображення $\psi : B \to F$ також є епіморфізмом.

Очевидно, що коли $(a,b) \in H$, то $\varphi(a) = \pi((a,b)) = \psi(b)$. Навпаки, якщо $\varphi(a) = \psi(b)$, то існують такі $b_1 \in B$ і $a_1 \in A$, що елементи (a,b_1) і (a_1,b) належать одному класу суміжності групи H за підгрупою $A_1 \times B_1$. Тоді

$$(a,b_1)^{-1}(a_1,b) = (a^{-1}a_1, b_1^{-1}b) \in A_1 \times B_1\,,$$

звідки $b_1^{-1}b \in B_1$. Але $(a,b) = (a,b_1)(e,b_1^{-1}b)$. Тому $(a,b) \in H$.

Отже, $(a,b) \in H$ тоді й тільки тоді, коли $\varphi(a) = \psi(b)$, тобто $A \underset{F}{\times} B$. $\square$

Вправа 1.7. *Доведіть, що для епіморфізмів φ і ψ із другої частини доведення теореми* 1.4 *виконуються рівності* $\operatorname{Ker}\varphi = A_1$ *і* $\operatorname{Ker}\psi = B_1$.

Теорема 1.5 (Ремак)**.** *Нехай ρ_i, $i \in I$, — довільна родина конгруенцій на універсальній алгебрі $\mathcal{A}$, $\rho = \bigcap\limits_{i\in I} \rho_i$, а $\overline{a_\rho}$ є тим класом конгруенції ρ, який містить елемент a. Тоді відображення*

$$\varphi : \overline{a_\rho} \mapsto (\overline{a_{\rho_i}})_{i\in I}$$

є підпрямим зануренням факторалгебри $\mathcal{A}/\rho$ у прямий добуток $\prod\limits_{i\in I} \mathcal{A}/\rho_i$.

Доведення. Оскільки $\rho \subseteq \rho_i$ для всіх i, то відображення φ визначене коректно. Легко перевіряється, що воно є гомоморфізмом. Зрозуміло, що $\varphi(\overline{a_\rho}) = \varphi(\overline{b_\rho})$ тоді й лише тоді, коли $\overline{a_{\rho_i}} = \overline{b_{\rho_i}}$ для всіх i, тобто тоді й лише тоді, коли $\overline{a_\rho} = \overline{b_\rho}$. Отже, φ є мономорфізмом. Очевидно також, що проекція образу φ на кожен множник $\mathcal{A}/\rho_i$ збігається із самим множником. $\square$

Алгебра $\mathcal{A}$ називається *підпрямо нерозкладною*, якщо кожен її підпрямий розклад є тривіальним.

Теорема 1.6 (Критерій підпрямої розкладності)**.** *Універсальна алгебра $\mathcal{A}$ буде підпрямо розкладною тоді й лише тоді, коли перетин $\bigcap\limits_{i\in I} \rho_i$ усіх її ненульових конгруенцій є нульовою конгруенцією $\mathbf{o}_A$.*

Доведення. Достатність. Нехай ρ_i, $i \in I$, — родина всіх ненульових конгруенцій на алгебрі $\mathcal{A}$ і $\bigcap_{i\in I} \rho_i = \mathbf{o}_A$. Із теореми Ремака випливає, що відображення

$$\varphi : \mathcal{A} \to \prod_{i\in I} \mathcal{A}/\rho_i, \quad a \mapsto (\overline{a_{\rho_i}})_{i\in I},$$

є підпрямим зануренням. Ототожнюючи $\mathcal{A}$ з образом $\varphi(\mathcal{A})$, одержуємо розклад $\mathcal{A}$ у підпрямий добуток алгебр $\mathcal{A}/\rho_i$. Цей розклад є нетривіальним, бо проекція $\mathcal{A}$ на множник $\mathcal{A}/\rho_i$ збігається з канонічним епіморфізмом π_i, а тому не є ізоморфізмом.

Необхідність. Припустимо, що $\mathcal{A} \hookrightarrow \prod_{i\in I} \mathcal{A}_i$, $a \mapsto (a_i)_{i\in I}$, — підпрямий розклад алгебри $\mathcal{A}$. Позаяк для кожного $i \in I$ проекція $\pi_i : \mathcal{A} \to \mathcal{A}_i$ не є ізоморфізмом, то ядро $\operatorname{Ker}\pi_i$ цієї проекції є ненульовою конгруенцією. Але перетин $\rho = \bigcap_{i\in I} \operatorname{Ker}\pi_i$ є нульовою конгруенцією $\mathbf{o}_A$. Справді, якщо a і b — два різні елементи з $\mathcal{A}$, то існує таке i, що $\pi_i(a) \neq \pi_i(b)$. Але тоді $(a,b) \notin \operatorname{Ker}\pi_i$ і $(a,b) \notin \rho$. Оскільки перетин τ всіх ненульових конгруенцій задовольняє включення $\rho \supseteq \tau \supseteq \mathbf{o}_A$, то $\tau = \mathbf{o}_A$. □

Наслідок 1.3. *Універсальна алгебра $\mathcal{A}$ є підпрямо нерозкладною тоді й лише тоді, коли серед ненульових конгруенцій на $\mathcal{A}$ є найменша.*

Звідси і з теореми 1.2 одразу випливає, що група буде підпрямо нерозкладною тоді й лише тоді, коли серед її неодиничних нормальних підгруп є найменша. Аналогічно із задачі 15 випливає, що кільце буде підпрямо нерозкладним тоді й лише тоді, коли серед його ненульових ідеалів є найменший. Зокрема, підпрямо нерозкладними є прості групи (бо вони мають лише одну неодиничну нормальну підгрупу), а також поля й тіла (бо там є лише один ненульовий ідеал).

Задача 1.5. *Доведіть, що такі групи є підпрямо нерозкладними: а) симетричні групи S_n; б) циклічні p-групи.*

Теорема 1.7 (Біркгоф)**.** *Кожна універсальна алгебра $\mathcal{A}$ розкладається у підпрямий добуток підпрямо нерозкладних алгебр.*

Доведення. Для довільної пари (a,b) різних елементів алгебри $\mathcal{A}$ розглянемо множину $\rho(a,b)$ тих конгруенцій на алгебрі $\mathcal{A}$, які розділяють ці елементи, тобто

$$\rho(a,b) := \{\rho \in \operatorname{Con}(\mathcal{A}) \mid \overline{a_\rho} \neq \overline{b_\rho}\}.$$

Множина $\rho(a,b)$, очевидно, не порожня, бо містить нульову конгруенцію, і природно впорядкована за включенням.

Покажемо, що в $\rho(a,b)$ є максимальні за включенням елементи. Згідно з лемою Цорна (див. розділ 3) для цього досить показати, що в $\rho(a,b)$ кожен ланцюг обмежений згори. Розглянемо довільний ланцюг $(\rho_i)_{i\in I}$ конгруенцій із $\rho(a,b)$ (тобто I — лінійно впорядкована множина і $\rho_i \subseteq \rho_j$ для довільних $i < j$) і покладемо $\rho^* = \bigcup\limits_{i\in I} \rho_i$. Очевидно, що ρ^* є відношенням еквівалентності.

Доведемо, що відношення ρ^* є стабільним на алгебрі $\mathcal{A}$. Справді, нехай ω — n-арна дія в $\mathcal{A}$ і $a_1\rho^*b_1, \ldots, a_n\rho^*b_n$. Тоді існують такі $i_1, \ldots, i_n$, що $a_1\rho_{i_1}b_1, \ldots, a_n\rho_{i_n}b_n$. Нехай $i = \max(i_1, \ldots, i_n)$. Тоді $a_1\rho_i b_1, \ldots$ $\ldots, a_n\rho_i b_n$. Позаяк ρ_i — конгруенція, то $\omega(a_1, \ldots, a_n)\rho_i\omega(b_1, \ldots, b_n)$, звідки $\omega(a_1, \ldots, a_n)\rho^*\omega(b_1, \ldots, b_n)$.

Таким чином, відношення ρ^* є конгруенцією на алгебрі $\mathcal{A}$. Воно розділяє елементи a і b, бо пара (a, b) не належить жодній із конгруенцій ρ_i, $i \in I$. Очевидно також, що ρ^* є верхньою гранню ланцюга $(\rho_i)_{i\in I}$. Тому лему Цорна можна застосовувати.

Виберемо в кожній із множин $\rho(a, b)$ якийсь максимальний елемент $\rho^*_{(a,b)}$. Позаяк $\bigcap\limits_{a\neq b} \rho*_{(a,b)} = \mathbf{o}_A$, то з теореми Ремака випливає, що відображення

$$\varphi : x \mapsto (\overline{x_{\rho^*_{(a,b)}}})_{a\neq b}$$

є підпрямим зануренням алгебри $\mathcal{A}$ у прямий добуток $\prod\limits_{a\neq b} \mathcal{A}/\rho^*_{(a,b)}$.

Лишилося показати, що кожна з факторалгебр $\mathcal{A}/\rho^*_{(a,b)}$ є підпрямо нерозкладною. Згідно із другою теоремою про ізоморфізм (задача 1.4) існує взаємно однозначна відповідність між конгруенціями на факторалгебрі $\mathcal{A}/\rho^*_{(a,b)}$ і тими конгруенціями на алгебрі $\mathcal{A}$, які містять конгруенцію $\rho^*(a, b)$. Причому ця відповідність зберігає відношення включення. З означення $\rho^*(a, b)$ випливає, що будь-яка конгруенція, яка строго містить $\rho^*(a, b)$, не розділяє елементи a і b (тобто містить пару (a, b)). Тому й перетин усіх таких конгруенцій міститиме пару (a, b).

Отже, перетин усіх конгруенцій на $\mathcal{A}$, які строго містять конгруенцію $\rho^*(a, b)$, також буде строго містити $\rho^*(a, b)$. Але тоді перетин усіх ненульових конгруенцій на $\mathcal{A}/\rho^*_{(a,b)}$ буде ненульовою конгруенцією, а тому серед ненульових конгруенцій на $\mathcal{A}/\rho^*_{(a,b)}$ є найменша. Тому, за теоремою 1.6, факторалгебра $\mathcal{A}/\rho^*_{(a,b)}$ є підпрямо нерозкладною. □

1.3 Задачі

1. Доведіть, що в кожній алгебрі об'єднання довільного зростаючого ланцюга підалгебр є підалгеброю.
2. Доведіть, що коли сигнатура алгебри містить лише нульарні та унарні операції, то об'єднання довільної родини підалгебр знову буде підалгеброю.
3. Нехай кожне відображення $\omega \in A^A$ розглядається як унарна операція на A. Опишіть усі підалгебри алгебри $\langle A; A^A\rangle$.
4. Нехай A — абелева група. Доведіть, що підалгебри алгебри $\langle A; 0, -\rangle$ — це те ж саме, що й підгрупи групи A.

5. Нехай V — векторний простір над полем P. Знайдіть усі підалгебри алгебри $\langle V;\Omega\rangle$, де $\Omega = \{+,-,0\}\cup T$, якщо a) $T = \mathrm{Hom}(V,V)$; b) $T = GL(V)$; c) $T = \{\lambda E \mid \lambda \in P\}$.

6. Доведіть, що кожна алгебра не більше ніж зліченної сигнатури містить не більше ніж злічену підалгебру.

7. Доведіть, що коли алгебра має ізоморфну собі власну підалгебру, то вона має ізоморфну собі власну надалгебру.

8. Доведіть, що алгебра $\langle\mathbb{N};\cdot\rangle$ має континуум багато підалгебр, а алгебра $\langle\mathbb{N};+\rangle$ — лише зліченну кількість підалгебр.

9. Доведіть, що для кожного $x \in X$ множина $F(\Omega,X)\setminus\{x\}$ є максимальною підалгеброю вільної алгебри $F(\Omega,X)$ і що $F(\Omega,X)$ не має інших максимальних підалгебр.

10. Доведіть, що група автоморфізмів вільної алгебри $F(\Omega,X)$ ізоморфна групі $\mathrm{Sym}(X)$.

11. Нехай кожна власна підалгебра алгебри $\mathcal{A}$ міститься в деякій максимальній підалгебрі, X — система твірних алгебри $\mathcal{A}$, а B — перетин усіх максимальних підалгебр. Доведіть, що для кожного елемента $b \in B\cap X$ множина $X\setminus\{b\}$ також є системою твірних алгебри $\mathcal{A}$.

12. Доведіть, що коли всі конгруенції на алгебрі $\mathcal{A}$ комутують, то конгруенції на будь-якій її факторалгебрі також комутують.

13. Нехай $\mathcal{B}$ — підалгебра алгебри $\mathcal{A}$, $\sim$ — конгруенція на $\mathcal{A}$. Доведіть, що множина $C = \{x \in A \mid \text{існує такий } b \in B, \text{ що } x \sim b\}$ також є підалгеброю алгебри $\mathcal{A}$.

14. Доведіть, що кожна конгруенція на групі однозначно визначається будь-яким своїм класом еквівалентності.

15. Доведіть, що

    a) відношення еквівалентності на асоціативному кільці K буде конгруенцією тоді й лише тоді, коли класи еквівалентності цього відношення є класами суміжності за деяким ідеалом;

    b) відношення еквівалентності на векторному просторі V буде конгруенцією тоді й лише тоді, коли класи еквівалентності цього відношення є класами суміжності за деяким підпростором.

16. Нехай відношення $\varphi \subseteq \mathcal{A}\times\mathcal{B}$ і $\psi \subseteq \mathcal{B}\times\mathcal{C}$ є підалгебрами алгебр $\mathcal{A}\times\mathcal{B}$ і $\mathcal{B}\times\mathcal{C}$ відповідно. Доведіть, що їх деморганівський добуток $\varphi\circ\psi \subseteq \mathcal{A}\times\mathcal{C}$ є підалгеброю алгебри $\mathcal{A}\times\mathcal{C}$.

17. Доведіть, що деморганівський добуток двох конгруенцій на алгебрі $\mathcal{A}$ буде конгруенцією тоді й лише тоді, коли вони комутують.

18. Доведіть, що відношення еквівалентності на алгебрі $\mathcal{A}$ буде конгруенцією тоді й лише тоді, коли воно буде підалгеброю в $\mathcal{A}^2$.

19. a) Нехай θ_i — ядро канонічної проекції алгебри $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ на множник $\mathcal{A}_i$, $i = 1, 2$. Доведіть, що $\theta_1 \cap \theta_2 = \mathbf{o}_A$ і $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1 = \mathcal{A}^2$.

    b) Нехай θ_1 і θ_2 — такі дві конгруенції на алгебрі $\mathcal{A}$, що $\theta_1 \cap \theta_2 = \mathbf{o}_A$ і $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1 = A^2$. Доведіть, що $\mathcal{A} \simeq \mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$.

20. На двоелементній множині $A = \{0, 1\}$ визначимо унарні операції f і g: $f(0) = 0 = g(1), \quad f(1) = 1 = g(0)$. Доведіть, що $\langle A; f\rangle \not\simeq \langle A; g\rangle$, але $\langle A; f\rangle \times \langle A; g\rangle \simeq \langle A; g\rangle \times \langle A; g\rangle$.

21. Доведіть, що $\prod_{(i,j)\in I\times J} \mathcal{A}_{(i,j)} \simeq \prod_{i\in I}\big(\prod_{j\in J} \mathcal{A}_{(i,j)}\big)$.

22. Нехай $\mathcal{A}_i$, $i \in I$, — родина алгебр сигнатури Ω, $\mathcal{A} = \prod_{i\in I} \mathcal{A}_i$, $\pi_i : \mathcal{A} \to \mathcal{A}_i$ — канонічні проекції. Чи завжди існують такі гомоморфізми $\mu_i : \mathcal{A}_i \to \mathcal{A}$, що $\mu_i\pi_i = \mathrm{id}_{A_i}$?

23. Доведіть, що групи D_4 і D_5 є підпрямо нерозкладними.

24. Опишіть усі підпрямо нерозкладні абелеві групи.

2 Напівгрупи

У математиці часто виникають різні сукупності перетворень певних множин, причому так само часто ці сукупності виявляються замкненими відносно композиції перетворень. А композиція перетворень асоціативна. Так у математиці дуже природно з'являються напівгрупи. Неочікуваним є те, що використовуючи лише асоціативність операції, можна створити змістовну й багату теорію з численними застосуваннями. Так виникла й почала активно розвиватися теорія напівгруп. Цікаво, що основоположником теорії напівгруп є український математик Сушкевич.

2.1 Найпростіші властивості

Одним із найпростіших (і найважливіших) прикладів алгебричних систем є *напівгрупа* — довільна непорожня множина S із визначеною на ній асоціативною бінарною дією (тобто $(a*b)*c = a*(b*c)$ для довільних $a, b, c \in S$).

Зазвичай дію в напівгрупі називатимемо *множенням* і дотримуватимемося *мультиплікативних* позначень і термінології. Зокрема, дію позначатимемо символом $\cdot$, а результат $a \cdot b$ (або просто ab) її застосування до елементів a і b називатимемо *добутком* цих елементів.

Якщо бінарна дія на множині S визначається не яким-небудь "хорошим" правилом, а, наприклад, таблицею множення, то перевірка її асоціативності вимагає справдження $|S|^3$ рівностей і є досить громіздкою процедурою. Як випливає з наступної теореми, суттєво зменшити об'єм обчислень у загальному випадку не можна.

Теорема 2.1 (Сас, 1953). *Якщо $|S| > 3$, то для довільної наперед заданої впорядкованої трійки (a, b, c) елементів із S можна таким чином визначити бінарну дію $*$ на S, що для довільної відмінної від (a, b, c) трійки (x, y, z) елементів із S рівність $(x * y) * z = x * (y * z)$ виконується, але $(a * b) * c \neq a * (b * c)$.*

Елемент e напівгрупи S називається *ідемпотентом*, якщо $e \cdot e = e$. Множина всіх ідемпотентів напівгрупи S позначається $E(S)$. Кількість ідемпотентів у напівгрупі може варіювати у дуже широких межах. Наприклад, у напівгрупах $\langle \mathbb{N}; + \rangle$ і $\langle 2\mathbb{N}; \cdot \rangle$ ідемпотентів нема взагалі. З іншого боку, у напівгрупі $\langle 2^M; \cup \rangle$ усіх підмножин множини M відносно об'єднання (або в аналогічній напівгрупі $\langle 2^M; \cap \rangle$) кожен елемент є ідемпотентом. Напівгрупи останнього типу називають *ідемпотентними* або *зв'язками*.

Елемент $e \in S$ називається *лівим нейтральним елементом* (або *лівою одиницею*) напівгрупи S, якщо $e \cdot a = a$ для всіх $a \in S$. Аналогічно визначається *правий нейтральний елемент* (або *права одиниця*).

Елемент $o \in S$ називається *лівим нулем* напівгрупи S, якщо $o \cdot a = o$ для всіх $a \in S$. Аналогічно визначається *правий нуль*.

Очевидно, що ліві та праві нулі й одиниці є ідемпотентами. Їхня кількість також може варіювати в широких межах. Однак, якщо одночасно є і ліві, і праві одиниці (або ліві та праві нулі), то ситуація принципово інша.

Лема 2.1. *Якщо напігрупа S містить ліву одиницю e_l і праву одиницю e_r (відповідно лівий нуль o_l і правий нуль o_r), то вони збігаються: $e_l = e_r$ (відповідно $o_l = o_r$).*

Доведення. $e_r = e_l \cdot e_r = e_l, \quad o_l = o_l \cdot o_r = o_r$. □

Таким чином, якщо напівгрупа містить і ліві, і праві одиниці, то насправді вона містить одну-єдину одиницю, яка буде *двосторонньою*, тобто і лівою, і правою. У цьому випадку говорять просто про *одиницю* (або *нейтральний елемент*) напівгрупи і позначають його 1. Відповідно двосторонній нуль позначають 0.

Напівгрупу з одиницею часто називають *моноїдом*.

Якщо напівгрупа не містить одиниці, то цей "недолік" можна легко усунути, приєднавши одиницю силоміць. Це робиться таким чином:

Твердження 2.1. *Нехай $\langle S; * \rangle$ — напівгрупа, а e — новий елемент, що не належить S. Довизначимо операцію $*$ на множину $S \cup \{e\}$, поклавши $a * e = e * a = a$ для довільного $a \in S$ та $e * e = e$. Тоді $S \cup \{e\}$ з операцією $*$ є напівгрупою, в якій елемент e є одиницею.*

Доведення. Позаяк на S операція $*$ є асоціативною, то досить перевірити асоціативний закон $(a * b) * c = a * (b * c)$ лише для тих трійок a, b, c, в яких принаймні одна з компонент збігається з e (зробіть це!). Нейтральність елемента e очевидна. □

Аналогічно до напівгрупи можна приєднати і нуль:

Твердження 2.2. *Нехай $\langle S; * \rangle$ — напівгрупа, а o — новий елемент, що не належить S. Довизначимо операцію $*$ на множину $S \cup \{o\}$, поклавши $a * o = o * a = o$ для довільного $a \in S$ та $o * o = o$. Тоді $S \cup \{o\}$ з операцією $*$ є напівгрупою, в якій елемент o є нулем.*

Для довільної напівгрупи S через S^1 позначатимемо саму S, якщо вона має одиницю, і S з приєднаною одиницею у противному разі. Аналогічний зміст у випадку нуля має позначення S^0. (Не можна плутати S^0 і S^1 із множиною $S^k = \{a_1 a_2 \cdots a_k \mid a_i \in S\}$ $(k > 1)$ та з k-м декартовим степенем множини S.)

2.2 Основні приклади

У цьому розділі X — фіксована непорожня множина.

1. Вільна напівгрупа $F(X)$ і вільний моноїд X^*. Назвемо елементи множини X *буквами*, а саму множину X — *алфавітом*. На множині всіх скінченних слів (тобто послідовностей букв) над алфавітом X визначимо операцію приписування слів (її ще називають *конкатенацією*):

$$a_1 a_2 \dots a_k \cdot b_1 b_2 \dots b_m = a_1 a_2 \dots a_k b_1 b_2 \dots b_m \ ,$$

яка очевидним чином асоціативна. Отримана напівгрупа називається *вільною напівгрупою* над алфавітом X і позначається $F(X)$ або X^+. Очевидно, що $F(X)$ не містить жодного ідемпотента.

Приєднанням до $F(X)$ одиниці отримують так званий *вільний моноїд* X^* над алфавітом X. Приєднану одиницю в цьому випадку зручно інтерпретувати як *порожнє слово* (тобто слово без букв).

2. Напівгрупа з нульовим множенням. Нехай 0 — виділений елемент множини X. Для довільних $a, b \in X$ покладемо $a * b = 0$. Очевидно, що дія $*$ асоціативна. Елемент 0 є нулем цієї напівгрупи.

3. Напівгрупа з лівим (правим) множенням. Правило $a * b = a$ (відповідно $a * b = b$) визначає на множині X асоціативну дію (перевірте!). Отримана напівгрупа називається *напівгрупою з лівим* (відповідно *правим*) *множенням* і позначається X^l (відповідно X^r).

У напівгрупі X^l кожен елемент буде лівим нулем і правою одиницею. Аналогічно в X^r кожен елемент буде правим нулем і лівою одиницею. Тому X^l називають ще *напівгрупою лівих нулів*, а X^r — *правих нулів*.

4. Прямокутна зв'язка. Для довільних множин A і B на їхньому декартовому добуткові $A \times B$ можна визначити дію $(a, b)(c, d) = (a, d)$. Отримана напівгрупа називається *прямокутною зв'язкою*. Очевидно, що всі її елементи є ідемпотентами. Термін "прямокутна" пов'язаний із геометричною інтерпретацією декартового добутку.

5. Симетрична напівгрупа $\mathcal{T}(X)$. Множина $\mathcal{T}(X)$ усіх перетворень множини X (тобто всіх відображень із X в X) відносно природної композиції перетворень $(\varphi\cdot\psi)(x) = \psi(\varphi(x))$ (зауважте, що перетворення виконуються `зліва направо`), утворює напівгрупу, яка називається *симетричною напівгрупою* всіх перетворень множини X. Елементи $\mathcal{T}(X)$ зручно записувати у вигляді дворядкових таблиць $\varphi = \begin{pmatrix} x \\ \varphi(x) \end{pmatrix}_{x\in X}$, бо при такому записі композиція елементів обчислюється за звичайним правилом множення підстановок. Напівгрупа $\mathcal{T}(X)$ має одиницю — тотожне перетворення $e = \begin{pmatrix} x \\ x \end{pmatrix}_{x\in X}$. Якщо $|X| = n$, то $|\mathcal{T}(X)| = n^n$.

Поруч із $\varphi(x)$ для образу елемента x під дією перетворення φ часто вживають позначення x^φ. Зокрема, тоді $(x^\varphi)^\psi = x^{\varphi\psi}$. Ми також використовуватимемо це позначення.

Якщо перетворення виконувати `справа наліво`: $(\varphi\circ\psi)(x) = \varphi(\psi(x))$, то одержимо *двоїсту симетричну напівгрупу* $\overleftarrow{\mathcal{T}(X)}$.

6. Напівгрупа $\mathcal{PT}(X)$ усіх часткових перетворень множини X. Відображення φ з X в $X\cup\{\varnothing\}$ називатимемо *частковим перетворенням* множини X, а множину $\operatorname{dom}\varphi = \{x\in X \mid \varphi(x)\neq\varnothing\}$ — *областю визначення* часткового перетворення φ. Множина $\operatorname{ran}\varphi = \{\varphi(x) \mid x\in\operatorname{dom}\varphi\}$ називається *областю значень* перетворення φ. Якщо $\varphi(x) = \varnothing$, то вважатимемо, що перетворення φ в точці x не визначене. Множину всіх часткових перетворень множини X позначимо через $\mathcal{PT}(X)$.

Термін "часткове перетворення" пояснюється просто: φ можна розглядати як відображення з $\operatorname{dom}\varphi$ в X.

Природно визначається композиція $\varphi\circ\psi$ часткових перетворень: $(\varphi\circ\psi)(x) = \psi(\varphi(x))$, якщо $\varphi(x)\in\operatorname{dom}\psi$, і $(\varphi\circ\psi)(x) = \varnothing$ в іншому випадку. Легко бачити, що композиція є асоціативною.

Як і у випадку $\mathcal{T}(X)$, елементи $\mathcal{PT}(X)$ зручно записувати у вигляді дворядкових таблиць. Тоді їхня композиція обчислюється звичайним чином, наприклад,

$$\begin{pmatrix} 1 & 2 & 3 \\ \varnothing & 1 & 1 \end{pmatrix}\circ\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & \varnothing \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \varnothing & 2 & 2 \end{pmatrix}.$$

Напівгрупа $\mathcal{PT}(X)$ містить одиницю — тотожне перетворення множини X, і нуль — ніде не визначене перетворення. Якщо $|X| = n$, то її порядок дорівнює $(n+1)^n$.

Вправа 2.1. *Доведіть, що для довільних $\alpha,\beta\in\mathcal{PT}(X)$ виконуються включення* $\operatorname{dom}(\alpha\beta)\subseteq\operatorname{dom}\alpha$, $\operatorname{ran}(\alpha\beta)\subseteq\operatorname{ran}\beta$.

7. Симетрична інверсна напівгрупа $\mathcal{IS}(X)$. Виділимо в $\mathcal{PT}(X)$ підмножину $\mathcal{IS}(X)$ ін'єктивних часткових перетворень, тобто таких елементів $\varphi \in \mathcal{PT}(X)$, що для всіх $x \neq y$ із $\operatorname{dom}\varphi$ виконується нерівність $\varphi(x) \neq \varphi(y)$. Очевидно, що композиція часткових ін'єкцій знову є частковою ін'єкцією, тому $\mathcal{IS}(X)$ є піднапівгрупою напівгрупи $\mathcal{PT}(X)$. $\mathcal{IS}(X)$ називається *інверсною симетричною напівгрупою на множині* X, а її елементи — *частковими підстановками* на множині X.

8. Напівгрупа $\mathcal{B}(X)$ бінарних відношень на множині X. Нагадаємо, що бінарним відношенням на множині X називається довільна підмножина множини $X \times X$. Композиція $\varphi \circ \psi$ (її ще називають *деморганівським добутком*) бінарних відношень φ і ψ визначається так:

$$\varphi \circ \psi = \{(x, y) \ : \text{ існує такий } z \in X, \text{ що } (x, z) \in \varphi \text{ і } (z, y) \in \psi\}.$$

Відносно цієї дії множина $\mathcal{B}(X)$ всіх бінарних відношень на X утворює напівгрупу, одиницею якої є відношення рівності (перевірте!). Очевидно, що для n-елементної множини X порядок напівгрупи $\mathcal{B}(X)$ дорівнює 2^{n^2}.

Усі наведені вище напівгрупи перетворень множини X природно занурюються в напівгрупу $\mathcal{B}(X)$. Справді, із кожним (частковим) перетворенням $f : X \to X$ множини X природно пов'язується бінарне відношення $\varphi_f = \{(x, f(x)) \mid x \in \operatorname{dom} f\}$ і відображення $f \mapsto \varphi_f$ є ін'єктивним. Якщо тепер f і g — два (часткові) перетворення множини X, то пара (x, y) належить добуткові $\varphi_f \circ \varphi_g$ тоді й лише тоді, коли існує таке z, що $z = f(x)$ і $y = g(z)$, тобто коли $y = (fg)(x)$. Таким чином, $\varphi_f \circ \varphi_g = \varphi_{fg}$. Отже, відображення $f \mapsto \varphi_f$ є зануренням напівгрупи $\mathcal{PT}(X)$ у $\mathcal{B}(X)$.

Описане занурення $\mathcal{PT}(X) \hookrightarrow \mathcal{B}(X)$ підказує інтерпретацію бінарного відношення $\varphi \in \mathcal{B}(X)$ як "багатозначного" перетворення множини X. При такій інтерпретації φ зручно записувати у вигляді $\varphi = \begin{pmatrix} x \\ A_x \end{pmatrix}_{x \in X}$, де $A_x = \{y \in X \mid (x, y) \in \varphi\}$. Тоді множення бінарних відношень природно перетворюється в композицію таких "багатозначних" перетворень.

Елемент φ напівгрупи $\mathcal{B}(X)$ можна також зображувати орієнтованим графом із множиною вершин X: граф Γ_φ містить стрілку з a в b тоді й лише тоді, коли $(a, b) \in \varphi$. Якщо $X = \{1, 2, \ldots, n\}$, то елементи з $\mathcal{B}(X)$ інколи зручно зображувати $(0,1)$-матрицями порядку n: у матриці $A_\varphi = (a_{ij})$ кладемо $a_{ij} = 1$ тоді й лише тоді, коли $(i, j) \in \varphi$.

Вправа 2.2. *Як знайти матрицю $A_{\varphi\circ\psi}$ добутку $\varphi \circ \psi$, якщо відомі матриці A_φ і A_ψ?*

Зауваження. Якщо $X = \{1, 2, \ldots, n\}$, то напівгрупи $F(X)$, $\mathcal{T}(X)$, $\mathcal{PT}(X)$, $\mathcal{IS}(X)$, $\mathcal{B}(X)$ також позначатимемо F_n, $\mathcal{T}_n$, $\mathcal{PT}_n$, $\mathcal{IS}_n$, $\mathcal{B}_n$ відповідно.

9. Напівгрупа Брауера $\mathfrak{B}_n$. У 1937 р. Брауер побудував цікаву і "незвичну" напівгрупу, яка відіграє важливу роль у теорії зображень і на його честь позначається $\mathfrak{B}_n$. Її елементами є усі можливі розбиття множини $\{1, 2, \ldots, n, 1', 2', \ldots, n'\}$ (n фіксоване) на двоелементні підмножини. Елементи напівгрупи $\mathfrak{B}_n$ часто називають *чипами*, оскільки їх зручно зображувати у вигляді чипів, ліві ніжки яких відповідають нештрихованим числам, а праві — штрихованим, причому ніжки попарно з'єднані. Правило множення чипів легко зрозуміти з рис. 2: спочатку штриховані ніжки першого чипа з'єднуємо з відповідними нештрихованими ніжками другого. Це призводить до утворення ланцюгів, кінцями яких будуть ліві ніжки першого чипа та праві ніжки другого (причому всі такі ніжки будуть кінцями якихось ланцюгів) і, можливо, циклів, які містять лише праві ніжки першого чипа і ліві другого. Після цього кінці кожного ланцюга з'єднуємо безпосередньо, а праві ніжки першого чипа і ліві другого викидаємо. У результаті знову одержуємо чип, який і є добутком двох даних.

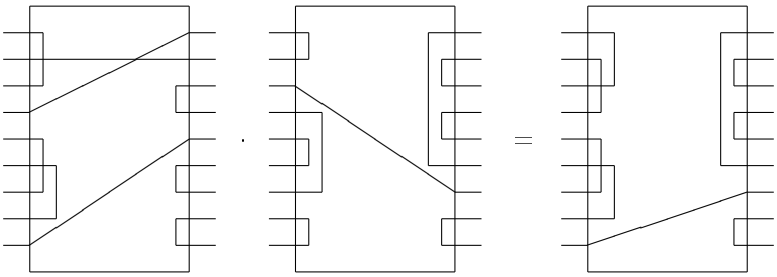


Рис. 2. Множення чипів

Асоціативність множення очевидна. Нейтральним елементом напівгрупи $\mathfrak{B}_n$ є розбиття на множини $\{1, 1'\}$, $\{2, 2'\}$, $\ldots$, $\{n, n'\}$.

10. Напівгрупа-степінь $\mathcal{P}(S)$. Ця напівгрупа є частковим випадком глобальної надалгебри. Нехай S — напівгрупа. На множині $\mathcal{P}(S)$ всіх підмножин напівгрупи S визначаємо множення:

$$A \cdot B = \{ab \ : \ a \in A, b \in B\}.$$

Легко перевіряється, що це множення асоціативне. Отримана таким чином напівгрупа $\mathcal{P}(S)$ називається *напівгрупою-степенем* або *глобальною наднапівгрупою* напівгрупи S. Вона містить нуль (ним буде порожня підмножина $\varnothing$).

Вправа 2.3. *$\mathcal{P}(S)$ буде напівгрупою з одиницею тоді й лише тоді, коли S — напівгрупа з одиницею.*

Оскільки добуток непорожніх підмножин теж буде непорожньою підмножиною, то нуль $\varnothing$ у напівгрупі $\mathcal{P}(S)$ є приєднаним. Піднапівгрупу $\mathcal{P}(S) \setminus \{\varnothing\}$ позначатимемо $\mathcal{P}^+(S)$.

11. Факторстепінь напівгрупи перетворень. Нехай S є напівгрупою (часткових) перетворень множини X (тобто піднапівгрупою напівгрупи $\mathcal{T}(X)$ або $\mathcal{PT}(X)$). Для довільних $Y \subseteq X$ і $A \subseteq S$ покладемо $A(Y) = \{a(y) \ : \ a \in A,\ y \in Y\}$ і визначимо на напівгрупі-степені $\mathcal{P}(S)$ таке відношення $\sim$:

$$A \sim B \ \Leftrightarrow \ A(x) = B(x) \ \text{ для всіх } \ x \in X\,.$$

Лема 2.2. *Відношення $\sim$ є конгруенцією на $\mathcal{P}(S)$.*

Доведення. Очевидно, що $\sim$ є відношенням еквівалентності. Нехай тепер $A \sim A_1$ і $B \sim B_1$. Тоді для довільного $x \in X$ маємо

$$(A \cdot B)(x) = B(A(x)) = B(A_1(x)) = B_1(A_1(x)) = (A_1 \cdot B_1)(x)\,,$$

тобто $A \cdot B \sim A_1 \cdot B_1$. Отже, $\sim$ є конгруенцією на $\mathcal{P}(S)$. □

Факторнапівгрупа $\mathcal{P}(S)/\sim$ називається *факторстепенем* напівгрупи перетворень S і позначається $\mathcal{FP}(S)$.

Позначимо через $\overline{A}$ той клас еквівалентності відношення $\sim$, в який попадає елемент $A \in \mathcal{P}(S)$. Очевидно, що клас $\overline{\{\varnothing\}}$ є нулем факторстепеня $\mathcal{FP}(S)$. Якщо напівгрупа S не містить ніде не визначеного перетворення (зокрема, якщо $S \subseteq \mathcal{T}(X)$), то $\overline{\{\varnothing\}} = \{\varnothing\}$ і нуль напівгрупи $\mathcal{FP}(S)$ є приєднаним. У цьому випадку його можна відкинути й розглядати напівгрупу $\mathcal{FP}^+(S) = \mathcal{FP}(S) \setminus \{\varnothing\}$, яка теж називається факторстепенем напівгрупи S.

Для довільного $A \in \mathcal{P}(S)$ елемент $\overline{A}$ факторстепеня $\mathcal{FP}(S)$ можна записувати у вигляді

$$\overline{A} = \binom{x}{A(x)}_{x \in X}\,. \tag{2.1}$$

Цей запис нагадує традиційний запис підстановок і зручний для виконання множення:

$$\begin{pmatrix} x \\ A(x) \end{pmatrix}_{x\in X} \cdot \begin{pmatrix} x \\ A(x) \end{pmatrix}_{x\in X} = \begin{pmatrix} x \\ \bigcup\limits_{y\in A(x)} B(y) \end{pmatrix}. \tag{2.2}$$

2.3 Зв'язок з універсальними алгебрами

Доцільність вивчення напівгруп більше ніж переконливо мотивується тим, що множина $\operatorname{End} A$ ендоморфізмів довільної універсальної алгебри A утворює напівгрупу відносно композиції. Із точністю до ізоморфізму такими напівгрупами фактично все й вичерпується.

Теорема 2.2. *Кожна напівгрупа S з одиницею ізоморфна напівгрупі* $\operatorname{End}\mathcal{S}$ *усіх ендоморфізмів деякої універсальної алгебри $\mathcal{S}$ із носієм S.*

Доведення. Кожному елементу $a \in S$ зіставимо унарну дію $\omega_a : S \to S$, $\omega_a(x) = ax$. Покладемо $\mathcal{S} = (S; (\omega_a)_{a\in S})$. Далі кожному $b \in S$ зіставимо перетворення $\varphi_b : S \to S$, $x \mapsto xb$. Позаяк

$$\varphi_b(\omega_a(x)) = axb = \omega_a(\varphi_b(x)),$$

то $\varphi_b \in \operatorname{End}\mathcal{S}$.

Покажемо, що відображення $\Phi : S \to \operatorname{End}\mathcal{S}$, $b \mapsto \varphi_b$, є ізоморфізмом. Справді, $\varphi_b(1) = b$. Тому якщо $b_1 \neq b_2$, то $\varphi_{b_1} \neq \varphi_{b_2}$. Отже, відображення Φ є ін'єктивним. З іншого боку, нехай $\varphi \in \operatorname{End}\mathcal{S}$ і $\varphi(1) = b$. Тоді для довільного x

$$\varphi(x) = \varphi(x \cdot 1) = \varphi(\omega_x(1)) = \omega_x(\varphi(1)) = \omega_x(b) = xb = \varphi_b(x),$$

тобто $\varphi = \varphi_b$. Отже, відображення Φ є сюр'єктивним. Нарешті, із рівностей

$$\varphi_{ab}(x) = xab = xa \cdot b = \varphi_b(\varphi_a(x)) = (\varphi_a \cdot \varphi_b)(x)$$

випливає, що відображення Φ є гомоморфізмом. □

Наслідок 2.1. *Кожна група G ізоморфна групі всіх автоморфізмів деякої універсальної алгебри з носієм G.*

Наслідок 2.2 (Теорема Келі)**. 1.** *Кожна напівгрупа S з одиницею ізоморфна деякій піднапівгрупі з $\mathcal{T}(S)$.*

2. *Кожна група G ізоморфна деякій підгрупі симетричної групи* $\operatorname{Sym}(G)$.

Нехай Ω — сигнатура, T — напівгрупа. Кожному символу $\omega \in \Omega$ зіставимо фіксований елемент $a_\omega \in T$, і якщо ω має арність n, то розглянемо на T n-арну операцію

$$(x_1, x_2, \ldots, x_n) \mapsto x_1 x_2 \cdots x_n a_\omega \,.$$

Таким чином на напівгрупі T індукується так звана *спеціальна похідна алгебра сигнатури* Ω.

Теорема 2.3 (Кон–Ребане)**.** *Кожна універсальна алгебра $\mathcal{A}$ сигнатури Ω ізоморфно занурюється в деяку спеціальну похідну алгебру сигнатури Ω на певній напівгрупі S.*

Доведення. Нехай Ω_0 — множина всіх 0-арних символів з Ω. Розглянемо множину M усіх скінченних наборів

$$(\alpha_1, \ldots, \alpha_k), \quad k \geq 1, \quad \alpha_1, \ldots, \alpha_k \in A \cup (\Omega \setminus \Omega_0)\,,$$

які задовольняють таку умову:

якщо в наборі $(\alpha_1, \ldots, \alpha_k)$ зустрічається символ $\omega \in \Omega$ арності n, то перед ним не може стояти n елементів множини A.

За напівгрупу S візьмемо симетричну напівгрупу $\mathcal{T}(M)$ усіх перетворень множини M.

Кожному символу $\omega \in \Omega$ поставимо у відповідність перетворення $\varphi_\omega \in \mathcal{T}(M)$ за правилом:

— якщо $(\alpha_1, \ldots, \alpha_k) \in M$ і $\omega \in \Omega_0$, то

$$(\alpha_1, \ldots, \alpha_k)^{\varphi_\omega} = (\alpha_1, \ldots, \alpha_k, a_\omega),$$

де a_ω — відповідна константа з $\mathcal{A}$;

— якщо ж $\omega \in (\Omega \setminus \Omega_0)$, то

$$(\alpha_1, \ldots, \alpha_k)^{\varphi_\omega} = \begin{cases} (\alpha_1, \ldots, \alpha_k, \omega), & \text{якщо цей набір} \\ & \text{належить } M; \\ (\alpha_1, \ldots, \alpha_{k-n}, \omega(\alpha_{k-n+1}, \ldots, \alpha_k)) & \text{у противному разі.} \end{cases}$$

Відображення $\omega \mapsto \varphi_\omega$ дозволяє визначити на $\mathcal{T}(M)$ спеціальну похідну алгебру сигнатури Ω. Розглянемо тепер відображення

$$\psi : \mathcal{A} \to \mathcal{T}(M), \quad a \mapsto \psi(a),$$

де перетворення $\psi(a)$ визначається правилом

$$(\alpha_1, \ldots, \alpha_k)^{\psi(a)} = (\alpha_1, \ldots, \alpha_k, a)\,.$$

Очевидно, що ψ є ін'єкцією і зберігає 0-арні операції. Нехай тепер ω — операція арності $n > 0$. Тоді

$$(\alpha_1, \ldots, \alpha_k)^{\psi(\omega(a_1,\ldots,a_n))} = (\alpha_1, \ldots, \alpha_k, \omega(a_1, \ldots, a_n)) =$$
$$= (\alpha_1, \ldots, \alpha_k)^{\psi(a_1)\cdots\psi(a_n)\cdot\varphi_\omega}.$$

Отже, операції додатної арності також зберігаються. Тому ψ — мономорфізм. □

Таким чином, у певному сенсі теорія напівгруп містить у собі всю загальну алгебру.

2.4 Циклічні напівгрупи

Означення 2.1. *Множина $\langle a\rangle = \{a, a^2, a^3, \ldots\}$ усіх степенів елемента a утворює напівгрупу, яка називається* ***моногенною*** *(****циклічною****) напівгрупою, породженою елементом a. Число $|\langle a\rangle|$ називається* ***порядком*** *елемента a і позначається $|a|$.*

Напівгрупа називається *періодичною*, якщо всі її елементи мають скінченний порядок.

Якщо $|a| < \infty$, то нехай n — найменше натуральне число, для якого елемент a^n зустрічається в послідовності $a, a^2, a^3, \ldots$ більше одного разу, а k — найменше натуральне число, для якого $a^n = a^{n+k}$. Число n називається *індексом*, k — *періодом*, а пара (n, k) — *типом* елемента a і моногенної напівгрупи $\langle a\rangle$. Очевидно, що $n+k = |a|+1$ і що ідемпотенти мають тип $(1, 1)$.

Вправа 2.4. *У моногенній напівгрупі типу (n, k) виконується рівність $a^{n+i} \cdot a^{n+j} = a^{n+l}$, де $l = (n + i + j) \bmod k$.*

Теорема 2.4 (Фробеніус, 1895)**.**

1. *Всі нескінченні моногенні напівгрупи ізоморфні між собою.*

2. *Для довільних $1 \le n, k < \infty$ існує скінченна моногенна напівгрупа типу (n, k).*

3. *У моногенній напівгрупі $\langle a\rangle$ типу (n, k) множина елементів $G_a = \{a^n, a^{n+1}, \ldots, a^{n+k-1}\}$ утворює циклічну підгрупу, яка є максимальною підгрупою напівгрупи $\langle a\rangle$.*

4. *Дві скінченні моногенні напівгрупи ізоморфні тоді й лише тоді, коли їхні типи збігаються.*

5. *Єдиним ідемпотентом моногенної напівгрупи $\langle a\rangle$ типу (n, k) (і одиницею підгрупи G_a) буде a^{n+i}, де $i = -n \bmod k$.*

Доведення. 1. Нехай $\langle a\rangle = \{a, a^2, a^3, \ldots\}$ і $\langle b\rangle = \{b, b^2, b^3, \ldots\}$ — дві нескінченні моногенні напівгрупи. Тоді відображення $a^k \mapsto b^k$ $(k \geq 1)$ буде, очевидно, ізоморфізмом.

2. Моногенна напівгрупа, породжена елементом

$$a = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & k+2 & \cdots & k+n-1 & k+n \\ 2 & 3 & \cdots & k & 1 & k+2 & k+3 & \cdots & k+n & \varnothing \end{pmatrix}$$

із $\mathcal{IS}_{n+k}$ або елементом

$$b = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & k+2 & \cdots & k+n-1 & k+n & k+n+1 \\ 2 & 3 & \cdots & k & 1 & k+2 & k+3 & \cdots & k+n & k+n+1 & k+n+1 \end{pmatrix}$$

із $\mathcal{T}_{n+k}$, має тип (n, k).

3. Із означення типу моногенної напівгрупи випливає, що множина G_a замкнена відносно множення. Тому для доведення першої частини твердження досить переконатися, що відображення $\varphi : G_a \to \mathbb{Z}_k$, $a^i \mapsto i + k\mathbb{Z}$, є ізоморфізмом. Позаяк показники елементів із G_a — це k послідовних натуральних чисел, то відображення φ є взаємно однозначним. Тому треба перевірити лише гомоморфність. Але вона випливає з вправи 2.4, позаяк

$$(n+i+k\mathbb{Z})+(n+j+k\mathbb{Z}) = n+(n+i+j)+k\mathbb{Z} = n+(n+i+j) \bmod k + k\mathbb{Z}\,.$$

З іншого боку, напівгрупа $\langle a\rangle$ є скінченною, тому кожен елемент b, який належить якійсь із її підгруп, має скінченний порядок. Зокрема, існує таке натуральне число m, що $b^m = b$. Елементи $a, a^2, \ldots, a^{n-1}$ такої властивості не мають, тому вони не належать жодній підгрупі. Отже, підгрупа G_a є максимальною.

4. Якщо

$$\langle a\rangle = \{a, a^2, \ldots, a^n, a^{n+1}, a^{n+k-1}\} \quad \text{і} \quad \langle b\rangle = \{b, b^2, \ldots, b^n, b^{n+1}, b^{n+k-1}\}$$

— дві моногенні напівгрупи типу (n, k), то відображення $a^k \mapsto b^k$, $1 \leq k < n + k$, буде ізоморфізмом.

Навпаки, нехай дві моногенні напівгрупи ізоморфні. Якщо вони групи, то однаковість типів очевидна. Якщо ж моногенна напівгрупа не є групою, то вона має лише один твірний елемент, а тому її тип визначається однозначно.

5. Очевидно, що жоден з елементів $a, a^2, \ldots, a^{n-1}$ не є ідемпотентом. Тому ідемпотенти треба шукати лише серед елементів із G_a. Із правила множення елементів підгрупи G_a (вправа 2.4) випливає, що елемент a^{n+i} буде ідемпотентом тоді й лише тоді, коли $i \equiv n + i + i (\bmod k)$, тобто коли $i = -n \bmod k$. Оскільки в групі тільки один ідемпотент — її одиниця e — то це завершує доведення теореми. □

Наслідок 2.3. **1.** *Моногенна напівгрупа* $\langle a\rangle$ *є напівгрупою з одиницею тоді й лише тоді, коли вона є групою.*

2. *Існує рівно* m *попарно неізоморфних моногенних напівгруп порядку* m*.*

Доведення. 1. Єдиний ідемпотент напівгрупи $\langle a\rangle$ типу (n,k) має вигляд a^{n+i}, де $i \geq 0$. Але для довільного $m < n$

$$a^m \cdot a^{n+i} = a^{n+\,(m+i) \bmod k} \neq a^m\,.$$

Отже, для наявності одиниці необхідно, щоб було $n = 1$, тобто щоб напівгрупа $\langle a\rangle$ була групою. Достатність умови очевидна.

2. Для напівгрупи $\langle a\rangle$ типу (n,k) і порядку m маємо: $m+1 = n+k$. Очевидно, що записати число $m+1$ у вигляді впорядкованої суми двох натуральних чисел n і k можна рівно m способами. □

Наслідок 2.4. *У періодичній (зокрема, скінченній) напівгрупі кожний елемент у деякому степені буде ідемпотентом. Зокрема, кожна скінченна напівгрупа містить ідемпотент.*

Зауваження. 1. Фробеніус доводив свою теорему для напівгруп, породжених елементами глобальної наднапівгрупи $\mathcal{P}(G)$ скінченної групи G. Але зрозуміло, що конкретна природа твірного елемента a не відіграє жодної ролі. Тому його теорема є правильною для довільних моногенних напівгруп.

2. У 30—40-х рр. XX ст. теорема Фробеніуса не раз перевідкривалася (деталі див. в [5], с. 39). Та й пізніше з'являлися роботи, в яких пропонувалися "нові" доведення цієї теореми[1].

2.5 Підгрупи та ідеали

Нехай S — напівгрупа з одиницею e. Елемент a називається *оборотним зліва* (*справа*), якщо існує такий елемент b, що $ba = e$ ($ab = e$), і просто *оборотним*, якщо він є оборотним і зліва, і справа. Легко зрозуміти, що множина S^* оборотних елементів напівгрупи S утворює групу.

Якщо e — довільний ідемпотент, то множина всіх елементів із S, для яких e є двосторонньою одиницею, збігається з eSe і є піднапівгрупою. Підгрупу оборотних елементів з eSe позначимо через H_e, тобто $H_e = (eSe)^*$.

[1] Одна з останніх — Lipscomb S. L. Cyclic subsemigroups of symmetric inverse semigroups / S. L. Lipscomb // Semigroups Forum — **34**. — 1986. — P. 243–248.

Теорема 2.5. *Якщо G — підгрупа напівгрупи S і для деякого ідемпотента e $G \cap H_e \neq \varnothing$, то $G \subseteq H_e$.*

Доведення. Якщо $a \in G \cap H_e$, то e є для a двосторонньою одиницею. Позаяк для довільного $g \in G$ існують такі елементи $x, y \in G$, що $g = ax$ і $g = ya$, то $eg = e \cdot ax = ea \cdot x = ax = g$ і $ge = ya \cdot e = g$. Отже, $ege = g$ і $g \in eSe$.

З іншого боку, існують такі елементи $u, v \in G$, що $a = ug$ і $a = gv$. Нехай a^{-1} — елемент, обернений до a у групі H_e. Тоді $a^{-1}u \cdot g = g \cdot va^{-1} = e$, звідки випливає, що $g \in H_e$. Оскільки елемент $g \in G$ — довільний, то $G \subseteq H_e$. □

Наслідок 2.5. **1.** *У напівгрупі S кожна підгрупа H_e, $e \in E(S)$, є максимальною і кожна максимальна підгрупа має такий вигляд.*

2. *Якщо $e \neq f$, то $H_e \cap H_f = \varnothing$.*

Доведення. Перше твердження випливає з того, що одиниця підгрупи є ідемпотентом, а тому кожна підгрупа перетинається з якоюсь H_e, отже, міститься в якійсь H_e.

Припустимо, що $H_e \cap H_f \neq \varnothing$. Тоді $H_e \subseteq H_f$ і $H_f \subseteq H_e$, звідки $H_e = H_f$. Друге твердження тепер випливає з того, що в підгрупі може бути лише одна одиниця. □

Елемент напівгрупи називається *груповим*, якщо він належить якійсь із її підгруп.

Розглянемо, як влаштовані максимальні підгрупи в напівгрупі $\mathcal{IS}_n$.

Лема 2.3. *Елемент $\alpha \in \mathcal{IS}_n$ буде ідемпотентом тоді й лише тоді, коли він діє тотожно на своїй області визначення.*

Доведення. Нагадаємо, що через $\operatorname{dom}\alpha$ позначається область визначення елемента α. Якщо для всіх $x \in \operatorname{dom}\alpha$ маємо $\alpha(x) = x$, то для всіх $x \in \operatorname{dom}\alpha$ також маємо $\alpha^2(x) = \alpha(\alpha(x)) = \alpha(x)$. Тому $\operatorname{dom}\alpha^2 \supseteq \operatorname{dom}\alpha$. Із другого боку, завжди $\operatorname{dom}\alpha^2 \subseteq \operatorname{dom}\alpha$. Тому $\operatorname{dom}\alpha^2 = \operatorname{dom}\alpha$ і $\alpha^2 = \alpha$.

Нехай тепер $\alpha^2 = \alpha$. Тоді $\alpha(\alpha(x)) = \alpha(x)$ для кожного $x \in \operatorname{dom}\alpha$. Отже, точка $\alpha(x)$ також належить $\operatorname{dom}\alpha$, причому значення α в точках x та $\alpha(x)$ однакові. Оскільки α є ін'єктивним перетворенням, то $\alpha(x) = x$. □

Таким чином, у напівгрупі $\mathcal{IS}_n$ ідемпотенти однозначно задаються своїми областями визначення. Отримуємо взаємно однозначну відповідність між ідемпотентами з $\mathcal{IS}_n$ та підмножинами з $\{1, 2, \ldots, n\}$, звідки одразу випливає

Твердження 2.3. *Напівгрупа $\mathcal{IS}_n$ містить 2^n ідемпотентів.*

Теорема 2.6. *Нехай $e \in \mathcal{IS}_n$ — ідемпотент. Елемент $\alpha \in \mathcal{IS}_n$ належить підгрупі H_e тоді й лише тоді, коли $\operatorname{dom}\alpha = \operatorname{ran}\alpha = \operatorname{dom} e$. Зокрема, підгрупа H_e ізоморфна симетричній групі S_k, де k — ранг ідемпотента e.*

Доведення. Нехай $\operatorname{dom} e = A = \{a_1, a_2, \ldots, a_k\}$. Позаяк e — ідемпотент, то e є тотожним перетворенням множини A і $\operatorname{ran} e = A$.

Якщо $\alpha \in H_e$, то існує таке натуральне число $m > 1$, що $\alpha^m = \alpha \cdot \alpha^{m-1} = e$. Крім того, $e \cdot \alpha = \alpha$. Звідси і з вправи 2.1 випливає, що $\operatorname{dom} e \subseteq \operatorname{dom}\alpha$ і $\operatorname{dom}\alpha \subseteq \operatorname{dom} e$. Отже, $\operatorname{dom}\alpha = \operatorname{dom} e$. Аналогічно доводиться, що $\operatorname{ran}\alpha \subseteq \operatorname{ran} e$. Отже, $\operatorname{dom}\alpha = \operatorname{ran}\alpha = \operatorname{dom} e$.

Нехай тепер $\operatorname{dom}\alpha = \operatorname{ran}\alpha = \operatorname{dom} e$. Очевидно, що $e\alpha = \alpha e = \alpha$. Із ін'єктивності α випливає, що α є бієктивним перетворенням множини A. Але тоді для нього існує обернене перетворення β множини A. Якщо β розглядати як визначене на A часткове перетворення множини $\{1, 2, \ldots, n\}$, то β є елементом із $\mathcal{IS}_n$. Очевидно, що $\alpha\beta = \beta\alpha = e$. Отже, α є оборотним елементом напівгрупи $e\mathcal{IS}_n e$, а тому $\alpha \in H_e$.

Таким чином, у підгрупу H_e потрапляють ті й лише ті елементи з $\mathcal{IS}_n$, які є бієктивними перетвореннями множини $A = \{a_1, a_2, \ldots, a_k\}$. Зрозуміло, що сукупність таких перетворень утворює групу, ізоморфну групі S_k. □

Означення 2.2. *Непорожня підмножина I напівгрупи $\langle S; * \rangle$ називається* ***правим*** *(відповідно* ***лівим***, ***двостороннім***) ***ідеалом***, *якщо для довільних $a \in I$ і $x \in S$ виконується $a * x \in I$ (відповідно $x * a \in I$, $a * x \in I$ і $x * a \in I$). Іншими словами, якщо $I * S \subseteq I$ (відповідно $S * I \subseteq I$, $I * S \subseteq I$ і $S * I \subseteq I$). Двосторонні ідеали часто називають просто* ***ідеалами***.

Якщо I є правим (відповідно лівим, двостороннім) ідеалом напівгрупи S, то пишуть $I \trianglelefteq_r S$ (відповідно $I \trianglelefteq_l S$, $I \trianglelefteq S$).

Очевидно, що кожний лівий (правий, двосторонній) ідеал буде піднапівгрупою. Однак обернене твердження є неправильним. Крім того, у комутативній напівгрупі поняття лівого, правого та двостороннього ідеалів збігаються.

Приклади. **1.** Для довільної непорожньої підмножини $M \subseteq S$ множини $S * M$, $M * S$ і $S * M * S$ будуть відповідно лівим, правим і двостороннім ідеалами напівгрупи S. Зокрема, для довільного натурального числа $n > 1$ множина S^n буде двостороннім ідеалом.

2. Для довільного натурального k множина $N_k = \{n \in \mathbb{N} \mid n \geq k\}$ буде ідеалом напівгрупи $\langle \mathbb{N}; + \rangle$. Легко бачити, що інших ідеалів ця напівгрупа не має.

3. У напівгрупі з нульовим множенням ідеалом є будь-яка множина, що містить 0.

4. У напівгрупі лівих нулів кожна підмножина є лівим ідеалом, а правий ідеал лише один — уся напівгрупа.

5. У групі є тільки один лівий (він же єдиний правий і єдиний двосторонній) ідеал — сама група.

Вправа 2.5. **1.** *Об'єднання* $\bigcup_k I_k$ *довільної родини лівих (правих, двосторонніх) ідеалів буде лівим (правим, двостороннім) ідеалом.*

2. *Непорожній перетин* $\bigcap_k I_k$ *довільної родини лівих (правих, двосторонніх) ідеалів знову буде лівим (правим, двостороннім) ідеалом.*

3. *Добуток* $I * J$ *двох лівих (правих, двосторонніх) ідеалів* I *та* J *буде лівим (правим, двостороннім) ідеалом.*

Очевидно, що для довільних двох ідеалів I і J напівгрупи S виконується включення $IJ \subseteq I \cap J$. Тому перетин довільної скінченної родини двосторонніх ідеалів є непустим. Як наслідок отримуємо, що кожна напівгрупа містить не більше одного мінімального за включенням ідеалу.

Зауваження. На відміну від двосторонніх, перетин двох односторонніх ідеалів може виявитися порожнім (наприклад, перетин двох лівих ідеалів у напівгрупі лівих нулів). У таких випадках, щоб зробити множину односторонніх ідеалів замкненою відносно перетинів, до ідеалів часто буває зручно зарахувати і порожню множину.

Вправа 2.6. *Доведіть, що в напівгрупі* $\langle \mathbb{N}; + \rangle$ *перетин усіх ідеалів є порожнім. Зокрема, ця напівгрупа не містить мінімальних за включенням ідеалів.*

Із вправи 2.5.2 випливає, що серед усіх лівих ідеалів напівгрупи S, які містять даний елемент a, є найменший (він є перетином усіх лівих ідеалів, що містять a). Він називається *головним лівим ідеалом*, породженим елементом a. Легко бачити, що цей ідеал повинен містити a і всі його ліві кратні, тому він збігається з множиною S^1a. Аналогічно визначаються породжені елементом a *головні правий* aS^1 і *двосторонній* S^1aS^1 ідеали.

Зрозуміло, що кожний (односторонній) ідеал є об'єднанням тих (односторонніх) головних ідеалів, які в ньому містяться. Тому при дослідженні ідеалів конкретної напівгрупи насамперед звертають увагу на

головні ідеали. Розглянемо, як улаштовані головні ідеали в класичних напівгрупах перетворень.

Теорема 2.7. *Нехай S — одна з напівгруп $\mathcal{T}_n$, $\mathcal{PT}_n$ або $\mathcal{IS}_n$. Тоді лівий головний ідеал, породжений елементом α, збігається з множиною*

$$I_l(\alpha) = \{\beta \in S \mid \operatorname{ran}\beta \subseteq \operatorname{ran}\alpha\}.$$

Доведення. Із вправи 2.1 одразу випливає, що $S\alpha \subseteq I_l(\alpha)$. Тому треба довести лише зворотне включення.

Нехай $\beta \in I_l(\alpha)$ і $\operatorname{ran}\beta = \{b_1, b_2, \ldots, b_k\}$. Позаяк $\operatorname{ran}\beta \subseteq \operatorname{ran}\alpha$, то для кожного i $(1 \leq i \leq k)$ існує таке $a_i \in \operatorname{dom}\alpha$, що $\alpha(a_i) = b_i$. Розглянемо тепер елемент γ, який має ту саму область визначення, що й β, і відрізняється від β тільки тим, що коли $\beta(x) = b_i$, то $\gamma(x) = a_i$. Тоді $\beta = \gamma\alpha$. А це означає, що $\beta \in S\alpha$, що й доводить зворотне включення. □

Таким чином, у кожній із напівгруп $\mathcal{T}_n$, $\mathcal{PT}_n$ або $\mathcal{IS}_n$ лівий головний ідеал повністю визначається заданням деякої підмножини з $\{1, 2, \ldots, n\}$ — множини значень елемента α. Зокрема, у кожній із напівгруп $\mathcal{PT}_n$ або $\mathcal{IS}_n$ є рівно 2^n лівих головних ідеалів, а в напівгрупі $\mathcal{T}_n$ їх $2^n - 1$ (в останньому випадку множина значень не може бути порожньою).

Вправа 2.7. *Доведіть, що в напівгрупі $\mathcal{IS}_n$ правий головний ідеал, породжений елементом α, збігається з множиною*

$$I_r(\alpha) = \{\beta \in S \mid \operatorname{dom}\beta \subseteq \operatorname{dom}\alpha\}.$$

Праві головні ідеали в напівгрупах $\mathcal{T}_n$ і $\mathcal{PT}_n$ влаштовані трохи інакше (див. задачі 28 і 29).

Нехай I — ідеал напівгрупи S. Легко перевіряється, що відношення

$$a \sim_I b \;:\Leftrightarrow\; a = b \text{ або } a \text{ і } b \text{ одночасно належать ідеалу } I$$

є конгруенцією на напівгрупі S, яка називається *конгруенцією Ріса* за ідеалом I. Факторнапівгрупа $S/\!\sim_I$ за цією конгруенцією називається *факторнапівгрупою Ріса* або *фактором Ріса* за ідеалом I і позначається S/I.

Зауважимо, що в конгруенції Ріса всі класи конгруенції (за винятком, можливо, класу, що збігається з ідеалом I) є одноелементними. Тому легко зрозуміти, що не кожна конгруенція на напівгрупі є конгруенцією Ріса. Наприклад, у напівгрупі з нульовим множенням кожне відношення еквівалентності буде конгруенцією. Водночас, як випливає

з прикладу 3 на с. 37, конгруенція Ріса на цій напівгрупі може містити щонайбільше один неодноелементний клас — той, куди потрапляє нуль.

Головним ідеальним рядом напівгрупи S називається максимальний за включенням скінченний ланцюг

$$I_1 \subset I_2 \subset \cdots \subset I_n = S \tag{2.3}$$

ідеалів з S. Зокрема, у такому ряді ідеал I_1 є мінімальним і для довільних k $(1 \leq k < n)$ та ідеалу I з $I_k \subseteq I \subseteq I_{k+1}$ випливає $I = I_k$ або $I = I_{k+1}$.

Факторнапівгрупи Ріса I_{k+1}/I_k та ідеал I_1 називаються *факторами* головного ідеального ряду (2.3).

У скінченних напівгрупах головні ідеальні ряди завжди існують, і їх може бути багато. У нескінченних напівгрупах головні ідеальні ряди можуть і не існувати.

Вправа 2.8. *Опишіть усі головні ідеальні ряди і підрахуйте їхню кількість у n-елементній напівгрупі з нульовим множенням.*

Лема 2.4. *Нехай $I_2 \subset I_1$ — ідеали напівгрупи S, причому між I_2 та I_1 немає проміжних ідеалів. Для довільного $a \in I_1 \setminus I_2$ покладемо $J(a) = \{x \in (a) \mid a \notin (x)\}$. Тоді $I_1 \setminus I_2 = (a) \setminus J(a)$.*

Доведення. Доведення розіб'ємо на кілька кроків.

1. $I_2 \cup (a) = I_1$, бо між I_2 та I_1 немає проміжних ідеалів. Тому $I_1 \setminus I_2 \subseteq (a)$ (рис. 3).

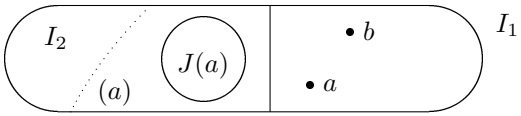


Рис. 3

2. Якщо $b \in I_1 \setminus I_2$, то за попереднім $b \in (a)$ і $a \in (b)$. Отже, $b \notin J(a)$ і $(a) \setminus J(a) \supseteq I_1 \setminus I_2$.

3. Якщо $x \in I_2$, то $(x) \subseteq I_2$ і $a \notin (x)$. Тому або $x \notin (a)$, або $x \in J(a)$. В обох випадках $x \notin (a) \setminus J(a)$. Отже, $(a) \setminus J(a) \subseteq I_1 \setminus I_2$. Разом із п. 1 це доводить твердження леми. □

Теорема 2.8 (Теорема Жордана–Гельдера для напівгруп)**.** *Будь-які два головні ідеальні ряди напівгрупи S мають однакову довжину, а їхні фактори, із точністю до перестановки, попарно ізоморфні.*

Доведення. Для кожного $a \in S$ однозначно визначена та ланка $I_2 \subset I_1$ головного ідеального ряду, для якої $a \in I_1 \setminus I_2$. Із доведення леми 2.4 випливає, що $J(a) = (a) \cap I_2$, а тому $J(a)$ є ідеалом в (a). Із цієї леми також випливає, що $I_1/I_2 = (a)/J(a)$. Отже, фактор I_1/I_2 залежить лише від елемента a, а не від ідеального ряду. Таким чином, усі фактори головного ідеального ряду однозначно визначаються напівгрупою S. □

2.6 Відношення Ґріна

Очевидно, що кожний лівий (правий, двосторонній) ідеал є об'єднанням головних. Природно виникає питання, які елементи напівгрупи породжують один і той самий головний ідеал. Це безпосередньо приводить нас до відношень Ґріна.

Елементи a і b напівгрупи S називаються *$\mathcal{L}$-еквівалентними*, якщо вони породжують один і той самий лівий головний ідеал. Іншими словами, $a\mathcal{L}b$ тоді й лише тоді, коли $S^1a = S^1b$. Очевидно, що $\mathcal{L}$ є відношенням еквівалентності. Класи еквівалентності цього відношення називаються $\mathcal{L}$-класами. Через $\mathcal{L}(a)$ позначається той $\mathcal{L}$-клас, який містить елемент a.

Наступне твердження випливає безпосередньо з означення.

Твердження 2.4. *$a\mathcal{L}b$ тоді й лише тоді, коли існують такі елементи $x, y \in S^1$, що $b = xa$ і $a = yb$.*

Двоїстим чином визначається відношення $\mathcal{R}$: елементи a і b напівгрупи S називаються *$\mathcal{R}$-еквівалентними*, якщо вони породжують один і той самий правий головний ідеал. Іншими словами, $a\mathcal{R}b$ тоді й лише тоді, коли $aS^1 = bS^1$. Класи еквівалентності цього відношення називаються $\mathcal{R}$-класами, а через $\mathcal{R}(a)$ позначається той $\mathcal{R}$-клас, який містить a.

Твердження 2.5. *$a\mathcal{R}b$ тоді й лише тоді, коли існують такі елементи $x, y \in S^1$, що $b = ax$ і $a = by$.*

Лема 2.5. *Відношення $\mathcal{L}$ і $\mathcal{R}$ комутують як елементи напівгрупи $\mathcal{B}(S)$, тобто $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$.*

Доведення. Нехай $(a,b) \in \mathcal{L}\circ\mathcal{R}$. Тоді існує такий елемент $c \in S$, що $a\mathcal{L}c$ і $c\mathcal{R}b$. За твердженнями 2.4 і 2.5 існують такі $u,v,x,y \in S^1$, що

$$a = uc, \qquad c = va, \qquad c = bx, \qquad b = cy.$$

Для елемента $d = ucy$ тепер маємо

$$d = uc \cdot y = ay \quad \text{і} \quad a = uc = u \cdot bx = u \cdot cy \cdot x = ucy \cdot x = dx.$$

Тому $a\mathcal{R}d$. Крім того,

$$d = u \cdot cy = ub \quad \text{і} \quad b = cy = va \cdot y = v \cdot uc \cdot y = v \cdot ucy = vd.$$

Тому $d\mathcal{L}b$. Отже, $(a,b) \in \mathcal{R}\circ\mathcal{L}$ і $\mathcal{L}\circ\mathcal{R} \subseteq \mathcal{R}\circ\mathcal{L}$.

Аналогічно доводиться зворотне включення. □

Лема 2.6. *$\mathcal{L}\circ\mathcal{R}$ є відношенням еквівалентності, причому це найменше відношення еквівалентності, яке містить кожне з відношень $\mathcal{L}$ і $\mathcal{R}$.*

Доведення. Рефлексивність відношення $\mathcal{L}\circ\mathcal{R}$ очевидна.

Симетричність. Нехай $(a,b) \in \mathcal{L}\circ\mathcal{R}$. Тоді існує таке c, що $(a,c) \in \mathcal{L}$ і $(c,b) \in \mathcal{R}$. Оскільки $\mathcal{L}$ і $\mathcal{R}$ є відношеннями еквівалентності, то $(b,c) \in \mathcal{R}$ і $(c,a) \in \mathcal{L}$. Отже, $(b,a) \in \mathcal{R}\circ\mathcal{L}$. Але $\mathcal{L}$ і $\mathcal{R}$ комутують, тому $(b,a) \in \mathcal{L}\circ\mathcal{R}$.

Транзитивність. Нехай пари (a,b) і (b,c) належать відношенню $\mathcal{L}\circ\mathcal{R}$. Тоді існують такі u і v, що $(a,u) \in \mathcal{L}$, $(u,b) \in \mathcal{R}$, $(b,v) \in \mathcal{L}$, $(v,c) \in \mathcal{R}$. Звідси випливає, що $(u,v) \in \mathcal{R}\circ\mathcal{L}$. Позаяк $\mathcal{R}\circ\mathcal{L} = \mathcal{L}\circ\mathcal{R}$, то існує таке w, що $(u,w) \in \mathcal{L}$, $(w,v) \in \mathcal{R}$. Із транзитивності відношень еквівалентності $\mathcal{L}$ і $\mathcal{R}$ отримуємо, що $(a,w) \in \mathcal{L}$, $(w,c) \in \mathcal{R}$, звідки $(a,c) \in \mathcal{L}\circ\mathcal{R}$. □

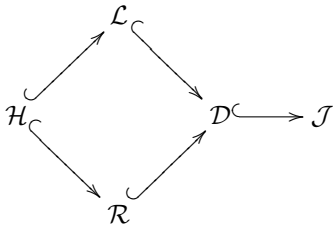
Відношення $\mathcal{L}\circ\mathcal{R}$ позначають символом $\mathcal{D}$. Якщо $a\mathcal{D}b$, то елементи a і b називаються *$\mathcal{D}$-еквівалентними*. Класи еквівалентності відношення $\mathcal{D}$ називаються $\mathcal{D}$-класами, а через $\mathcal{D}(a)$ позначається той $\mathcal{D}$-клас, який містить a.

Відношення $\mathcal{L}\cap\mathcal{R}$ позначають символом $\mathcal{H}$. Подібно попереднім відношенням, визначаються *$\mathcal{H}$-еквівалентні* елементи і $\mathcal{H}$-класи. Зокрема, через $\mathcal{H}(a)$ позначається той $\mathcal{H}$-клас, який містить a.

Нарешті, елементи a і b називаються *$\mathcal{J}$-еквівалентними*, якщо вони породжують один і той самий двосторонній головний ідеал. Іншими словами, $a\mathcal{J}b$ тоді й лише тоді, коли $S^1aS^1 = S^1bS^1$. Класи еквівалентності цього відношення називаються $\mathcal{J}$-класами, а через $\mathcal{J}(a)$ позначається той $\mathcal{J}$-клас, який містить a.

Твердження 2.6. *$a\mathcal{J}b$ тоді й лише тоді, коли існують такі елементи $x, y, u, v \in S^1$, що $b = xay$ і $a = ubv$.*

Відношення $\mathcal{L}$, $\mathcal{R}$, $\mathcal{D}$, $\mathcal{H}$ і $\mathcal{J}$ називаються *відношеннями Ґріна*. Очевидно, що відношення $\mathcal{J}$ містить кожне з відношень $\mathcal{L}$ і $\mathcal{R}$, а тому, за лемою 2.6, воно містить і відношення $\mathcal{D}$. Тому для цих відношень маємо таку діаграму включень



Теорема 2.9. *Для періодичної напівгрупи S відношення Ґріна $\mathcal{D}$ і $\mathcal{J}$ збігаються.*

Доведення. Позаяк $\mathcal{D} \subseteq \mathcal{J}$, то треба довести лише включення $\mathcal{D} \supseteq \mathcal{J}$. Нехай $a\mathcal{J}b$. За твердженням 2.6 існують такі елементи $x, y, u, v \in S^1$, що $b = xay$ і $a = ubv$. Тоді

$$a = uxayv = (ux)^k \cdot a \cdot (yv)^k$$

для довільного натурального числа k. Із періодичності напівгрупи S випливає існування таких чисел m і n, що елементи $e = (ux)^m$ і $f = (yv)^n$ є ідемпотентами. Тому

$$a = (ux)^{mn} \cdot a \cdot (yv)^{mn} = eaf = ea = af\,.$$

Для елемента $c = x \cdot a$ маємо:

$$a = ea = (ux)^m a = (ux)^{m-1}u \cdot xa = (ux)^{m-1}u \cdot c\,.$$

Тому $a\mathcal{L}c$. З іншого боку, $b = xay = c \cdot y$ і

$$c = xa = xaf = xa(yv)^n = xay \cdot v(yv)^{n-1} = b \cdot v(yv)^{n-1}\,.$$

Тому $c\mathcal{R}b$. Але тоді $(a, b) \in \mathcal{L} \circ \mathcal{R} = \mathcal{D}$, що й доводить включення $\mathcal{J} \subseteq \mathcal{D}$. □

Зокрема, $\mathcal{D} = \mathcal{J}$ для кожної скінченної напівгрупи.

Лема 2.7 (Ґрін). *Нехай $a\mathcal{R}b$ і u, v — такі елементи з S^1, що $au = b$, $bv = a$. Тоді відображення $\mu_u : x \mapsto xu$ і $\mu_v : y \mapsto yv$ є взаємно оберненими відображеннями $\mathcal{L}$-класу $L(a)$ на $\mathcal{L}$-клас $L(b)$ і навпаки. Крім того, ці відображення зберігають $\mathcal{H}$-класи, тобто два елементи x_1 і x_2 із $L(a)$ належать одному $\mathcal{H}$-класу тоді й лише тоді, коли їх образи $y_1 = x_1u$ і $y_2 = x_2u$ при відображенні μ_u належать одному $\mathcal{H}$-класу.*

Доведення. Позаяк відношення $\mathcal{L}$ стабільне справа, то з $a\mathcal{L}x$ випливає $au\mathcal{L}xu$. Отже, μ_u відображає клас $L(a)$ у клас $L(b)$. Аналогічно μ_v відображає клас $L(b)$ у клас $L(a)$.

Якщо $x \in L(a)$, то існує такий $z \in S^1$, що $x = za$. Далі маємо

$$x = za \overset{\mu_u}{\longmapsto} zau = zb \overset{\mu_v}{\longmapsto} zbv = za = x\,.$$

Отже, $\mu_u\mu_v = \mathrm{id}_{L(a)}$. Аналогічно доводиться, що $\mu_v\mu_u = \mathrm{id}_{L(b)}$. Тому відображення μ_u і μ_v є взаємно оберненими.

Нехай тепер $x_1, x_2 \in L(a)$ і $x_1\mathcal{H}x_2$. Із доведеного вище випливає, що $x_1u\mathcal{L}x_2u$. Крім того, $x_1\mathcal{R}x_2$. Оскільки $x_1u = x_1 \cdot u$ і $x_1 = x_1uv = x_1u \cdot v$, то $x_1\mathcal{R}x_1u$. Аналогічно доводиться, що $x_2\mathcal{R}x_2u$. Тому $x_1u\mathcal{R}x_2u$ і $x_1u\mathcal{H}x_2u$. Обернене твердження доводиться аналогічно. □

Очевидно, що буде правильним і двоїстий варіант леми Ґріна:

Якщо $a\mathcal{L}b$ і u, v — такі елементи з S^1, що $ua = b$, $vb = a$, то відображення $\lambda_u : x \mapsto ux$ і $\lambda_v : y \mapsto vy$ є бієкціями між класами $R(a)$ і $R(b)$, які зберігають $\mathcal{H}$-класи.

Наслідок 2.6. *Всі $\mathcal{R}$-класи (відповідно $\mathcal{L}$-класи, $\mathcal{H}$-класи) напівгрупи S, що належать одному $\mathcal{D}$-класу, рівнопотужні.*

Доведення. Нехай $a\mathcal{D}b$. Тоді існує такий елемент c, що $a\mathcal{L}c$ і $c\mathcal{R}b$. За твердженням 2.5 існують такі u і v, що $cu = b$ і $bv = c$. Із леми Ґріна одразу випливає, що класи $\mathcal{L}(b)$ і $\mathcal{L}(c)$ рівнопотужні. Крім того, $\mathcal{L}(a) = \mathcal{L}(c)$. Отже, $\mathcal{L}(a)$ і $\mathcal{L}(b)$ рівнопотужні.

Рівнопотужність класів $\mathcal{R}(a)$ і $\mathcal{R}(b)$ доводиться аналогічно.

Далі, із леми Ґріна випливає, що відображення $\mu_u : x \mapsto xu$ клас $\mathcal{H}(c)$ бієктивно відображає на клас $\mathcal{H}(b)$. Аналогічно з двоїстого варіанта леми Ґріна випливає, що існує бієкція класу $\mathcal{H}(c)$ на клас $\mathcal{H}(a)$. Тому $\mathcal{H}(a)$ і $\mathcal{H}(b)$ також рівнопотужні. □

Із цього наслідку випливає, що кожний $\mathcal{D}$-клас D можна зобразити у вигляді прямокутної таблиці

$\mathcal{R}(a_1)$			$\dots$	
$\mathcal{R}(a_2)$			$\dots$	
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\mathcal{R}(a_k)$			$\dots$	
	$\mathcal{L}(b_1)$	$\mathcal{L}(b_2)$	$\dots$	$\mathcal{L}(b_m)$

Її рядки відповідають $\mathcal{R}$-класам, що містяться в D, а стовпчики — аналогічним $\mathcal{L}$-класам. Клітинки таблиці будуть відповідати $\mathcal{H}$-класам, що містяться в D. Цю таблицю називають *egg-box–діаграмою*[2] класу D.

Теорема 2.10. *Максимальні підгрупи напівгрупи S — це ті $\mathcal{H}$-класи, які містять ідемпотенти.*

Доведення. Зрозуміло, що $\mathcal{H}$-клас, який не містить ідемпотента, не може бути підгрупою. Нехай тепер $\mathcal{H}$-клас H містить ідемпотент e. Легко перевіряється, що максимальна підгрупа H_e міститься в H. Розглянемо довільний елемент $a \in H$. Оскільки $e\mathcal{L}a$ і $e\mathcal{R}a$, то існують такі $x, y \in S^1$, що $a = ex = ye$. Але тоді $ea = ae = a$. Отже, e є двосторонньою одиницею для всіх елементів із H, а тому H міститься в піднапівгрупі eSe. Крім того, із співвідношень $e\mathcal{L}a$ і $e\mathcal{R}a$ випливає, що коли $a \neq e$, то існують такі $u, v \in S$, що $e = ua = av$. Звідси випливає, що $e = eue \cdot a = a \cdot eve$. Отже, елемент a є оборотним у напівгрупі eSe, тобто належить максимальній підгрупі H_e. Тому $H \subseteq H_e$. Таким чином, $H = H_e$. □

2.7 Нільпотентні напівгрупи

Нехай S — напівгрупа з нулем 0. Елемент $a \in S$ називається *нільпотентним* або *нільелементом*, якщо $a^n = 0$ для деякого натурального числа n. Напівгрупа, усі елементи якої є нільпотентними, називається *нільнапівгрупою*.

Напівгрупа S називається *нільпотентною*, якщо існує таке натуральне число n, що $a_1 a_2 \cdots a_n = 0$ для довільних $a_1, a_2, \dots, a_n \in S$. Найменше таке n називається *класом* (або *ступенем*) *нільпотентності* напівгрупи S.

Очевидно, що нільпотентна напівгрупа є нільнапівгрупою. Обернене твердження, узагалі кажучи, неправильне.

[2] Англійське слово egg-box означає лоток для яєць.

Приклад. У напівгрупі

$$T = \{\tau \in \mathcal{IS}(\mathbb{N}) \ : \ |\mathrm{dom}\,\tau| \leq 1 \ \text{ і якщо } \ \mathrm{dom}\,\tau = \{x\}, \ \text{ то } \ x^\tau > x\} \quad (2.4)$$

кожен елемент є нільпотентним, бо вже у квадраті дорівнює 0. Але T не є нільпотентною. Справді, позначимо через $\tau_{a,b}$ елемент, для якого $\mathrm{dom}\,\tau = \{a\}$ і $a^\tau = b$. Тоді для довільного натурального n маємо

$$\tau_{1,2}\tau_{2,3}\cdots\tau_{n,n+1} = \tau_{1,n+1} \neq 0\,.$$

Однак скінченні нільнапівгрупи є нільпотентними.

Теорема 2.11. *Для скінченної напівгрупи S із нулем 0 наступні умови рівносильні:*
(i) S — нільпотентна напівгрупа;
(ii) S — нільнапівгрупа;
(iii) 0 є єдиним ідемпотентом напівгрупи S.

Доведення. Імплікації $(i) \Rightarrow (ii)$ та $(ii) \Rightarrow (iii)$ є очевидними.

$(iii) \Rightarrow (i)$. Припустимо, що 0 є єдиним ідемпотентом напівгрупи S. Нехай $|S| = n$. Якщо $S^n \neq 0$, то існує добуток вигляду $a_1a_2a_3\cdots a_n$, який не дорівнює 0. Тоді всі добутки a_1, a_1a_2, $a_1a_2a_3$, $\ldots$, $a_1a_2a_3\cdots a_n$ також ненульові, а позаяк ненульових елементів лише $n-1$, то серед цих добутків є принаймні два рівні. Нехай $a_1\cdots a_k = a_1\cdots a_ka_{k+1}\cdots a_m$. Позначимо $a = a_1\cdots a_k$, $b = a_{k+1}\cdots a_m$. Тоді $a = ab$, звідки $a = ab^r$ для довільного натурального числа r. Отже, $b^r \neq 0$. З іншого боку, за теоремою Фробеніуса серед степенів елемента b має бути ідемпотент, що суперечить припущенню. Отже, $S^n = 0$, і S — нільпотентна. □

Вправа 2.9. *Доведіть, що клас нільпотентних напівгруп (нільнапівгруп) є замкненим відносно взяття піднапівгруп, факторнапівгруп і скінченних прямих добутків.*

Теорема 2.12. *У нільнапівгрупі всі відношення Ґріна є тривіальними (тобто збігаються з відношенням рівності).*

Доведення. Позаяк усі відношення Ґріна містяться в $\mathcal{J}$-відношенні, то досить довести тривіальність лише останнього. Нехай $a\mathcal{J}b$. Тоді існують такі $x, y, u, v \in S^1$, що $a = xby$, $b = uav$. Очевидно, що з $0\mathcal{J}b$ випливає $b = 0$. Тому можна вважати, що $a \neq 0$. Але тоді з рівностей $a = xuavy = (xu)^n a(vy)^n$ випливає, що елементи xu і vy не є нільпотентними. Отже, $xu \notin S$, $vy \notin S$, що можливе лише тоді, коли $x = u = v = y = 1$. Але тоді $a = b$. □

Уже майже півстоліття залишається відкритою відома **проблема Шевріна**: *чи буде нільпотентною нільнапівгрупа, усі власні піднапівгрупи якої є нільпотентними?*

Трохи детальніше зупинимося на будові нільелементів та нільпотентних піднапівгруп у напівгрупі $\mathcal{IS}_n$. Для цього нам корисно узагальнити поняття циклового розкладу підстановки.

Графіком часткового перетворення $\pi \in \mathcal{PT}(X)$ називається множина $E_\pi = \{(x, y) : x \in \operatorname{dom}\pi,\ \pi(x) = y\}$. E_π можна розглядати як множину стрілок орієнтованого графа $\Gamma_\pi = (X, E_\pi)$ із множиною вершин X, який називається *графом дії* перетворення π. Очевидно, що орієнтований граф $\Gamma = (X, E)$ буде графом дії деякого перетворення $\pi \in \mathcal{PT}(X)$ тоді й лише тоді, коли з кожної вершини виходить не більше однієї стрілки.

Для довільного впорядкованого набору $a_1, a_2, \ldots, a_k$ попарно різних елементів множини $\{1, 2, \ldots, n\}$ розглянемо такі два перетворення цієї множини:

$$(a_1, a_2, \ldots, a_k)(x) = \begin{cases} x, & \text{якщо } x \notin \{a_1, a_2, \ldots, a_k\}; \\ a_{i+1}, & \text{якщо } x \in \{a_1, a_2, \ldots, a_{k-1}\}; \\ a_1, & \text{якщо } x = a_k; \end{cases} \tag{2.5}$$

$$[a_1, a_2, \ldots, a_k](x) = \begin{cases} x, & \text{якщо } x \notin \{a_1, a_2, \ldots, a_k\}; \\ a_{i+1}, & \text{якщо } x \in \{a_1, a_2, \ldots, a_{k-1}\}; \\ \varnothing, & \text{якщо } x = a_k. \end{cases} \tag{2.6}$$

Очевидно, що обидва перетворення є елементами напівгрупи $\mathcal{IS}_n$. Компонентами зв'язності графа дії першого перетворення буде цикл $a_1 \to a_2 \to \cdots \to a_k \to a_1$ і одноелементні цикли (які відповідають нерухомим точкам), а другого — ланцюг $a_1 \to a_2 \to \cdots \to a_k$ і такі ж самі одноелементні цикли. Тому й самі перетворення (2.5) і (2.6) називатимемо відповідно *циклом* і *ланцюгом*. Очевидно, що різні впорядковані набори $a_1, a_2, \ldots, a_k$ визначають різні ланцюги. Із циклами трохи складніше: усі цикли (2.5) довжини 1 є тотожним перетворенням, а при $k > 1$ впорядковані набори $a_1, a_2, \ldots, a_k$ і $b_1, b_2, \ldots, b_k$ визначають один і той самийе цикл тоді й лише тоді, коли одержуються один з одного циклічним зсувом.

Множину $\{a_1, a_2, \ldots, a_k\}$ назвемо *областю нетривіальності* відповідного циклу (ланцюга).

Визначені наборами $a_1, \ldots, a_k$ і $b_1, \ldots, b_m$ ланцюги (цикли) будемо називати *диз'юнктними*, якщо множини $\{a_1, \ldots, a_k\}$ і $\{b_1, \ldots, b_m\}$ не перетинаються. Позаяк ланцюги (цикли) поза своєю областю нетривіальності діють тотожно, то диз'юнктні ланцюги і/або цикли комутують.

Твердження 2.7. *Кожен елемент напівгрупи $\mathcal{IS}_n$ розкладається в добуток диз'юнктних ланцюгів і/або циклів. Такий розклад є однозначним із точністю до порядку множників і кількості одноелементних циклів.*

Доведення. Існування розкладу. Нехай $\pi \in \mathcal{IS}_n$. Із ін'єктивності π випливає, що в кожну вершину графа Γ_π входить теж не більше однієї стрілки. Тому компонентами зв'язності графа Γ_π будуть лише цикли й ланцюги. Для кожної компоненти зв'язності Λ графа Γ_π природно будується відповідний ланцюг або цикл π_Λ уже як елемент напівгрупи $\mathcal{IS}_n$. Очевидно, що ланцюги/цикли π_Λ, які відповідають різним компонентам зв'язності, будуть диз'юнктними, а добуток у довільному порядку всіх таким чином побудованих π_Λ збігатиметься з π.

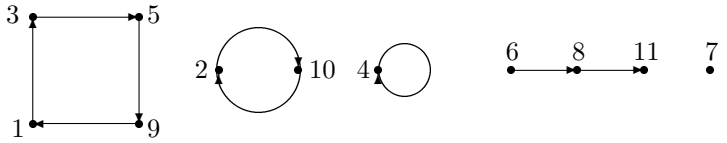
Однозначність розкладу. Нехай $\pi = \pi_1 \cdots \pi_m$ — розклад π у добуток диз'юнктних ланцюгів і/або циклів. Позаяк кожний множник π_i поза своєю областю нетривіальності діє тотожно, то компонентами зв'язності графа Γ_π будуть лише цикли й ланцюги, які відповідають множникам розкладу (і, можливо, одноелементні цикли, які відповідають точкам, що не входять в область нетривіальності жодного із множників). Таким чином, множники розкладу $\pi = \pi_1 \cdots \pi_m$ повністю визначаються графом дії часткової підстановки π, що й доводить однозначність розкладу. □

Розклад

$$\pi = (a_1, \ldots, a_k) \cdots (b_1, \ldots, b_l)[c_1, \ldots, c_p] \cdots [d_1, \ldots, d_q] \qquad (2.7)$$

елемента $\pi_i \in \mathcal{IS}_n$ у добуток диз'юнктних ланцюгів і/або циклів, у правій частині якого кожен елемент множини $N = \{1, 2, \ldots, n\}$ зустрічається рівно один раз, називається *ланцюговим розкладом* часткової підстановки π_i. Він є аналогом розкладу підстановки в добуток незалежних циклів.

Приклад. Граф дії часткової підстановки $\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 10 & 5 & 4 & 9 & 8 & \varnothing & 11 & 1 & 2 & \varnothing \end{smallmatrix}\right)$ має вигляд



а тому ланцюговий розклад π має вигляд $\pi = (1\ 3\ 5\ 9)(2\ 10)(4)[6\ 8\ 11][7]$.

Твердження 2.8. *Часткова підстановка $\pi_i \in \mathcal{IS}_n$ буде нільпотентною тоді й лише тоді, коли її ланцюговий розклад не містить циклів.*

Доведення. Якщо ланцюговий розклад часткової підстановки π містить цикл $(a_1, \ldots, a_k)$, то для довільного m буде $\{a_1, \ldots, a_k\} \subseteq \operatorname{dom} \pi^m$. А тому $\operatorname{dom} \pi^m \neq \varnothing$ і $\pi^m \neq 0$. Отже, π не є нільелементом.

Навпаки, нехай ланцюговий розклад π містить лише ланцюги і m — максимум довжин ланцюгів. Тоді з означення ланцюга одразу випливає, що $\pi^m = 0$. Отже, π є нільелементом. □

Нільпотентну піднапівгрупу з $\mathcal{IS}_n$ назвемо *максимальною*, якщо вона не міститься в жодній іншій нільпотентній піднапівгрупі.

Теорема 2.13. *Нехай $\prec$ — лінійний порядок на множині $N = \{1, 2, \ldots, n\}$. Тоді множина*

$$T_\prec = \{\tau \in \mathcal{IS}_n \mid \textit{якщо} \quad x \in \operatorname{dom} \tau, \quad \textit{то} \quad x^\tau \prec x\}$$

буде максимальною нільпотентною піднапівгрупою напівгрупи $\mathcal{IS}_n$.

Навпаки, кожна максимальна нільпотентна піднапівгрупа з $\mathcal{IS}_n$ має вигляд $T_\prec$ для деякого лінійного порядку $\prec$ на N.

Доведення. Очевидно, що $T_\prec$ є піднапівгрупою. Нехай $\tau_1, \tau_2 \ldots, \tau_n \in T_\prec$. Якщо $\tau_1\tau_2 \cdots \tau_n \neq 0$, то для довільного $x \in \operatorname{dom}(\tau_1\tau_2 \cdots \tau_n)$ маємо

$$x^{\tau_1\tau_2\cdots\tau_n} \prec \cdots \prec x^{\tau_1\tau_2} \prec x^{\tau_1} \prec x\,,$$

що неможливо. Отже, $T_\prec^n = 0$ і $T_\prec$ є нільпотентною напівгрупою.

Розглянемо довільний нільелемент $\nu \notin T_\prec$. Тоді існує такий $x \in \operatorname{dom} \nu$, що $x^\nu \not\prec x$. Позаяк ν є нільелементом, то $x^\nu \neq x$. Отже, $x^\nu \succ x$. Тому існує такий елемент $\mu \in T_\prec$, що $\operatorname{dom} \mu = \{x^\nu\}$ і $(x^\nu)^\mu = x$. Але тоді x є нерухомою точкою добутку $\nu\mu$ і цей добуток не є нільелементом. Таким чином, для довільного нільелемента $\nu \notin T_\prec$ напівгрупа $\langle T_\prec \cup \{\nu\}\rangle$ уже не є нільпотентною, що доводить максимальність $T_\prec$.

Нехай тепер T є нільпотентною піднапівгрупою з $\mathcal{IS}_n$. Для довільних $x, y \in N$ покладемо $y \propto x$ тоді й тільки тоді, коли існує такий $\tau \in T$, що $x^\tau = y$. Із нільпотентності T випливають антирефлексивність і антисиметричність відношення $\propto$ (якби було $x^\tau = y$ і $y^\mu = x$, то добуток $\tau\mu$ мав би нерухому точку x, що суперечить нільпотентності T). Транзитивність $\propto$ також очевидна: якщо $x^\tau = y$ і $y^\mu = z$, то $x^{\tau\mu} = z$. Отже, відношення $\propto$ є частковим порядком на множині N. За теоремою

Шпільрайна (див. розділ 3) кожен частковий порядок можна розширити до лінійного. Нехай $\prec$ — лінійний порядок на множині N, який містить $\propto$. Із побудови $\propto$ і означення $T_\prec$ одразу випливає, що $T \subseteq T_\prec$. Отже, максимальними можуть бути лише нільпотентні піднапівгрупи вигляду $T_\prec$. $\square$

Нагадаємо, що n-м числом Белла B_n називається кількість різних розбиттів n-елементної множини на непорожні блоки.

Наслідок 2.7. *$\mathcal{IS}_n$ містить рівно $n!$ різних максимальних нільпотентних піднапівгруп. Ці піднапівгрупи попарно ізоморфні і порядок кожної з них дорівнює n-му числу Белла B_n.*

Доведення. Оскільки на n-елементній множині лінійний порядок можна визначити $n!$ способами, то для доведення першої частини досить показати, що різним лінійним порядкам відповідають різні піднапівгрупи.

Нехай

$$a_1 \prec_1 a_2 \prec_1 a_3 \prec_1 \cdots \prec_1 a_n$$

і

$$b_1 \prec_2 b_2 \prec_2 b_3 \prec_2 \cdots \prec_2 b_n$$

— два різні лінійні порядки на множині N. Тоді знайдуться такі x і y, що $y \prec_1 x$, але $y \not\prec_2 x$. Тому часткова підстановка τ, для якої $\operatorname{dom}\tau = \{x\}$ і $x^\tau = y$, належатиме $T_{\prec_1}$, але не буде належати $T_{\prec_2}$. Отже, $T_{\prec_1} \neq T_{\prec_2}$, що доводить першу частину твердження.

Розглянемо тепер підстановку

$$\pi = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}.$$

Безпосередньо перевіряється, що відображення $\tau \mapsto \pi^{-1}\tau\pi$ є автоморфізмом напівгрупи $\mathcal{IS}_n$, який відображає $T_{\prec_1}$ у $T_{\prec_2}$. Позаяк обернене відображення $\mu \mapsto \pi\mu\pi^{-1}$ також є автоморфізмом $\mathcal{IS}_n$ і відображає $T_{\prec_2}$ в $T_{\prec_1}$, то $T_{\prec_1}$ і $T_{\prec_2}$ ізоморфні.

Ізоморфні напівгрупи мають однаковий порядок, тому досить підрахувати порядок напівгрупи $T_<$, яка відповідає звичайному лінійному порядку $<$ на множині $N = \{1, 2, \dots, n\}$. Для цього елемента $\tau \in T_<$ з ланцюговим розкладом

$$\tau = [a_1, \dots, a_k][b_1, \dots, b_l] \cdots [d_1, \dots, d_q]$$

поставимо у відповідність розбиття множини N на блоки $\{a_1, \dots, a_k\}$, $\{b_1, \dots, b_l\}$, …, $\{d_1, \dots, d_q\}$. Очевидно, що таким чином отримаємо всі

розбиття множини N. Крім того, кожне розбиття отримаємо тільки один раз, бо за блоком $\{a_1, a_2 \ldots, a_k\}$ відповідний ланцюг $[a_1, a_2 \ldots, a_k]$ відновлюється однозначно: у ланцюгу елементи блоку мають іти в порядку спадання: $a_1 > a_2 > \cdots > a_k$.

Таким чином, ми встановили бієкцію між елементами напівгрупи $T_<$ та розбиттями множини N. Але це й доводить, що $|T_<| = B_n$. □

2.8 Регулярні та інверсні напівгрупи

Елемент a напівгрупи S називається *регулярним*, якщо існує такий елемент $x \in S$, що $axa = a$. Напівгрупа, в якій усі елементи регулярні, називається *регулярною*.

Регулярність можна вважати дуже далеким узагальненням оборотності, позаяк для оборотного елемента a виконується рівність $aa^{-1}a = a$. Зокрема, кожен оборотний елемент є регулярним.

Приклади. 1. У напівгрупі $\langle \mathbb{N}; + \rangle$ регулярних елементів нема, а в напівгрупі $\langle \mathbb{N}; \cdot \rangle$ регулярним елементом буде лише 1.

2. Кожна група і кожна прямокутна зв'язка є регулярними напівгрупами.

Твердження 2.9. *Напівгрупи $\mathcal{IS}(M)$ та $\mathcal{T}(M)$ є регулярними.*

Доведення. Доведемо спочатку регулярність $\mathcal{IS}(M)$. Нехай π — довільний елемент із $\mathcal{IS}(M)$. Позаяк π є взаємно однозначним відображенням множини $\operatorname{dom}\pi$ на $\operatorname{ran}\pi$, то можна коректно визначити обернене відображення $\pi^{-1} : \operatorname{ran}\pi \to \operatorname{dom}\pi$, яке теж, очевидно, буде елементом напівгрупи $\mathcal{IS}(M)$. Але тоді $\pi \cdot \pi^{-1} \cdot \pi = \pi$.

Розглянемо тепер довільний елемент $\mu \in \mathcal{T}(M)$. Для кожного елемента $x \in \operatorname{ran}\mu$ виберемо в його прообразі $\mu^{-1}(x)$ довільний елемент a_x і визначимо перетворення $\nu : M \to M$ таким правилом:

$$\nu(x) = \begin{cases} a_x, & \text{якщо } x \in \operatorname{ran}\mu; \\ x, & \text{у противному разі.} \end{cases}$$

Згідно з означенням перетворення ν одразу маємо рівність $\mu \cdot \nu \cdot \mu = \mu$. □

Лема 2.8. *Якщо $axa = a$, то ax і xa — ідемпотенти.*

Доведення випливає з очевидних рівностей $axax = ax$ і $xaxa = xa$. □

Лема 2.9 (фон Нойман). *Наступні умови рівносильні:*
(i) елемент a — регулярний;
(ii) існує такий ідемпотент $e \in E(S)$, що $aS^1 = eS^1$;
(iii) існує такий ідемпотент $e \in E(S)$, що $S^1a = S^1e$.

Доведення. Доведемо лише рівносильність (i) та (ii) (рівносильність (i) та (iii) доводиться аналогічно).

(i) $\Rightarrow$ (ii). Нехай a — регулярний і $axa = a$. Тоді

$$aS^1 \supseteq axS^1 \supseteq axaS^1 = aS^1.$$

Отже, для ідемпотента $e = ax$ маємо $aS^1 = eS^1$.

(ii) $\Rightarrow$ (i). Якщо $aS^1 = eS^1$, то існують такі $x, y \in S^1$, що $e = ax$, $a = ey$. Якщо $x = 1$ або $y = 1$, то $a = e$ — регулярний. Якщо ж $a \neq e$, то маємо:

$$a = ey = e \cdot ey = ax \cdot ey = axa\,. \qquad \square$$

Із леми фон Ноймана випливає, що для регулярного елемента a $\mathcal{R}$-клас $\mathcal{R}(a)$ містить ідемпотент, а тому всі елементи з $\mathcal{R}(a)$ будуть регулярними. З іншого боку, із наслідку 2.6 випливає, що кожен $\mathcal{L}$-клас із $\mathcal{D}$-класу $\mathcal{D}(a)$ має непорожній перетин з $\mathcal{R}(a)$. А тому кожен такий $\mathcal{L}$-клас містить регулярні елементи. Аналогічно попередньому, із леми фон Ноймана одержуємо, що всі ці $\mathcal{L}$-класи складаються з регулярних елементів. Таким чином, одержуємо наслідок, який фактично стверджує, що регулярність є не так властивістю елементів напівгрупи, як її $\mathcal{D}$-класів:

Наслідок 2.8. *Якщо елемент a регулярний, то всі елементи $\mathcal{D}$-класу $\mathcal{D}(a)$ також є регулярними. У цьому випадку кожен $\mathcal{L}$-клас і кожен $\mathcal{R}$-клас із $\mathcal{D}(a)$ мають принаймні по одному ідемпотенту.*

Елемент b називається *інверсним* до a, якщо $aba = a$ і $bab = b$.

Твердження 2.10. *Для кожного регулярного елемента існує інверсний.*

Доведення. Якщо $axa = a$, то елемент xax буде інверсним до a. Справді,

$$a \cdot xax \cdot a = axa \cdot xa = a \cdot xa = a\,,$$
$$xax \cdot a \cdot xax = x \cdot axa \cdot xax = x \cdot a \cdot xax = x \cdot axa \cdot x = xax\,. \qquad \square$$

Кількість інверсних до даного регулярного елемента може варіювати в дуже широких межах. Наприклад, у групі для кожного елемента a існує рівно один інверсний — це обернений елемент a^{-1}. Із другого боку,

у напівгрупі з лівим (правим) множенням і в прямокутній зв'язці для довільних a і b виконуються рівності $aba = a$ і $bab = b$. Тому в цих напівгрупах будь-які два елементи є інверсними.

Регулярна напівгрупа, в якій для кожного елемента існує єдиний інверсний, називається *інверсною*. Інверсні напівгрупи є природним узагальненням поняття групи. В інверсній напівгрупі елемент, інверсний до a, будемо позначати a^{-1}. Із означення a^{-1} та леми 2.8 одразу випливає, що $(a^{-1})^{-1} = a$ і що елементи aa^{-1} та $a^{-1}a$ є ідемпотентами.

Теорема 2.14 (Критерій інверсності)**.** *Напівгрупа S буде інверсною тоді й лише тоді, коли вона регулярна й будь-які два її ідемпотенти комутують.*

Доведення. Достатність. Нехай напівгрупа S регулярна й ідемпотенти комутують. Припустимо, що елементи b і c є інверсними до a. Тоді

$$aba = a, \quad bab = b, \quad aca = a, \quad cac = c$$

і елементи ab, ba, ac, ca є ідемпотентами. Оскільки ідемпотенти комутують, то отримуємо

$$b = bab = bacab = cabab = cab = cacab = cabac = cac = c\,.$$

Необхідність. Нехай напівгрупа S інверсна і $e, f \in E(S)$. Розглянемо елемент $a = (ef)^{-1}$. Із рівностей

$$a \cdot ef \cdot a = a, \quad ef \cdot a \cdot ef = ef$$

випливають рівності

$$fa \cdot ef \cdot fa = fa, \quad ef \cdot fa \cdot ef = ef\,.$$

Отже, fa також буде інверсним до ef. Аналогічно доводиться, що елемент ae є інверсним до ef. Із єдиності інверсного елемента випливає, що $a = fa = ae$. Але тоді $a^2 = ae \cdot fa = a \cdot ef \cdot a = a$, тобто a є ідемпотентом. Оскільки ідемпотент інверсний сам до себе, то $a = ef$.

Аналогічно доводиться ідемпотентність елемента fe. Із рівностей

$$ef \cdot fe \cdot ef = e \cdot f^2 \cdot e^2 \cdot f = efef = (ef)^2 = ef\,,$$

$$fe \cdot ef \cdot fe = f \cdot e^2 \cdot f^2 \cdot e = fefe = (fe)^2 = fe$$

випливає, що ідемпотенти ef і fe є інверсними один до одного. Але ідемпотент збігається зі своїм інверсним, тому $ef = fe$. □

Наслідок 2.9. 1. $(ab)^{-1} = b^{-1}a^{-1}$;

2. *кожна комутативна регулярна напівгрупа буде інверсною*;

3. *напівгрупа* $\mathcal{IS}(M)$ *є інверсною*;

4. *при* $|M| > 1$ *напівгрупа* $\mathcal{T}(M)$ *не є інверсною.*

Доведення. 1. Враховуючи, що ідемпотенти bb^{-1} та $a^{-1}a$ можна переставляти, отримуємо:

$$ab \cdot b^{-1}a^{-1} \cdot ab = a \cdot bb^{-1} \cdot a^{-1}a \cdot a = aa^{-1}a \cdot bb^{-1}b = ab.$$

Аналогічно доводиться рівність $b^{-1}a^{-1} \cdot ab \cdot b^{-1}a^{-1} = b^{-1}a^{-1}$.

2. Очевидно.

3. За твердженням 2.9 напівгрупа $\mathcal{IS}(M)$ є регулярною, а за лемою 2.3 кожен ідемпотент з $\mathcal{IS}(M)$ повністю визначається своєю областю визначення. Позначимо через e_A ідемпотент з областю визначення A. Тоді

$$e_A \cdot e_B = e_{A\cap B} = e_{B\cap A} = e_B \cdot e_A\,.$$

Позаяк ідемпотенти комутують, то $\mathcal{IS}(M)$ є інверсною.

4. Позначимо через 0_x елемент із $\mathcal{T}(M)$, який тотожно дорівнює x. Очевидно, що 0_x є ідемпотентом. Нехай тепер a і b — два різні елементи з M. Тоді

$$0_a \cdot 0_b = 0_b \neq 0_a = 0_b \cdot 0_a\,.$$

Позаяк ідемпотенти 0_a і 0_b не комутують, то $\mathcal{T}(M)$ не є інверсною. □

Теорема 2.15 (Вагнер–Престон)**.** *Кожна інверсна напівгрупа* S *ізоморфна деякій піднапівгрупі симетричної інверсної напівгрупи* $\mathcal{IS}(S)$.

Доведення. Кожному елементу $a \in S$ зіставимо відображення $\mu_a : x \mapsto xa$ множини Sa^{-1} у множину Sa.

1. *Відображення* μ_a *є бієкцією множини* Sa^{-1} *на множину* Sa. *Зокрема,* μ_a *є частковою підстановкою множини* S.

Справді, розглянемо відображення $\mu_{a^{-1}} : Sa \to Sa^{-1}$, $y \mapsto ya^{-1}$. Тоді для довільного $x = za^{-1}$ із Sa^{-1} маємо

$$\mu_{a^{-1}}(\mu_a(x)) = (za^{-1} \cdot a) \cdot a^{-1} = z \cdot a^{-1}aa^{-1} = za^{-1} = x\,.$$

Аналогічно доводиться, що $\mu_a(\mu_{a^{-1}}(y)) = y$ для довільного y із Sa. Отже, відображення μ_a і $\mu_{a^{-1}}$ є взаємно оберненими. Зокрема, вони є бієкціями.

2. *Відображення* $a \mapsto \mu_a$ *є ін'єктивним відображенням напівгрупи* S *у напівгрупу* $\mathcal{IS}(S)$.

Припустимо, що $\mu_a = \mu_b$. Тоді $Sa^{-1} = Sb^{-1}$, $Sa = Sb$ і $xa = xb$ для довільного $x \in Sa^{-1}$.

Зауважимо, що для довільного c $Sc^{-1} = Scc^{-1}$. Справді, включення $Sc^{-1} \supseteq Sc \cdot c^{-1}$ очевидне, а зворотне включення випливає із $Sc^{-1} = Sc^{-1} \cdot cc^{-1} \subseteq Scc^{-1}$. Крім того, з рівності $aa^{-1} = aa^{-1} \cdot aa^{-1}$ випливає включення $aa^{-1} \in Saa^{-1}$. А тому з рівності $Sa^{-1} = Sb^{-1}$ випливає існування таких елементів p і q, що $aa^{-1} = pbb^{-1}$, $bb^{-1} = qaa^{-1}$. Тоді

$$aa^{-1} \cdot bb^{-1} \cdot aa^{-1} = pbb^{-1} \cdot bb^{-1} \cdot aa^{-1} = pbb^{-1} \cdot aa^{-1} = aa^{-1} \cdot aa^{-1} = aa^{-1}\,.$$

Аналогічно перевіряється, що $bb^{-1} \cdot aa^{-1} \cdot bb^{-1} = bb^{-1}$. Отже, aa^{-1} і bb^{-1} є інверсними один до одного. З єдиності інверсного елемента випливає, що $aa^{-1} = bb^{-1}$. Але тоді

$$a = aa^{-1}a = \mu_a(aa^{-1}) = \mu_b(aa^{-1}) = aa^{-1} \cdot b = bb^{-1} \cdot b = b\,.$$

3. *Відображення $a \mapsto \mu_a$ є гомоморфізмом напівгрупи S у напівгрупу $\mathcal{IS}(S)$.*

Якщо точка x входить в область визначення кожного з відображень μ_{ab} і $\mu_a\mu_b$, то

$$\mu_{ab}(x) = x \cdot ab = xa \cdot b = \mu_b(\mu_a(x)) = (\mu_a\mu_b)(x)\,.$$

Тому для доведення гомоморфності відображення $a \mapsto \mu_a$ досить показати, що області визначення відображень μ_{ab} і $\mu_a\mu_b$ збігаються. Позаяк

$$\operatorname{dom}\mu_{ab} = S(ab)^{-1} = Sb^{-1}a^{-1}$$

і

$$\operatorname{dom}(\mu_a\mu_b) = (\operatorname{ran}\mu_a \cap \operatorname{dom}\mu_b) \cdot a^{-1} = (Sa \cap Sb^{-1}) \cdot a^{-1}\,,$$

то треба довести, що

$$Sb^{-1}a^{-1} = (Sa \cap Sb^{-1}) \cdot a^{-1}\,. \tag{2.8}$$

Позаяк $Sb^{-1} \supseteq Sa \cap Sb^{-1}$, то включення $Sb^{-1}a^{-1} \supseteq (Sa \cap Sb^{-1}) \cdot a^{-1}$ очевидне.

Навпаки, якщо $x \in Sb^{-1}a^{-1}$, то $x = yb^{-1}a^{-1} = yb^{-1}bb^{-1}a^{-1}aa^{-1}$. Позаяк bb^{-1} і $a^{-1}a$ — ідемпотенти, то $yb^{-1}bb^{-1}a^{-1}a = yb^{-1}a^{-1}abb^{-1}$, а тому $yb^{-1}bb^{-1}a^{-1}a \in Sa \cap Sb^{-1}$. Отже, $x \in (Sa \cap Sb^{-1}) \cdot a^{-1}$ і $Sb^{-1}a^{-1} \subseteq (Sa \cap Sb^{-1}) \cdot a^{-1}$, що й доводить рівність (2.8). $\square$

Частковий автоморфізм універсальної алгебри — це ізоморфізм однієї її підалгебри на іншу. Множина $\mathcal{P}\mathrm{Aut}\, A$ всіх часткових автоморфізмів алгебри $A = (A; \Omega)$ утворює напівгрупу відносно композиції часткових перетворень, яка є піднапівгрупою напівгрупи $\mathcal{IS}(A)$. Зауважимо, що $\mathcal{P}\mathrm{Aut}\, A$ містить нуль і одиницю.

За аналогією з теоремою 2.2 і наслідком 2.1 можна ставити питання: чи кожна інверсна напівгрупа з нулем і одиницею ізоморфна напівгрупі всіх часткових автоморфізмів деякої універсальної алгебри A? Цього разу відповідь негативна[3].

2.9 Задачі

1. Випишіть таблиці Келі всіх попарно неізоморфних напівгруп порядку 2.
2. Якщо S — множина з бінарною дією, то для кожного фіксованого елемента $a \in S$ можна визначити на S *сендвіч-дію* $*_a : x *_a y = xay$.

   a) Доведіть, що коли S є напівгрупою (відповідно групою), то $\langle S, *_a \rangle$ також є напівгрупою (відповідно групою).

   b) Нехай S — напівгрупа з одиницею. З'ясуйте, чи буде $\langle S, *_a \rangle$ напівгрупою з одиницею і яку умову має задовольняти елемент a, щоб напівгрупа $\langle S, *_a \rangle$ була ізоморфною напівгрупі S.
3. Наведіть приклад нескінченної зв'язки, в якій кожний елемент є, з одного боку, нулем для деякої нескінченної піднапівгрупи, а з іншого — одиницею для деякої іншої нескінченної піднапівгрупи.
4. Знайдіть кількість елементів рангу k у напівгрупах: a) IS_n; b) $\mathcal{T}_n$; c) $\mathcal{PT}_n$.
5. Доведіть, що $|\mathfrak{B}_n| = (2n-1)!!$.
6. Доведіть, що коли в напівгрупі S для довільних a і b кожне з рівнянь $ax = b$ і $ya = b$ має розв'язок, то S є групою.
7. a) Нехай $*$ — бінарна дія на множині S, а X — система твірних універсальної алгебри $\langle S, * \rangle$. Припустимо, що рівність $a * (b * c) = (a * b) * c$ виконується для довільних елементів $a, b, c \in X$. Чи випливає звідси, що $\langle S, * \rangle$ є напівгрупою?

   b) Чи зміниться відповідь у попередній задачі, якщо система твірних X складається з одного елемента?
8. Нехай A — n-елементна підмножина напівгрупи $(2^M, \cap)$. Яку найбільшу потужність може мати піднапівгрупа $\langle A \rangle$?

[3] Доманов О. И. Полугруппы всех частичных автоморфизмов универсальных алгебр / О. И. Доманов // Изв. вузов. Математика. — 1971. — № 8 (111). — С. 52–58.

9. Нехай S — одноелементна напівгрупа. Позначимо через $T_n^{(1)}$ напівгрупу, яка одержується з S $(n-1)$-кратним приєднанням одиниці, а через $T_n^{(0)}$ напівгрупу, яка одержується з S $(n-1)$-кратним приєднанням нуля:

   a) доведіть, що напівгрупи $T_n^{(1)}$ і $T_n^{(0)}$ ізоморфні;

   b) доведіть, що кожна підмножина напівгрупи $T_n^{(1)}$ буде піднапівгрупою.

10. Знайдіть необхідну й достатню умову того, щоб кожна піднапівгрупа групи G була групою.

11. Доведіть, що напівгрупи $\langle 2^M, \cap\rangle$ і $\langle 2^M, \cup\rangle$ ізоморфні.

12. Доведіть, що напівгрупа ендоморфізмів алгебри $\langle \mathbb{N}; f\rangle$, де $f(n) = n+1$, ізоморфна напівгрупі $\langle \mathbb{N}_0; +\rangle$.

13. Доведіть, що елемент $\alpha \in \mathcal{PT}_n$ буде ідемпотентом тоді й лише тоді, коли він діє тотожно на своїй області значень.

14. Підрахуйте кількість ідемпотентів у напівгрупах: a) $\mathcal{T}_n$; b) $\mathcal{PT}_n$.

15. Скільки різних піднапівгруп містить моногенна напівгрупа типу
    a) $(5,3)$; b) $(6,1)$; c) $(6,6)$; d) $(7,1)$?

16. Доведіть, що моногенна напівгрупа типу (n,k) має рівно n ідеалів.

17. Опишіть усі конгруенції на моногенній напівгрупі $\langle a\rangle$ типу (n,k) і підрахуйте їхню кількість.

18. Опишіть усі гомоморфні образи напівгрупи $(\mathbb{N}, +)$.

19. Доведіть, що для довільних $n > 1$ і $k \geq 1$ напівгрупа $\mathcal{T}(\mathbb{N})$ містить континуум багато попарно неподібних моногенних піднапівгруп типу (n,k).

20. Доведіть, що для довільних $n > 1$ і $k \geq 1$ напівгрупа $\mathcal{IS}(\mathbb{N})$ містить лише зліченну кількість попарно неподібних моногенних піднапівгруп типу (n,k).

21. Доведіть, що єдиною конгруенцією Ріса на групі G є тотальна конгруенція $\mathbf{i}_G$.

22. Опишіть усі конгруенції на напівгрупі $(\mathbb{N}, +)$. Які з них будуть конгруенціями Ріса?

23. Доведіть, що в напівгрупі S із нулем для кожної конгруенції ρ клас $\overline{0}_\rho$ є ідеалом в S.

24. Нехай I_1, I_2, …, I_n — усі ідеали скінченної напівгрупи S. Доведіть, що a) $I_1 \cdot I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$; b) $I_1 \cdot I_2 \cdots I_n$ є єдиним мінімальним ідеалом напівгрупи S.

25. Доведіть, що кожна підмножина I напівгрупи T буде правим ідеалом тоді й лише тоді, коли T є напівгрупою лівих нулів.

26. Доведіть, що напівгрупа $(\mathbb{N}, \cdot)$ має континуум багато ідеалів.

27. Для кожної з напівгруп a) IS_n, b) $\mathcal{T}_n$, c) $\mathcal{PT}_n$ знайдіть потужність головного лівого ідеалу, породженого елементом рангу k.

28. Доведіть, що в напівгрупі $\mathcal{T}_n$ правий головний ідеал $I_r(\alpha)$, породжений елементом α, збігається з множиною тих $\beta \in S$, для яких із $\alpha(x) = \alpha(y)$ випливає $\beta(x) = \beta(y)$.

29. Доведіть, що в напівгрупі $\mathcal{PT}_n$ правий головний ідеал $I_r(\alpha)$, породжений елементом α, збігається з множиною тих елементів $\beta \in S$, для яких $\operatorname{dom}\beta \subseteq \operatorname{dom}\alpha$ і для довільних $x, y \in \operatorname{dom}\beta$ із $\alpha(x) = \alpha(y)$ випливає $\beta(x) = \beta(y)$.

30. Для кожної з напівгруп a) IS_n, b) $\mathcal{T}_n$, c) $\mathcal{PT}_n$ знайдіть потужність головного правого ідеалу, породженого елементом рангу k.

31. Для кожної з напівгруп a) IS_n, b) $\mathcal{T}_n$, c) $\mathcal{PT}_n$ знайдіть потужність головного двостороннього ідеалу, породженого елементом рангу k.

32. a) Нехай S — напівгрупа. Доведіть, що відображення $\varphi_{a,b} : x \mapsto axb$ буде ін'єктивним ендоморфізмом тоді й лише тоді, коли S — моноїд з одиницею e і $ba = e$.

    b) Нехай S — комутативний моноїд. Доведіть, що відображення $\varphi_{a,b} : x \mapsto axb$ буде ендоморфізмом тоді й лише тоді, коли ab — ідемпотент.

33. Підрахуйте кількість різних головних правих ідеалів у напівгрупах: a) $\mathcal{T}_n$, b) $\mathcal{PT}_n$.

34. Доведіть, що в кожній із напівгруп IS_n, $\mathcal{T}_n$ та $\mathcal{PT}_n$ $\mathcal{D}$-клас, породжений елементом рангу k, містить рівно $\binom{n}{k}$ різних $\mathcal{L}$-класів.

35. Для кожної з напівгруп: a) IS_n, b) $\mathcal{T}_n$, c) $\mathcal{PT}_n$ підрахуйте кількість різних $\mathcal{R}$-класів, що містяться в $\mathcal{D}$-класі, породженому елементом рангу k.

36. Доведіть, що в кожній із напівгруп IS_n, $\mathcal{T}_n$ та $\mathcal{PT}_n$ $\mathcal{R}$-клас, породжений елементом рангу k, містить рівно $\binom{n}{k}k!$ елементів.

37. Для кожної з напівгруп: a) IS_n, b) $\mathcal{T}_n$, c) $\mathcal{PT}_n$ знайдіть кількість елементів, що містяться в $\mathcal{L}$-класі, породженому елементом рангу k.

38. Для кожної з напівгруп: a) IS_n, b) $\mathcal{T}_n$, c) $\mathcal{PT}_n$ знайдіть кількість ідемпотентів, що містяться в $\mathcal{D}$-класі, породженому елементом рангу k.

39. Доведіть, що коли елемент $a \in \mathcal{T}_n$ має ранг k, то клас $\mathcal{L}(a)$ містить k^{n-k} ідемпотентів.

40. Опишіть відношення Ґріна на мультиплікативній напівгрупі матриць $S = \left\{ \left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right) \mid a, b \in \mathbb{R}, a \geq 1, b > 0 \right\}$.

41. Доведіть, що напівгрупа буде регулярною тоді й лише тоді, коли для довільних правого ідеалу R і лівого ідеалу L виконується рівність $R \cap L = RL$.

42. Доведіть, що регулярна напівгрупа містить рівно один ідемпотент тоді й лише тоді, коли вона є групою.

43. Доведіть, що кожна регулярна напівгрупа зі скороченням є групою.

44. Доведіть, що в напівгрупі S будь-які два елементи є взаємно інверсними тоді й лише тоді, коли напівгрупа S антикомутативна (тобто з $ab = ba$ випливає $a = b$).

45. Доведіть, що регулярна напівгрупа S буде інверсною тоді й лише тоді, коли існує антигомоморфізм $\varphi : S \to S$ (тобто $\varphi(ab) = \varphi(b)\varphi(a)$ для довільних $a, b \in S$), який задовольняє такі дві умови: а) φ^2 — тотожний автоморфізм, b) $\varphi(e) = e$ для кожного ідемпотента e.

46. Доведіть, що елементи a і b напівгрупи S є взаємно інверсними і комутують тоді й лише тоді, коли вони є оберненими один до одного елементами деякої підгрупи $H \subseteq S$. Зокрема, якщо кожний елемент інверсної напівгрупи S комутує зі своїм інверсним, то S є об'єднанням груп.

47. Доведіть, що коли для довільної четвірки a, b, c, d елементів напівгрупи S із рівності $ab = cd$ випливає, що $a = c$ або $b = d$, то або S є напівгрупою лівих одиниць, або S є напівгрупою правих одиниць.

48.* Нехай на компактному гаусдорфовому топологічному просторі S визначена асоціативна дія $* : S \times S \to S$, яка неперервна за кожним з аргументів. Доведіть, що напівгрупа $\langle S, * \rangle$ містить ідемпотент.

3 Решітки

3.1 Решітки

Нехай M — частково впорядкована множина. Елемент b називається *нижньою гранню* підмножини $A \subseteq M$, якщо для кожного $a \in A$ виконується нерівність $b \leq a$. Аналогічно визначається *верхня грань* підмножини A.

Нижня грань множини A називається *точною*, якщо вона більша за будь-яку іншу нижню грань цієї множини. Іншими словами, точна нижня грань множини A — це найбільший елемент множини всіх нижніх граней множини A. Якщо точна нижня грань множини A існує, то позначаємо її $\inf A$.

Аналогічно визначається *точна верхня грань* множини A (позначається $\sup A$).

Найбільший елемент частково впорядкованої множини M (якщо він існує) будемо називати *одиницею* і позначати символом 1. Аналогічно найменший називатимемо *нулем* і позначатимемо 0. Якщо M містить одиницю (відповідно нуль), то зручно покласти $\inf(\varnothing) = 1$ (відповідно $\sup(\varnothing) = 0$).

Нагадаємо, що *ланцюгом* називається лінійно впорядкована множина.

Лема 3.1 (Куратовський–Цорн)**.** *Якщо в частково впорядкованій множині M кожен ланцюг має верхню грань, то в M є максимальний елемент.*

Можна показати (див., наприклад, [10], § 1.6), що ця лема еквівалентна аксіомі вибору. Зрозуміло, що вибір із кількох еквівалентних тверджень того, яке вважати аксіомою (тоді решта тверджень стають теоремами) є справою домовленості та зручності. Так, у геометрії аксіома паралельності зараз формулюється зазвичай не в тому вигляді, який вона мала в Евкліда. Позаяк в алгебрі лема Куратовського–Цорна використовується дуже часто (зокрема, ми вже застосовували її в розділі 1 при доведенні теореми Біркгофа), то нам зручно вважати аксіомою саме її.

Лему 3.1 часто називають просто *лемою Цорна*, хоча Куратовський довів її значно раніше. Нехтування питаннями пріоритету викликане не тільки тим, що друга назва коротша. Саме Цорн у кінці 1930-х рр. дав перші яскраві приклади застосування цієї леми. Із того часу лема

Куратовського–Цорна стала популярною і майже витіснила доведення з використанням трансфінітної індукції.

Як типовий приклад застосування цієї леми, розглянемо доведення наступної теореми, на яку ми вже посилалися в розділі 2. Через $a_\triangle$ і $a^\triangledown$ позначаються відповідно *нижній* $\{x \in M \mid x \leq a\}$ і *верхній* $\{y \in M \mid y \geq a\}$ *конуси* елемента $a \in M$.

Теорема 3.1 (Шпільрайн)**.** *Кожен частковий порядок $<$ на множині M можна продовжити до лінійного порядку.*

Доведення. Часткові порядки розглядаємо як бінарні відношення на множині M (тобто як підмножини з $M \times M$). Розглянемо множину S усіх продовжень порядку $<$, упорядковану за включенням (множина S не порожня, бо містить початковий порядок $<$). Кожен ланцюг множини S буде обмежений згори об'єднанням елементів цього ланцюга. За лемою Цорна у множині S є максимальні елементи. Якщо для часткового порядку $<$ існують непорівняльні елементи a і b, то його можна продовжити: легко перевіряється, що $< \cup \{(x, y) \mid x \in a_\triangle,\ y \in b^\triangledown\}$ також є частковим порядком. Тому максимальні елементи є лінійними порядками. □

Зауважимо, що для скінченних множин теорему Шпільрайна можна доводити індукцією за потужністю часткового порядку (як бінарного відношення на M). Інший спосіб: перенумерацією елементів частково впорядкованої множини матрицю інцидентності часткового порядку можна зробити верхньою трикутною, після чого верхній трикутник матриці заповнити одиницями.

Якщо точна нижня грань існує для довільних двох елементів, то частково впорядкована множина M називається *нижньою напіврешіткою*. У цьому випадку взяття точної нижньої грані можна розглядати як бінарну операцію на M, яку зазвичай позначають символом $\wedge$. Таким чином, $a \wedge b = \inf(a, b)$.

Аналогічно *верхньою напіврешіткою.* називається частково впорядкована множина M, у якій для довільних двох елементів існує точна верхня грань. Відповідну бінарну операцію на M позначають символом $\vee$ (тобто $a \vee b = \sup(a, b)$).

Частково впорядкована множина, яка є як нижньою напіврешіткою, так і верхньою, називається просто *решіткою*[4].

[4] У теорії решіток поруч із символом $\vee$ часто використовують знак додавання, а поруч із символом $\wedge$ — знак множення. Це інколи полегшує читання формул.

Вправа 3.1. *Доведіть, що кожна нижня (відповідно верхня) напівре-шітка утворює відносно операції $a \wedge b$ (відповідно $a \vee b$) комутативну інверсну ідемпотентну напівгрупу.*

Приклади. **1**. Кожна лінійно впорядкована множина M є решіткою. Справді, в цьому випадку для довільних двох елементів a і b маємо $\inf(a,b) = \min(a,b)$, $\sup(a,b) = \max(a,b)$.

2. Упорядкована за включенням множина $\mathfrak{B}(M)$ усіх підмножин множини M також буде решіткою: $\inf(A,B) = A \cap B$, $\sup(A,B) = A \cup B$. Ця решітка містить одиницю M і нуль $\varnothing$.

3. Оскільки перетин і об'єднання двох скінченних множин також буде скінченною множиною, то решіткою буде і впорядкована за включенням множина $\mathfrak{B}_{fin}(M)$ усіх скінченних підмножин множини M.

4. Якщо частковий порядок на множині визначити за допомогою відношення подільності (тобто покладемо $m \preceq n$ тоді й лише тоді, коли $m \mid n$), то знову отримаємо решітку. У цьому випадку $\inf(m,n) = \text{НСД}(m,n)$ і $\sup(m,n) = \text{НСК}(m,n)$. Цю решітку позначатимемо $(\mathbb{N}, \mid)$.

Багато прикладів решіток дає алгебра. Головними з них є впорядковані за включенням множина $\mathrm{Sub}(A)$ усіх підалгебр універсальної алгебри A та множина $\mathrm{Con}(A)$ усіх конгруенцій на алгебрі A. Із решітками конгруенцій відповідних алгебр тісно пов'язані такі решітки, як решітка всіх нормальних підгруп групи, решітка ідеалів кільця, решітка підпросторів векторного простору і т. д.

Частковий порядок $\preceq$ називається *двоїстим* до часткового порядку $\leq$, якщо $a \preceq b$ тоді й лише тоді, коли $b \leq a$. Очевидно, що частково впорядкована множина, двоїста до нижньої напіврешітки (верхньої напіврешітки, решітки), буде верхньою напіврешіткою (нижньою напіврешіткою, решіткою).

Із леми 2.3 випливає, що зіставляючи кожному ідемпотенту з напівгрупи $\mathcal{IS}(M)$ його область визначення, одержуємо бієкцію між ідемпотентами напівгрупи $\mathcal{IS}(M)$ та елементами решітки $\mathfrak{B}(M)$. Ця бієкція є навіть ізоморфізмом між напівгрупами $E(\mathcal{IS}(M))$ і $\langle \mathfrak{B}(M); \cap \rangle$, позаяк областю визначення добутку ef двох ідемпотентів з $\mathcal{IS}(M)$ є перетин областей визначення множників. Із цього зауваження, вправи 3.1 і теореми Вагнера–Престона отримуємо

Твердження 3.1. *Кожна нижня напіврешітка S занурюється в решітку $\mathfrak{B}(S)$.*

Зауважимо, що занурення $S \hookrightarrow \mathfrak{B}(S)$, про яке йдеться в цьому твердженні, є саме зануренням напіврешіток, бо при цьому зберігається не тільки частковий порядок, а й точні нижні грані переходять у точні нижні грані.

Ураховуючи двоїстість операцій $\cup$ і $\cap$ у решітці $\mathfrak{B}(M)$, після переходу до доповнень аналогічне твердження можна отримати і для верхніх напіврешіток.

Легко зрозуміти, що коли точна нижня (або верхня) грань існує для довільних двох елементів, то відповідна точна грань існує і для довільної скінченної кількості елементів. Але для нескінченних підмножин точних граней може і не існувати. Якщо ж точна нижня грань існує для довільної підмножини, то говоримо про *повну нижню напіврешітку*. Очевидно, що кожна повна нижня напіврешітка містить нуль — це буде точна нижня грань множини всіх елементів.

Аналогічно визначається *повна верхня напіврешітка*. Вона завжди містить одиницю — точну верхню грань множини всіх елементів. Якщо ж для довільної підмножини існують обидві точні грані, то говоримо про *повну решітку*. Така решітка містить і нуль, і одиницю.

Твердження 3.2. *Якщо частково впорядкована множина M із одиницею є повною нижньою напіврешіткою, то M є повною верхньою напіврешіткою.*

Доведення. Досить довести існування точної верхньої грані для $A \neq \varnothing$. Множина B всіх верхніх граней для A непорожня, оскільки містить 1. Розглянемо $b = \inf B$. Позаяк кожен елемент $a \in A$ є нижньою гранню для B, то $a \leq b$ для всіх $a \in A$. Тому b є верхньою гранню для A. Із означення b одразу випливає, що $b = \sup A$. $\square$

Зрозуміло, що кожна скінченна решітка буде повною. Серед нескінченних лінійно впорядкованих множини повні решітки є швидше винятком, ніж правилом. Зокрема, жодна з множин $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ із звичайним відношенням порядку не є повною решіткою. Але якщо поповнити $\mathbb{R}$ найбільшим елементом ∞ і найменшим елементом $-\infty$, то одержимо повну решітку.

Важливим прикладом повної решітки є $\mathfrak{B}(M)$. Повними є і решітка $\mathrm{Sub}(A)$ усіх підалгебр універсальної алгебри A та решітка $\mathrm{Con}(A)$ усіх конгруенцій на алгебрі A (це випливає із тверджень 1.1 і 3.2 і вправи 1.3).

Найбільший спільний дільник існує для довільної множини натуральних чисел. Але найменше спільне кратне існує лише для скінчен-

них множин натуральних чисел. Тому $(\mathbb{N}, |)$ є лише повною нижньою напіврешіткою.

Вправа 3.2. *Нехай A — універсальна алгебра. Доведіть, що перетин довільних класів конгруентності з A є або порожньою множиною, або класом конгруентності. Зокрема, поповнена порожньою множиною множина всіх класів конгруентності з A утворює відносно включення повну решітку.*

У випадку груп це дає решітку класів суміжності за нормальними підгрупами; у випадку векторних підпросторів — решітку лінійних многовидів.

Відображення $\varphi : M \to M$ частково впорядкованої множини M у себе називається ендоморфізмом, якщо для довільних $a, b \in M$ із $a \leq b$ випливає $\varphi(a) \leq \varphi(b)$. Наступна теорема має численні застосування.

Теорема 3.2 (Тарський, 1955)**.** *Кожний ендоморфізм повної решітки має нерухому точку.*

Доведення. Нехай $\varphi : L \to L$ — ендоморфізм повної решітки L. Покладемо $A = \{x \in L \mid x \leq \varphi(x)\}$ і нехай $a = \sup A$. Для довільного $x \in A$ із $x \leq a$ випливає $\varphi(x) \leq \varphi(a)$, а оскільки $x \leq \varphi(x)$, то $x \leq \varphi(a)$. Тому $\varphi(a)$ є верхньою гранню множини A. Але тоді

$$a \leq \varphi(a)\,. \tag{3.1}$$

Зауважимо тепер, що з (3.1) випливає нерівність $\varphi(a) \leq \varphi^2(a)$. Отже, $\varphi(a) \in A$. Але тоді $\varphi(a) \leq a$. Разом із (3.1) це дає $\varphi(a) = a$. □

Того ж року Дейвіс показав, що коли кожен ендоморфізм L решітки має нерухому точку, то решітка є повною. Таким чином, властивість мати нерухому точку є характеристичною для повних решіток[5].

Універсальна алгебра L сигнатури $(\vee, \wedge)$ називається *решіткою*, якщо в ній виконуються такі аксіоми:

(1) $a \vee a = a$, $\quad a \wedge a = a$ (закони ідемпотентності);
(2) $a \vee b = b \vee a$, $\quad a \wedge b = b \wedge a$ (закони комутативності);
(3) $a \vee (b \vee c) = (a \vee b) \vee c$, $\quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (закони асоціативності);
(4) $a \vee (a \wedge b) = a$, $\quad a \wedge (a \vee b) = a$ (закони поглинання).

[5]Доведення теореми Дейвіса є в книзі Скорняков Л.А. Элементы теории структур. — М., Наука, 1982.

Задача 3.1. *Доведіть, що аксіоми ідемпотентності випливають із решти аксіом решітки.* (*Вказівка.* $a = a \wedge (a \vee a) \Rightarrow a \vee a = a \vee (a \wedge (a \vee a)) = a$.)

Аксіоми, які визначають решітку, є двоїстими одна до одної: якщо в якійсь із аксіом замінити всі знаки $\vee$ на $\wedge$ і навпаки, то знову отримаємо аксіому. Звідси випливає

Принцип двоїстості для решіток: *якщо з аксіом решітки виводиться рівність $u = v$, то після заміни в цій рівності всіх знаків $\vee$ на $\wedge$ і навпаки знову отримаємо правильну рівність.*

Кожна решітка як частково впорядкована множина перетворюється в решітку як універсальну алгебру, якщо покласти

$$a \vee b := \sup(a, b), \quad a \wedge b := \inf(a, b) \tag{3.2}$$

(виконання співвідношень (1)–(4) легко перевіряється). Зворотний перехід від решітки як універсальної алгебри до решітки як частково впорядкованої множини теж робиться легко. Справді, покладемо

$$a \leq b : \Leftrightarrow \ a \wedge b = a\,. \tag{3.3}$$

З ідемпотентності операції $\wedge$ випливає, що визначене таким чином відношення $\leq$ є рефлексивним. Із комутативності $\wedge$ випливає, що одночасне виконання співвідношень $a \leq b$ і $b \leq a$ рівносильне виконанню рівностей $a \wedge b = a$ і $a \wedge b = b$. Отже, у цьому випадку $a = b$, а тому відношення $\leq$ є антисиметричним. Нарешті, якщо $a \leq b$ і $b \leq c$, то з рівностей $a \wedge b = a$ і $b \wedge c = b$ та асоціативності отримуємо

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a.$$

Тому відношення $\leq$ є транзитивним. Отже, відношення $\leq$ є відношенням часткового порядку.

Зауваження. Замість (3.3) відношення порядку в решітці $\langle L; \vee, \wedge \rangle$ можна визначати правилом $a \leq b : \Leftrightarrow \ a \vee b = b$. Вийде те саме відношення порядку, тому що рівності $a \wedge b = a$ й $a \vee b = b$ рівносильні. Справді, якщо $a \wedge b = a$, то за законом поглинання $a \vee b = (a \wedge b) \vee b = b$. Обернена імплікація доводиться аналогічно.

Покажемо, що для цього відношення порядку $\inf(a, b)$ збігається з $a \wedge b$, а $\sup(a, b)$ збігається з $a \vee b$. Справді,

$$(a \wedge b) \wedge a = a \wedge (b \wedge a) = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$$

і, аналогічно, $(a \wedge b) \wedge b = a \wedge b$. Отже, $a \wedge b \leq a$ і $a \wedge b \leq b$, тобто $a \wedge b$ є нижньою гранню елементів a і b. Нарешті, якщо $c \leq a$ і $c \leq b$, то $c \wedge a = c$ і $c \wedge b = c$. Але тоді

$$c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c\,,$$

тобто $c \leq (a \wedge b)$. Отже, $a \wedge b$ є найбільшою з нижніх граней елементів a і b, тобто точною нижньою гранню цих елементів.

Те, що $\sup(a, b)$ збігається з $a \vee b$, доводиться аналогічно, лише з використанням правила $a \leq b : \Leftrightarrow\ a \vee b = b$.

Таким чином, на решітку як частково впорядковану множину і на решітку як універсальну алгебру можна дивитися як на один і той самий об'єкт, описаний двома мовами. Тому для цих двох понять вживається один термін, і надалі, говорячи про решітку, ми розглядатимемо її, залежно від контексту, то як частково впорядковану множину, то як універсальну алгебру.

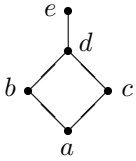
Зауваження. Замість (3.3) відношення порядку в решітці $\langle L; \vee, \wedge \rangle$ можна визначати правилом $a \leq b : \Leftrightarrow\ a \vee b = b$. Вийде те саме відношення порядку, тому що рівності $a \wedge b = a$ й $a \vee b = b$ рівносильні. Справді, якщо $a \wedge b = a$, то за законом поглинання $a \vee b = (a \wedge b) \vee b = b$. Обернена імплікація доводиться аналогічно.

Вправа 3.3. **1.** *Доведіть, що в решітці з нерівностей $a \leq b$ і $c \leq d$ випливають нерівності $a \vee c \leq b \vee d$ і $a \wedge c \leq b \wedge d$.*

2. *Доведіть, що декартів добуток решіток також є решіткою.*

Підмножина B решітки L називається *підрешіткою*, якщо вона є підалгеброю алгебри $\langle L; \vee, \wedge \rangle$. Таким чином, підмножина решітки, яка сама є решіткою відносно індукованого часткового порядку, і підрешітка — це різні речі: точні нижня і верхня грані відносно порядку, індукованого на B, можуть не збігатися з відповідними гранями в самій решітці L.

Наприклад, для решітки з діаграмою



підмножина $\{a, b, c, d\}$ буде підрешіткою, а підмножина $\{a, b, c, e\}$ хоч і є решіткою відносно індукованого порядку, але підрешіткою не є.

3.2 Дистрибутивні решітки

Решітка $\langle L; \vee, \wedge \rangle$ називається *дистрибутивною*, якщо для довільних $a, b, c \in L$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{3.4}$$

Закони (3.4) є двоїстими один до одного, тому в дистрибутивних решітках також виконується принцип двоїстості.

Задача 3.2. *Доведіть, що дистрибутивні закони* (3.4) *рівносильні, тобто що кожен із них виводиться з іншого.* (Увага! При розв'язуванні цієї задачі принцип двоїстості використовувати не можна!)

Приклади. **1**. Із рівності

$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c)) \tag{3.5}$$

і задачі 3.2 випливає, що кожна лінійно впорядкована множина є дистрибутивною решіткою.

2. Дистрибутивність решітки $\mathfrak{B}(M)$ усіх підмножин даної множини M випливає з рівностей

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \ \text{ і } \ A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Зрозуміло, що кожна підрешітка дистрибутивної решітки сама буде дистрибутивною.

Вправа 3.4. *Доведіть, що декартів добуток дистрибутивних решіток також є дистрибутивною решіткою.*

Задача 3.3. *Доведіть, що впорядкована за допомогою відношення подільності решітка* $\langle \mathbb{N}; | \rangle$ *є дистрибутивною.*

Твердження 3.3. *Множина лівих (правих, двосторонніх) ідеалів напівгрупи утворює відносно операцій* $\cup$ *і* $\cap$ *дистрибутивну решітку.*

Доведення. Позаяк об'єднання і перетин лівих (правих, двосторонніх) ідеалів напівгрупи також є лівим (правим, двостороннім) ідеалом. Тому множина лівих (правих, двосторонніх) ідеалів напівгрупи S є підрешіткою решітки $\mathfrak{B}(S)$. □

Лема 3.2. *У дистрибутивній решітці з рівностей* $a \vee c = b \vee c$ *і* $a \wedge c = b \wedge c$ *випливає рівність* $a = b$.

Доведення випливає з наступного ланцюжка рівностей:

$$a = a \vee (a \wedge c) = a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) =$$

$$= (a \vee b) \wedge (b \vee c) = b \vee (a \wedge c) = b \vee (b \wedge c) = b. \qquad \square$$

Лема 3.3. *Кожна підпрямо нерозкладна дистрибутивна решітка містить не більше двох елементів.*

Доведення. Припустимо, що дистрибутивна решітка L містить ≥ 3 елементів. Тоді в L можна вибрати ланцюг $a < b < c$ (це очевидно, якщо L є ланцюгом; якщо ж в L є непорівняльні елементи x і y, то можна взяти ланцюг $x \wedge y < x < x \vee y$). Розглянемо нижній $b_\triangle = \{x \mid x \leq b\}$ і верхній $b^\triangledown = \{y \mid y \geq b\}$ конуси елемента b і відображення

$$\varphi : L \to b_\triangle \times b^\triangledown, \qquad x \mapsto (x \wedge b, x \vee b). \tag{3.6}$$

Тоді

$$\varphi(x \vee y) = \big((x \vee y) \wedge b, (x \vee y) \vee b\big) = \big((x \wedge b) \vee (y \wedge b), (x \vee b) \vee (y \vee b)\big) =$$
$$= (x \wedge b, x \vee b) \vee (y \wedge b, y \vee b) = \varphi(x) \vee \varphi(y)$$

і

$$\varphi(x \wedge y) = \big((x \wedge y) \wedge b, (x \wedge y) \vee b\big) = \big((x \wedge b) \wedge (y \wedge b), (x \vee b) \wedge (y \vee b)\big) =$$
$$= (x \wedge b, x \vee b) \wedge (y \wedge b, y \vee b) = \varphi(x) \wedge \varphi(y).$$

Отже, φ — гомоморфізм решіток. Крім того, якщо $\varphi(x) = \varphi(y)$, то $x \wedge b = y \wedge b$ і $x \vee b = y \vee b$, звідки, за лемою 3.2, $x = y$. Тому φ — мономорфізм.

Очевидно, що при кожній із канонічних проекцій $\pi_{b_\triangle}$, $\pi_{b^\triangledown}$ прямого добутку $b_\triangle \times b^\triangledown$ на множники $b_\triangle$, $b^\triangledown$ образ $\varphi(L)$ проектується на весь множник. Однак

$$\pi_{b_\triangle}(\varphi(b)) = \pi_{b_\triangle}(\varphi(c)) = b, \qquad \pi_{b^\triangledown}(\varphi(b)) = \pi_{b^\triangledown}(\varphi(a)) = b,$$

тобто проекція $\varphi(L)$ на кожен із множників $b_\triangle, b^\triangledown$ не є ізоморфізмом. Таким чином, L розкладена в нетривіальний підпрямий добуток решіток $b_\triangle$ і $b^\triangledown$. $\square$

Теорема 3.3. *Кожна дистрибутивна решітка ізоморфна деякій решітці множин (тобто підрешітці решітки всіх підмножин деякої множини). Зокрема, кожна скінченна дистрибутивна решітка ізоморфна деякій підрешітці решітки всіх підмножин деякої скінченної множини.*

Доведення. За теоремою Біркгофа (теорема 1.7) кожна універсальна алгебра розкладається в підпрямий добуток підпрямо нерозкладних алгебр. Тому з леми 3.3 випливає, що дистрибутивна решітка L розкладається у підпрямий добуток $L \hookrightarrow \prod_{i\in I} U_i$ двоелементних решіток $U_i = \{0,1\}$. Елементи з $\prod_{i\in I} U_i$ природно розглядати як характеристичні функції підмножин із I. Крім того, із доведення леми 3.3 випливає, що для скінченної решітки L множина I також скінченна. □

3.3 Модулярні решітки

Для кожної пари $a \le c$ елементів частково впорядкованої множини L можна визначити *інтервал* $[a,c] := \{x \mid a \le x \le c\}$. Зрозуміло, що коли L є решіткою, то кожний інтервал є підрешіткою.

Для кожного інтервалу $[a,c]$, $a \le c$, решітки $\langle L; \vee, \wedge\rangle$ можна визначити так звані *відображення проектування* решітки на цей інтервал:

$$\lambda_{[a,c]} : x \mapsto a \vee (x \wedge c), \quad \rho_{[a,c]} : x \mapsto (a \vee x) \wedge c. \tag{3.7}$$

Зокрема, для довільного $x \in [a,c]$ маємо

$$\lambda_{[a,c]}(x) = a \vee (x \wedge c) = a \vee x = x \ \text{ і } \ \rho_{[a,c]}(x) = (a \vee x) \wedge c = x \wedge c = x\,.$$

Отже, точки інтервалу $[a,c]$ при цих відображеннях лишаються нерухомими (саме тому ці відображення називаються проектуваннями). Крім того маємо такі імплікації:

$$x \le y \ \Rightarrow \ x \wedge c \le y \wedge c \ \Rightarrow \ a \vee (x \wedge c) \le a \vee (y \wedge c) \ \Rightarrow \ \lambda_{[a,c]}(x) \le \lambda_{[a,c]}(y)\,.$$

Аналогічно доводиться, що й відображення $\rho_{[a,c]}$ зберігає відношення порядку.

Вправа 3.5. *Перевірте, що*

$$\lambda_{[a,c]} = \lambda^2_{[a,c]} = \lambda_{[a,c]}\rho_{[a,c]}, \qquad \rho_{[a,c]}\lambda_{[a,c]} = \rho^2_{[a,c]} = \rho_{[a,c]}.$$

Оскільки $x \le a \vee x$, то $x \wedge c \le (a \vee x) \wedge c$. Крім того, $a \le (a \vee x) \wedge c$. Тому для довільного $x \in L$ виконується нерівність

$$\lambda_{[a,c]}(x) = a \vee (x \wedge c) \le (a \vee x) \wedge c = \rho_{[a,c]}(x)\,. \tag{3.8}$$

Якщо в (3.8) для всіх x має місце рівність, то інтервал $[a, c]$ називається *модулярним*. Решітка $\langle L; \vee, \wedge \rangle$, в якій кожен інтервал є модулярним, називається *модулярною* (або *дедекіндовою*). Іншими словами, решітка $\langle L; \vee, \wedge \rangle$ називається *модулярною*, якщо

для довільних $a, b, c \in L$ *із нерівності* $a \leq c$ *випливає рівність*

$$(a \vee b) \wedge c = a \vee (b \wedge c)\,. \tag{3.9}$$

Легко бачити, що аксіома модулярності є самодвоїстою (для цього нерівність $a \leq c$ краще переписати у вигляді $a \wedge c = a$). Тому для модулярних решіток також виконується принцип двоїстості.

Важливість модулярних решіток для алгебри пояснюється просто: решітка всіх конгруенцій на алгебричній системі дуже часто є модулярною. Зокрема, це так для груп і кілець (див. задачі 26 і 27).

Вправа 3.6. **1.** *Доведіть, що кожна дистрибутивна решітка є модулярною.*

1. *Доведіть, що декартів добуток модулярних решіток також є модулярною решіткою.*

Теорема 3.4. *Якщо конгруенції на універсальній алгебрі A комутують як бінарні відношення, то решітка $Con(A)$ її конгруенцій буде модулярною.*

Доведення розіб'ємо на кілька кроків.

1. *Якщо відношення еквівалентності φ і ψ комутують (тобто $\varphi \circ \psi = \psi \circ \varphi$), то їх добуток $\varphi \circ \psi$ є відношенням еквівалентності.* Справді, рефлексивність добутку $\varphi \circ \psi$ очевидна. Якщо $(a, c) \in \varphi \circ \psi$, то існує таке b, що $(a, b) \in \varphi$, $(b, c) \in \psi$. Але тоді $(c, b) \in \psi$ і $(b, a) \in \varphi$, звідки $(c, a) \in \psi \circ \varphi$. Тому $(c, a) \in \varphi \circ \psi$ і добуток $\varphi \circ \psi$ є симетричним відношенням. Нарешті, якщо ще $(c, e) \in \varphi \circ \psi$, то існує таке d, що $(c, d) \in \varphi$, $(d, e) \in \psi$. Позаяк $(b, d) \in \psi \circ \varphi$, то $(b, d) \in \varphi \circ \psi$ і для деякого x буде $(b, x) \in \varphi$, $(x, d) \in \psi$. Із транзитивності φ і ψ випливає, що $(a, x) \in \varphi$, $(x, e) \in \psi$, а тому $(a, e) \in \varphi \circ \psi$. Отже, добуток $\varphi \circ \psi$ є й транзитивним відношенням.

2. *Якщо відношення еквівалентності φ і ψ комутують, то добуток $\varphi \circ \psi$ є найменшим відношенням еквівалентності, яке містить φ і ψ.* Справді, із рефлексивності φ і ψ випливає, що $\varphi \cup \psi \subseteq \varphi \circ \psi$. З іншого боку, якщо відношення еквівалентності τ містить φ і ψ, то з транзитивності τ випливає, що воно містить і $\varphi \circ \psi$.

3. *Якщо конгруенції φ і ψ комутують, то їх добуток $\tau = \varphi \circ \psi$ також є конгруенцією.* Справді, із попереднього випливає, що τ є відношенням еквівалентності. Нехай $\omega : A^n \to A$ — довільна n-арна операція з A. Припустимо, що $(a_1, c_1), \ldots, (a_n, c_n) \in \tau$. Тоді існують такі $b_1, \ldots, b_n$, що

$$(a_1, b_1), \ldots, (a_n, b_n) \in \varphi, \quad (b_1, c_1), \ldots, (b_n, c_n) \in \psi.$$

Звідси випливає, що

$$\big(\omega(a_1,\dots,a_n),\omega(b_1,\dots,b_n)\big)\in\varphi,\quad \big(\omega(b_1,\dots,b_n),\omega(c_1,\dots,c_n)\big)\in\psi\,.$$

Але тоді

$$\big(\omega(a_1,\dots,a_n),\omega(c_1,\dots,c_n)\big)\in\tau\,.$$

Отже, відношення τ узгоджене з усіма операціями з A і є конгруенцією.

4. Таким чином, якщо конгруенції комутують, то в упорядкованій за включенням решітці $\mathrm{Con}(A)$ маємо $\inf(\varphi,\psi)=\varphi\cap\psi$, $\sup(\varphi,\psi)=\varphi\circ\psi$. Тому для доведення модулярності лишилося показати, що коли $\varphi\subseteq\tau$, то

$$(\varphi\circ\psi)\cap\tau=\varphi\circ(\psi\cap\tau)\,. \tag{3.10}$$

Нехай $(a,c)\in(\varphi\circ\psi)\cap\tau$. Тоді $(a,c)\in\tau$ та існує таке b, що $(a,b)\in\varphi$, $(b,c)\in\psi$. Позаяк $\varphi\subseteq\tau$, то $(a,b)\in\tau$. Із симетричності та транзитивності τ випливає, що $(b,c)\in\tau$. Отже, $(b,c)\in\psi\cap\tau$. Але тоді $(a,c)\in\varphi\circ(\psi\cap\tau)$.

Навпаки, нехай $(a,c)\in\varphi\circ(\psi\cap\tau)$. Тоді існує таке b, що $(a,b)\in\varphi$ і $(b,c)\in\psi\cap\tau$. Тоді $(a,c)\in\varphi\circ\psi$. Крім того, з $(a,b),(b,c)\in\tau$ і того, що τ — відношення еквівалентності, випливає, що $(a,c)\in\tau$. Отже, $(a,c)\in(\varphi\circ\psi)\cap\tau$, що завершує доведення (3.10). □

Твердження 3.4. *Решітка підпросторів векторного простору є модулярною.*

Доведення. Нехай $V\subseteq W$. Якщо $\boldsymbol{a}\in V+(W\cap U)$, то $\boldsymbol{a}=\boldsymbol{v}+\boldsymbol{w}$, де $\boldsymbol{v}\in V$, $\boldsymbol{w}\in(W\cap U)$. Позаяк обидва доданки з W, то $\boldsymbol{a}\in W$. Включення $\boldsymbol{a}\in(V+U)$ очевидне. Отже, $\boldsymbol{a}\in W\cap(V+U)$.

Якщо $\boldsymbol{a}\in W\cap(V+U)$, то $\boldsymbol{a}\in W$ і $\boldsymbol{a}=\boldsymbol{v}+\boldsymbol{u}$, де $\boldsymbol{v}\in V$, $\boldsymbol{u}\in U$. Але тоді $\boldsymbol{u}=\boldsymbol{a}-\boldsymbol{v}\in W$ і $\boldsymbol{a}\in V+(W\cap U)$. □

Задача 3.4. *Виведіть твердження* 3.4 *із задачі* 15 *і теореми* 3.4.

Якщо L частково впорядкована множина з найменшим елементом 0, то мінімальні елементи множини $L\setminus\{0\}$ називаються *атомами*.

Нехай L — решітка з найменшим елементом 0 і найбільшим елементом 1. Скінченний ланцюг $0<a_1<\dots<a_{n-1}<1$, який не ущільнюється, називається *композиційним рядом*. Зокрема, елемент a_1 такого ланцюга є атомом.

Головні ідеальні ряди, з якими ми зустрічалися в підрозділі 2.5, є ні чим іншим як композиційними рядами в решітці ідеалів напівгрупи. В інших конкретних решітках композиційні ряди також можуть мати власні назви. Наприклад, композиційні ряди в решітці нормальних підгруп групи називають *головними рядами*, а в решітці підпросторів скінченновимірного простору — *максимальними прапорами*.

Теорема 3.5 (Теорема про ущільнення). *У модулярній решітці будь-які два скінченні ланцюги зі спільними початком і кінцем можна ущільнити до ланцюгів однакової довжини.*

Доведення. Нехай L — модулярна решітка і

$$a = c_0 < c_1 < \cdots < c_{k-1} < c_k = b, \quad a = d_0 < d_1 < \cdots < d_{m-1} < d_m = b \quad (3.11)$$

— два скінченні ланцюги зі спільними початком a і кінцем b, які ми позначимо L_c і L_d. Аналогічно (3.7) для кожного інтервалу $[d_i, d_{i+1}]$ $(0 \le i < m)$ решітки L визначимо відображення

$$L_c \to [d_i, d_{i+1}], \quad c_j \mapsto d_{ij} = d_i \vee (c_j \wedge d_{i+1}),$$

а для кожного інтервалу $[c_j, c_{j+1}]$ $(0 \le j < k)$ — відображення

$$L_d \to [c_j, c_{j+1}], \quad d_i \mapsto c_{ji} = c_j \vee (d_i \wedge c_{j+1}).$$

Ураховуючи, що

$$c_{jm} = c_{j+1} = c_{j+1,0} \ (0 \le j < k) \quad \text{і} \quad d_{ik} = d_{i+1} = d_{i+1,0} \ (0 \le i < m),$$

одержуємо, що перший із ланцюгів (3.11) ущільнюється до послідовності

$$a = c_{00} \le c_{01} \le \cdots \le c_{0m} \le c_{11} \le \cdots \le c_{1m} \le \cdots \\ \cdots \le c_{k-2,m} \le c_{k-1,1} \le \cdots \le c_{k-1,m} = b, \quad (3.12)$$

а другий — до послідовності

$$a = d_{00} \le d_{01} \le \cdots \le d_{0k} \le d_{11} \le \cdots \le d_{1k} \le \cdots \\ \cdots \le d_{m-2,k} \le d_{m-1,1} \le \cdots \le d_{m-1,k} = b, \quad (3.13)$$

кожна з яких містить $km+1$ членів. Для доведення леми лишилось показати, що коли ми в кожній із послідовностей (3.12) і (3.13) викреслимо повторення, то одержимо ланцюги однакової довжини. А для цього досить показати, що кількість повторень у послідовностях (3.12) і (3.13) однакова.

Справді, нехай

$$c_{ji} = c_{j,i+1}, \quad \text{тобто } c_j \vee (d_i \wedge c_{j+1}) = c_j \vee (d_{i+1} \wedge c_{j+1}) \quad (3.14)$$

(зауважимо, що рівності $c_{jm} = c_{j+1,1}$ також можна надати такого вигляду, бо за означенням $c_{jm} = c_{j+1,0}$). Ураховуючи нерівності

$d_i \wedge c_{j+1} \le d_{i+1}$ і $d_{i+1} \wedge c_{j+1} \le d_{i+1}$, модулярність решітки та рівність (3.14), маємо

$$(c_{j+1} \wedge d_i) \vee (c_j \wedge d_{i+1}) = \big((c_{j+1} \wedge d_i) \vee c_j\big) \wedge d_{i+1} =$$
$$= \big((c_{j+1} \wedge d_{i+1}) \vee c_j\big) \wedge d_{i+1} = (c_{j+1} \wedge d_{i+1}) \vee (c_j \wedge d_{i+1}) = c_{j+1} \wedge d_{i+1}$$

(остання рівність випливає з нерівності $c_j \le c_{j+1}$). Ураховуючи отриману рівність і очевидну нерівність $d_i \ge c_{j+1} \wedge d_i$, маємо

$$d_{i,j+1} = d_i \vee (c_{j+1} \wedge d_{i+1}) = d_i \vee (c_{j+1} \wedge d_i) \vee (c_j \wedge d_{i+1}) = d_i \vee (c_j \wedge d_{i+1}) = d_{i,j}\,.$$

Таким чином, кожному повторенню членів у послідовності (3.12) відповідає повторення в послідовності (3.13), причому ця відповідність взаємно однозначна. Це завершує доведення теореми. □

Наслідок 3.1. *У скінченній модулярній решітці будь-які два максимальні ланцюги зі спільними початком і кінцем мають однакову довжину.*

Наслідок 3.2 (Теорема Жордана–Гельдера для модулярних решіток)**.** *Якщо в модулярній решітці існують композиційні ряди, то всі вони мають однакову довжину.*

Зауваження. Частковим випадком теореми Жордана-Гельдера про композиційні ряди для модулярних решіток є доведена раніше теорема Жордана-Гельдера про головні ідеальні ряди для напівгруп (теорема 2.8).

Твердження 3.5. *У модулярній решітці композиційні ряди існують тоді й лише тоді, коли вона задовольняє умови обриву зростаючих і спадних ланцюгів.*

Доведення. За наявності композиційних рядів довжина кожного ланцюга обмежена згори довжиною композиційного ряду. Тому всі ланцюги обриваються. З другого боку, з умови обриву спадних ланцюгів випливає, що в самій решітці і в кожній підрешітці є найменший елемент і атоми. Тому можна побудувати зростаючий ланцюг

$$0 = a_0 < a_1 < a_2 < \cdots \tag{3.15}$$

де a_{i+1} є атомом решітки a_i^{∇}. За умовою він має обірватися на якомусь елементі a_n. Тоді $a_n = 1$, а ланцюг (3.15) є композиційним рядом. □

Завершимо цей підрозділ критеріями модулярності та дистрибутивності у термінах підрешіток. Для цього знадобляться дві спеціальні п'ятиелементні решітки, які називаються відповідно *пентагоном* і *діамантом* (рис. 4):

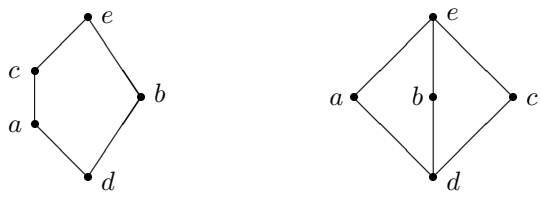


Рис. 4

Далі буде зручніше замість символу $\vee$ використовувати знак додавання, а замість символу $\wedge$ — знак множення.

Теорема 3.6 (Критерій модулярності)**.** *Решітка буде модулярною тоді й лише тоді, коли серед її підрешіток немає пентагонів.*

Доведення. Достатність. Нехай пентагон із рис. 4 є підрешіткою. Тоді $a < c$, але

$$a + b \cdot c = a + d = a \neq c = e \cdot c = (a + b) \cdot c\,.$$

Отже, решітка не є модулярною.

Необхідність. Якщо решітка не є модулярною, то існують такі елементи a, b, c, що $a \leq c$, але елементи $a' = a + b \cdot c$ і $c' = (a + b) \cdot c$ — різні. Зауважимо, що тоді $b \cdot c \leq a' < c' \leq a + b$.

Покажемо, що елементи a', c', $b \cdot c$, b, $a + b$ утворюють пентагон, зображений на рис. 5.

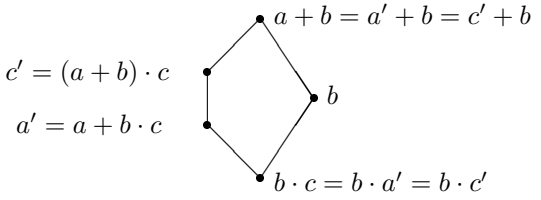


Рис. 5

Зрозуміло, що $bc \leq a' < c' \leq a + b$ і $bc \leq b \leq a + b$. Крім того,

$$a' + b = (a + bc) + b = a + (bc + b) = a + b\,.$$

Позаяк $a' < c' \le a + b$, то $c' + b = a + b$. Аналогічно доводиться, що $c'b = c(a + b)b = bc$ і $a'b = c(a + b)b = bc$.

Для завершення доведення лишилося показати, що елементи a', c', $b \cdot c$, b, $a+b$ — попарно різні. Скористаємося тим, що $b \cdot c \le a' < c' \le a+b$, і розглянемо можливі випадки.

Якщо $a + b = c'$, то $a + b \le c$, звідки $b \le c$ і $a' = a + bc = a + b$, що неможливо.

Якщо $a' = bc$, то $a \le bc$, звідки $a \le b$ і $c' = (a + b)c = bc$, що також неможливо.

Із рівності $a' + b = a + b$ тепер випливає, що b не дорівнює жодному з елементів $b \cdot c$, a' і c'. Нарешті з рівності $c'b = bc$ одержуємо, що $b \ne a + b$. □

Теорема 3.7 (Критерій дистрибутивності)**.** *Модулярна решітка буде дистрибутивною тоді й лише тоді, коли серед її підрешіток немає діамантів.*

Доведення. Достатність. Нехай діамант із рис. 4 є підрешіткою. Тоді

$$a \cdot (b + c) = a \cdot e = a \ne d = d + d = a \cdot b + a \cdot c\,.$$

Отже, решітка не є дистрибутивною.

Необхідність доводиться дещо складніше. Припустимо, що решітка є модулярною, але не є дистрибутивною.

Лема 3.4. *У модулярній решітці для довільних елементів x, y, z виконується рівність* $x(y + z) + y(z + x) = (x + y)(y + z)(z + x)$.

Доведення. Використовуючи нерівності $x(y + z) \le x \le z + x$ і $y \le y + z$ та модулярність, отримуємо

$$x(y + z) + y(z + x) = \big(x(y + z) + y\big)(z + x) = (y + x)(y + z)(z + x).$$ □

Із принципу двоїстості тепер випливає, що в кожній модулярній решітці виконується рівність

$$(x + yz)(y + zx) = xy + yz + zx\,. \tag{3.16}$$

Для елементів x, y, z покладемо

$$d = xy + yz + zx\,, \quad e = (y + x)(y + z)(z + x)\,,$$
$$a = yz + x(y + z)\,, \quad b = zx + y(z + x)\,, \quad c = xy + z(x + y)$$

(елементи a, b, c одержуються один з одного циклічною перестановкою x, y і z; крім того, із модулярності випливає, що $a = (yz + x)(y + z)$, $b = (zx + y)(z + x)$, $c = (xy + z)(x + y)$).

Лема 3.5. $a+b=b+c=c+a=e, \qquad ab=bc=ca=d.$

Доведення. Використовуючи лему 3.4, отримуємо

$$a+b=\big(yz+x(y+z)\big)+\big(y(z+x)+zx\big)=$$
$$=yz+\big(x(y+z)+y(z+x)\big)+zx=yz+(x+y)(y+z)(z+x)+zx.$$

Але $yz\le(x+y)(y+z)(z+x)$, бо $y\le(x+y)(y+z)$ і $z\le z+x$. Із аналогічних міркувань $zx\le(x+y)(y+z)(z+x)$. Тому

$$a+b=(x+y)(y+z)(z+x)\,.$$

Аналогічно доводяться рівності $b+c=c+a=e$.

Друге твердження леми одержується з першого за принципом двоїстості. □

Лема 3.6. *Якщо серед елементів a, b, c хоча б два збігаються, то трійка елементів x, y, z задовольняє дистрибутивний закон.*

Доведення. Якщо $a=b$, то з леми 3.5 одразу випливає, що $d=e=a$. Крім того, за цією самою лемою $d\le c\le e$, звідки $c=a$. Отже, якщо серед елементів a, b, c хоча б два збігаються, то збігаються всі 5 елементів a, b, c, d, e. Зокрема, $d=e$, тобто

$$xy+yz+zx=(y+x)(y+z)(z+x)\,.$$

Оскільки $z\ge yz+zx$, то з модулярності випливає, що

$$z(xy+yz+zx)=z\cdot xy+(yz+zx)=yz+zx\,.$$

З іншого боку, позаяк $z\le y+z$ і $z\le z+x$, то

$$z(x+y)(y+z)(z+x)=z(x+y)\,.$$

Тому $z(x+y)=zx+zy$. □

За припущенням існує трійка елементів x, y, z, для якої

$$z(x+y)\ne zx+zy\,.$$

За лемою 3.6 для цієї трійки елементи a, b, c будуть попарно різними. Але тоді різними будуть всі 5 елементів a, b, c, d, e. Справді, припустимо, наприклад, що $a=e$. Тоді $a+b=a$, звідки $b\le a$ і $ab=b$. Отже, $b=d$. Аналогічно доводиться, що $c=d$. Але це суперечить тому, що $b\ne c$.

Із леми 3.5 тепер випливає, що елементи a, b, c, d, e утворюють діамант із рис. 4. □

Звернемо увагу, що в теоремах 3.6 і 3.7 ідеться саме про підрешітки, а не про довільні п'ятиелементні підмножини решітки.

3.4 Булеві алгебри

Решітка L називається *решіткою з доповненнями*, якщо вона містить 0 і 1 та для кожного $a \in L$ існує *доповнення* a', яке задовольняє рівності

$$a + a' = 1, \qquad a \cdot a' = 0\,. \tag{3.17}$$

Кількість доповнень елемента може змінюватися в дуже широких межах. Однак у дистрибутивних решітках ситуація визначеніша.

Твердження 3.6. *У дистрибутивній решітці з нулем і одиницею кожен елемент має не більше одного доповнення. Крім того, якщо a' і b' — доповнення до a і b, то*

$$(a')' = a, \qquad (a+b)' = a' \cdot b', \qquad (a \cdot b)' = a' + b'\,. \tag{3.18}$$

Доведення. Єдиність доповнення випливає з леми 3.2. Рівність $(a')' = a$ випливає безпосередньо з означення доповнення. Далі маємо

$$\begin{gathered}(a+b)\cdot a'b' = aa'b' + ba'b' = 0\cdot b' + 0\cdot a' = 0,\\ (a+b) + a'b' = a(b+b') + (a+a')b + a'b' = ab + ab' + ab + a'b + a'b' =\\ = ab + ab' + a'b + a'b' = (a+a')(b+b') = 1.\end{gathered}$$

Отже, $(a+b)' = a'\cdot b'$. Рівність $(a\cdot b)' = a'+b'$ доводиться аналогічно. □

Дистрибутивна решітка з доповненнями називається *булевою решіткою*.

Зауваження. Із твердження 3.18 випливає, що в булевій решітці перехід до доповнення є інволютивним антиізоморфізмом. Іншим добре відомим прикладом такого антиізоморфізму є перехід до транспонованої матриці в кільці матриць.

Якщо взяття доповнення розглядати як окрему унарну операцію, то булеву решітку можна розглядати як алгебру із сигнатурою $(+, \cdot\,, {}', 0, 1)$, яка задовольняє такі *аксіоми булевої алгебри*:

(B1) $a + a = a, \quad aa = a$;
(B2) $a + b = b + a, \quad ab = ba$;
(B3) $a + (b + c) = (a + b) + c, \quad (ab)c = a(bc)$;
(B4) $a(b + c) = ab + ac, \quad a + bc = (a + b)(a + c)$;
(B5) $a + a' = 1, \quad aa' = 0$;
(B6) $(a')' = a$;

(B7) $(a+b)' = a'b', \quad (ab)' = a' + b'$;
(B8) $1 \cdot a = a, \quad 0 + a = a$.

Ці аксіоми не є незалежними: можна лишити або тільки перші рівності з кожної пари, або тільки другі.

Задача 3.5. *Доведіть, що з аксіом* (B1)–(B8) *випливають закони поглинання*

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

Класичним прикладом булевої алгебри є алгебра $\mathcal{B}(M)$ усіх підмножин деякої множини M з операціями об'єднання, перетину і взяття доповнення. Нулем і одиницею будуть відповідно порожня підмножина $\varnothing$ і вся множина M. У скінченному випадку інших булевих алгебр фактично і нема.

Теорема 3.8 (Стоун[6]). *Кожна скінченна булева алгебра $\mathcal{A}$ ізоморфна алгебрі $\mathcal{B}(M)$, де M — множина атомів алгебри $\mathcal{A}$.*

Доведення. Оскільки для одноелементної булевої алгебри це очевидно, то далі вважаємо, що $|\mathcal{A}| > 1$. За теоремою 3.3 $\mathcal{A}$ можна вважати підрешіткою деякого скінченного булеану $\mathcal{B}(I)$, причому з доведення теореми 3.3 випливає, що нулем алгебри $\mathcal{A}$ буде порожня множина $\varnothing$, а одиницею — множина I. Тоді атоми алгебри $\mathcal{A}$ — це мінімальні непорожні множини, які є елементами $\mathcal{A}$.

Нехай M — множина атомів алгебри $\mathcal{A}$. Покажемо, що кожен елемент A із $\mathcal{A}$ (якщо його розглядати як підмножину множини I) збігається з об'єднанням A^* усіх тих атомів із M, які містяться в A. Справді, $A \supseteq A^*$. Крім того, множина $\overline{A^*}$ — як доповнення A^* — міститься в $\mathcal{A}$. Якби було $A \neq A^*$, то елемент $A \cap \overline{A^*} = A \setminus A^*$ був би ненульовим елементом із $\mathcal{A}$. Але тоді $A \setminus A^*$ містив би якусь множину з M, що суперечить означенню A^*.

Зауважимо, що об'єднання різних наборів мінімальних множин будуть різними. Справді, перетин двох різних мінімальних множин є нулем алгебри $\mathcal{A}$, а тому мінімальна множина $B \in M$ міститься в об'єднанні A якихось мінімальних множин тоді й лише тоді, коли B є однією з компонент цього об'єднання.

Зіставляючи кожному елементу $A \in \mathcal{A}$ множину всіх тих множин із M, які містяться в A, одержуємо ізоморфізм алгебри $\mathcal{A}$ на $\mathcal{B}(M)$. $\square$

[6] Stone M. H. The representation theorem for Boolean algebra / M. H. Stone // Trans. Amer. Math. Soc. — **40**. — 1936, P. 37–111.

Для нескінченних булевих алгебр теорема Стоуна перестає бути правильною (див. задачу 53). Однак можна довести, що для кожної нескінченної булевої алгебри $\mathcal{A}$ знайдеться така множина M, що $\mathcal{A}$ ізоморфна деякій підалгебрі з $\mathcal{B}(M)$.

3.5 Історичні зауваження

Решітки вперше з'явилися 1897 р. у роботі Дедекінда "Über Zerlegung von Zahlen durch ihre größten gemeinsamen Teiler" ("Про розклад чисел за допомогою їх найбільшого спільного дільника")[7]. Робота цікава ще й тим, що це ледь не перше із сучасних аксіоматичних досліджень: і решітка, і група визначаються тут як абстрактні множини, на яких визначені певні операції, що задовольняють певні системи аксіом. Далі для цих абстрактних алгебричних систем розглядаються більш чи менш конкретні моделі-інтерпретації[8].

Дедекінд визначає решітку (у його термінології — *дуальну групу*) як алгебричну систему з двома операціями, що задовольняють аксіоми (2)–(4) із с. 63. Далі з цих аксіом виводяться закони ідемпотентності. Як одна з моделей розглядається решітка підмножин скінченної множини. Показано, що в цій моделі виконуються також дистрибутивні закони. Крім того, показано, що дистрибутивні закони не виводяться з аксіом (2)–(4), але за умови виконання цих аксіом виводяться один із другого.

До поняття решітки Дедекінд прийшов при вивченні модулів над кільцем цілих алгебричних чисел (множина підмодулів даного модуля утворює відносно суми та перетину підмодулів модулярну решітку). Звідси зрозуміло, чому Дедекінд у першу чергу зацікавився *модулярними* решітками і чому такі решітки часто називають *дедекіндовими* (цим пояснюється й походження терміна модулярна). Він також знайшов три рівносильні характеризації модулярних решіток: це виконання одного із двоїстих один до одного законів $a(ab+c) = ab+ac$ (який зараз називається *модулярним законом*) або $a(ab+c) = ab+ac$ $(a+b)(a+c) = a+(a+b)c$ чи самодвоїстого співвідношення $(a+bc)(b+c) = a(b+c)+bc$, яке він називає властивістю (M) і яке для нього було основним.

Решіткам присвячено ще одну роботу Дедекінда "Über die von drei Moduln erzeugte Dualgruppe" ("Про дуальні групи, породжені трьома модулями") (1900). Основним її результатом є побудова 2- і 3-породжених вільних модулярних решіток. Зокрема, показано, що перша має порядок 4, а друга — 28. Серед інших важливих результатів цієї роботи виділимо критерій модулярності решітки у термінах підрешіток (теорема 3.6) і теорему про те, що в модулярній решітці всі композиційні ряди мають однакову довжину (цю теорему зараз

[7] Назва роботи не зовсім відповідає її змісту.

[8] Зауважимо, що знамениті "Основи геометрії" Гільберта, які часто вважають початком сучасного етапу розвитку аксіоматичного методу, з'явилися лише наступного року.

зазвичай називають теоремою Жордана–Гельдера[9] — див. наслідок 3.2).

Нарешті, дуже важливим у загальноматематичному плані є спостереження Дедекінда, що кожна з операцій решітки природно індукує на множині її елементів відношення часткового порядку. Він же довів і деякі загальні властивості цього відношення. Таким чином, Дедекінд був першим, хто зрозумів необхідність вивчення довільних відношень порядку, адже до нього в математиці розглядалися лише лінійні порядки.

3.6 Задачі

1. Доведіть, що решітки ізоморфні як алгебричні системи тоді й лише тоді, коли вони ізоморфні як частково впорядковані множини.

2. Нехай M — частково впорядкована множина. Підмножина $A \subseteq M$ називається *лівим відрізком* множини M, якщо разом із кожним елементом вона містить й усі, менші за нього (тобто якщо для кожного $a \in A$ з $x \leq a$ випливає $x \in A$). Доведіть, що впорядкована за включенням множина $\mathcal{L}(M)$ усіх лівих відрізків множини M є повною решіткою.

3. Доведіть, що

   a) для кожної непорожньої множини A впорядкована за включенням множина $\operatorname{Eq} A$ усіх відношень еквівалентності на A є повною решіткою;

   b) для універсальної алгебри A решітка $\operatorname{Con}(A)$ усіх конгруенцій на A є повною підрешіткою решітки $\operatorname{Eq} A$.

4. З'ясуйте, чи буде решітка $\operatorname{Sub}(A)$ всіх підалгебр алгебри A підрешіткою решітки $\mathfrak{B}(A)$.

5. Для довільних визначених на $[0,1]$ дійсних функцій f і g покладемо: $f \leq g$ тоді й лише тоді, коли $f(a) \leq g(a)$ для всіх $a \in [0,1]$. Доведіть, що на множині $C[0,1]$ неперервних на $[0,1]$ дійсних функцій це відношення є відношенням часткового порядку, відносно якого $C[0,1]$ утворює решітку. Чи буде ця решітка повною?

6. Нехай $L \neq \varnothing$ — підмножина булеану $\mathfrak{B}(M)$, яка задовольняє таку умову: множина $A \subseteq M$ належить L тоді й тільки тоді, коли L належать усі скінченні підмножини множини A. Доведіть, що в L є максимальні за включенням елементи.

7. Укажіть у булеані $\mathfrak{B}(\mathbb{N})$ який-небудь антиланцюг континуальної потужності.

8. Нехай у частково впорядкованій множині M для кожних двох елементів існує верхня грань. Доведіть, що для довільного розкладу $M = M_1 \cup \cdots \cup M_k$ принаймні в одній із частково впорядкованих множин $M_1, \ldots, M_k$ для кожних двох елементів існує верхня грань.

[9] Жордан (1869) і Гельдер (1889) довели її для решітки нормальних підгруп групи.

9. Доведіть, що гомоморфізм решіток як алгебр є гомоморфізмом решіток як частково впорядкованих множин, однак обернене твердження неправильне.

10. Доведіть, що для довільних елементів a, b модулярної решітки інтервали $I = [a \wedge b, a]$ і $J = [b, a \vee b]$ ізоморфні як решітки.

11. Нехай у модулярній решітці L існують композиційні ряди. Позначимо через $l(a)$ довжину композиційного ряду в нижньому конусі $a_{\triangle}$ елемента a. Доведіть, що для довільних елементів a і b виконується рівність $l(a \vee b) = l(a) + l(b) - l(a \wedge b)$.

12. Доведіть, що для решітки L такі умови рівносильні:
    a) L — ланцюг;
    b) кожна непорожня підмножина з L є підрешіткою;
    c) якщо $a = b \wedge c$, то $a = b$ або $a = c$;
    d) якщо $a = b \vee c$, то $a = b$ або $a = c$.

    У задачах 13 — 23 замість символу $\vee$ використовується знак додавання, а замість символу $\wedge$ — знак множення.

13. Доведіть, що в кожній решітці з рівності $a+b+c = abc$ випливає рівність $a = b = c$.

14. Доведіть, що в кожній решітці виконуються такі нерівності:
    a) $ac + bc \leq (a + b)c$;
    b) $ac + bc + ad + bd \leq (a + b)(c + d)$;
    c) $a + bc \leq (a + b)(a + c)$;
    d) $ac + bd \leq (a + b)(c + d)$;
    e) $ab + cd + fg \leq (a + b)(c + d)(f + g)$.

15. Доведіть, що в модулярній решітці
    a) для довільних a, b, c виконується рівність $(a+bc)(b+c) = a(b+c)+bc$;
    b) із нерівностей $a \leq c \leq a + b$ випливає рівність $a + bc = c$;
    c) із рівності $(a + b)c = bc$ випливає рівність $a(b + c) = ab$.

16. Доведіть, що в модулярній решітці з нулем із рівності $(a_1+\cdots+a_n)b = 0$ випливає рівність $(a_1 + b) \cdots (a_n + b) = a_1 \cdots a_n + b$.

17. Доведіть, що для решітки L такі умови рівносильні:
    a) решітка L — модулярна;
    b) для довільних a, b, c виконується *модулярний* закон $a(ab+c) = ab+ac$;
    c) для довільних a, b, c $(a + b)(a + c) = a + (a + b)c$;
    d) якщо $a \leq c$ і $d \leq b$, то $a + b(c + d) = (a + b)c + d$;
    e) для довільних a, b, c з умов $a \leq c$, $ab = bc$, $a + b = b + c$ випливає рівність $a = c$;
    f) у кожній підрешітці решітки L, в якій існують композиційні ряди, ці ряди мають однакову довжину.

18. Доведіть, що решітка буде модулярною тоді й лише тоді, коли для довільних a, b, c рівності $c(a+b)+b = (a+b)(c+b)$ і $(c+ab)b = ab+cb$ рівносильні.

19. Нехай $a_1, \ldots, a_n, b_1, \ldots, b_n$ — такі елементи модулярної решітки, що для всіх $i \neq j$ виконується нерівність $a_i \leq b_j$. Доведіть, що $(a_1 + \cdots + a_n)\, b_1 \cdots b_n = a_1 b_1 + \cdots + a_n b_n$.

20. Доведіть, що такі умови рівносильні:

    a) решітка L — дистрибутивна;

    b) для довільних a, b, c виконується рівність $ab + c = (a+c)(b+c)$;

    c) для довільних a, b, c виконується рівність $ab + bc + ca = (a+b)(b+c)(c+a)$;

    d)* для довільних a, b, c із рівностей $ab = ac$ і $a + b = a + c$ випливає рівність $b = c$;

    e) для довільних a, b, c виконується нерівність $(a+b)c \leq a + bc$.

21. Доведіть, що такі умови рівносильні:

    a) решітка L — дистрибутивна;

    b) для довільних a, b, c виконується рівність $ab+bc+ca = (a+b)(c+ab)$;

    c) для довільних a, b, c виконується рівність $a+(a+b)c = (a+b)(a+c)$;

    d) $a \leq b$ тоді й лише тоді, коли існує такий c, що $ac \leq bc$ і $a + c \leq b + c$;

    e)* для довільних a, b, c з нерівностей $ab \leq c$ і $a \leq b + c$ випливає нерівність $a \leq c$.

22. Доведіть, що в дистрибутивній решітці співвідношення $ab \leq x \leq a + b$ і $x = ax + bx + ab$ рівносильні.

23. Нехай для атома a дистрибутивної решітки виконується нерівність $a \leq b_1 + \cdots + b_k$. Доведіть, що існує доданок b_i, для якого виконується нерівність $a \leq b_i$.

24. Доведіть, що в дистрибутивній решітці кожна скінченна підмножина породжує скінченну підрешітку.

25.* Доведіть, що коли в дистрибутивній решітці існує композиційний ряд, то вона скінченна.

26. Доведіть, що для кожної групи решітка конгруенцій на цій групі ізоморфна решітці нормальних підгруп і є модулярною.

27. Доведіть, що для кожного асоціативного кільця решітка конгруенцій на цьому кільці ізоморфна решітці його ідеалів і є модулярною.

28. Доведіть, що

    a) решітка підгруп групи S_3 є модулярною;

    b) решітка підгруп кожної з груп A_4, D_4 і S_4 не є модулярною.

29. Доведіть, що решітка підгруп скінченної абелевої групи G буде дистрибутивною тоді й лише тоді, коли група G є циклічною.

30.* Комутативна область цілісності називається *кільцем Безу*, якщо її головні ідеали утворюють підрешітку в решітці всіх ідеалів. Доведіть, що в кільці Безу решітка всіх ідеалів є дистрибутивною.

31. Доведіть, що множина всіх підпросторів скінченновимірного евклідового простору відносно операцій $U \vee V := U + V$, $U \wedge V := U \cap V$, $\overline{U} := U^{\perp}$ утворює модулярну решітку з доповненнями.

32. Нехай у дистрибутивній решітці з нулем 0 і одиницею 1 елементи a, b, a', b' задовольняють умови $a+a' = b+b' = 1$, $aa' = bb' = 0$. Доведіть, що
   a) $(a + b) + a'b' = 1$;
   b) $(a + b) \cdot a'b' = 0$;
   c) $ab + (a' + b') = 1$;
   d) $ab \cdot (a' + b') = 0$.

33. Нехай n — фіксоване натуральне число, вільне від квадратів. На множині $D(n)$ усіх дільників числа n розглянемо операції: $a \wedge b = \text{НСД}(a, b)$, $a \vee b = \text{НСК}(a, b)$, $a' = n/a$. Доведіть, що $D(n)$ є булевою алгеброю. Чи можна позбутися умови, що число n вільне від квадратів?

34. Доведіть, що коли на множині чисел з інтервалу $[0, 1]$ визначити операції $a \vee b := \max(a, b)$, $a \wedge b := \min(a, b)$, $a' := 1 - a$, то будуть виконуватися всі аксіоми булевої алгебри, за винятком аксіом (B5).

35.*Доведіть, що модулярна решітка з нулем і одиницею, в якій кожен елемент має рівно одне доповнення, буде булевою алгеброю.

36. Доведіть, що замість аксіом (B1)–(B8) булеву алгебру можна задати аксіомами
$$a(b + c) = ab + ac, \quad a + bc = (a + b)(a + c),$$
$$a + b = b + a, \quad ab = ba, \quad a + (b + c) = (a + b) + c, \quad (ab)c = a(bc),$$
$$a(a + b) = b, \quad a + ab = a, \quad aa' + b = b, \quad (a + a')b = b.$$

37. Доведіть, що замість аксіом (B1)–(B8) булеву алгебру можна задати аксіомами
$$a + a = a, \quad a + b = b + a, \quad a + (b + c) = (a + b) + c,$$
$$a(b + c) = ab + ac, \quad (a')' = a, \quad (a + b)' = a'b', \quad aa' + b = b.$$

38. Доведіть, що нескінченна булева алгебра містить нескінченний зростаючий і нескінченний спадний ланцюги.

39. Наведіть приклад зліченної булевої алгебри.

40. Доведіть, що в кожній нескінченній булевій алгебрі можна виділити нескінченну підмножину таких елементів, що добуток будь-яких двох із них дорівнює 0.

41. Доведіть, що кожна скінченнопороджена булева алгебра є скінченною. Яку найбільшу кількість елементів може містити n-породжена булева алгебра?

42. Скільки підалгебр має булева алгебра $\mathfrak{B}(M)$, якщо множина M має n елементів?

43. Асоціативне кільце K називається *булевим*, якщо $x^2 = x$ для всіх $x \in K$. Доведіть, що кожне булеве кільце є комутативним і в ньому виконується тотожність $2x = 0$.

44. Нехай $\langle B; \vee, \wedge, ^- \rangle$ — булева алгебра. Доведіть, що $\langle B; +, \cdot \rangle$, де $a + b := (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$, $a \cdot b := a \wedge b$, буде булевим кільцем із одиницею.

45. Нехай $\langle B; +, \cdot \rangle$ — булеве кільце з одиницею e. Доведіть, що $\langle B; \vee, \wedge, ^- \rangle$, де $a \vee b := a + b + ab$, $a \wedge b := ab$, $\overline{a} := e + a$, буде булевою алгеброю.

46. Доведіть, що ідемпотенти будь-якого комутативного кільця утворюють булеве кільце відносно дій $e \oplus f = e + f - 2ef$, $e \odot f = ef$.

У задачах 47—52 ідеться про *ідеали* решіток, тобто такі підмножини решіток, які разом із кожним елементом містять усі, менші за нього, і разом із кожними двома елементами містять їх точну верхню грань. Ідеал називається *головним*, якщо він є нижнім конусом $a_\triangle$ деякого елемента a. Ідеал I називається *простим*, якщо для довільних a, b із $a \wedge b \in I$ випливає, що принаймні один із множників a і b належить I. Ідеал I решітки L називається *максимальним*, якщо для довільного ідеалу J із включень $I \subseteq J \subseteq L$ випливає, що $I = J$ або $J = L$.

47. Доведіть, що в дистрибутивній решітці з одиницею кожен максимальний ідеал є простим.

48. Доведіть, що в булевій алгебрі ідеал буде простим тоді й тільки тоді, коли він буде максимальним.

49. Доведіть, що кожна дистрибутивна решітка з нулем і одиницею буде булевою алгеброю тоді й лише тоді, коли кожен її простий ідеал є максимальним.

50. Доведіть, що коли кожну конгруенцію ρ на булевій алгебрі B зіставити з тим її класом $\overline{0_\rho}$, який містить 0, то одержимо бієкцію між множиною конгруенцій на B і множиною ідеалів алгебри B.

51. Доведіть, що всі ідеали булевої алгебри будуть головними тоді й лише тоді, коли алгебра скінченна.

52. Доведіть, що ідеал I булевої алгебри B буде максимальним тоді й лише тоді, коли для довільного $a \in B$ ідеал I містить рівно один із елементів a і a'.

53. Нехай множина M — нескінченна. Доведіть, що множина $\mathcal{P}(M)$ всіх скінченних і коскінченних підмножин із M утворює підалгебру булевої алгебри $\mathfrak{B}(M)$, причому ця підалгебра не є ізоморфною $\mathfrak{B}(N)$ для жодної множини N.

4 Лінійні алгебри

4.1 Базові поняття

Перші приклади лінійних алгебр (під назвою "гіперкомплексні системи") з'явилися у другій половині XIX ст. при намаганні узагальнити поняття комплексного числа. Однак нові структури чим далі, тим усе менше нагадували комплексні числа. Тому термін "гіперкомплексні системи" поступово вийшов з ужитку.

Означення 4.1. ***Лінійною алгеброю*** *над полем* P (або просто P-***алгеброю***) *називається множина* A *з діями додавання, множення і множення на скаляри* (елементи поля P), *яка задовольняє такі вимоги*:
1) *відносно додавання і множення на скаляри множина* A *утворює векторний простір над полем* P;
2) *відносно додавання і множення множина* A *утворює кільце*;
3) *множення елементів алгебри і множення на скаляри переставні:* $\alpha(ab) = (\alpha a)b = a(\alpha b)$ *для довільних* $\alpha \in P$ *та* $a, b \in A$.

Таким чином, лінійна алгебра — це векторний простір над полем, елементи якого додатково можна множити між собою, причому це множення узгоджене із множенням на скаляри і пов'язане з додаванням дистрибутивними законами. Коли зрозуміло, що йдеться саме про лінійні алгебри (а не якісь інші, наприклад, універсальні), то слово "лінійні" зазвичай опускають. Алгебра над полем P називається *скінченновимірною*, якщо вона скінченновимірна як векторний простір над P. Алгебри над $\mathbb{R}$ і $\mathbb{C}$ часто називають відповідно *дійсними* і *комплексними*.

Приклади. 1. Кожне поле є алгеброю над будь-яким своїм підполем.

2. Множина векторів звичайного тривимірного простору V_3 разом із векторним множенням є алгеброю над $\mathbb{R}$.

3. Множина Map(A,P) усіх функцій, які визначені на множині A і набувають значень у полі P, є алгеброю над P відносно звичайних дій додавання та множення функцій і множення функцій на скаляри.

4. Множина многочленів $P[x_1, \ldots, x_n]$ є алгеброю над P відносно звичайних дій із многочленами.

5. Множина матриць $M_n(P)$ є алгеброю над P відносно звичайних дій із матрицями. Вона називається *повною матричною алгеброю* порядку n над полем P.

6. Для довільного векторного простору V над полем P множина $\operatorname{End} V$ усіх лінійних перетворень простору V є алгеброю над P відносно звичайних дій із лінійними перетвореннями.

Довільний векторний простір A можна перетворити в алгебру *з нульовим множенням* (тобто покласти $a \cdot b = 0$ для всіх $a, b \in A$). Таку алгебру ще називають *тривіальною*.

Означення 4.2. *Підмножина алгебри називається* ***підалгеброю****, якщо ця підмножина є одночасно і підпростором алгебри як векторного простору, і підкільцем.*

Якщо множення в алгебрі є асоціативним, то алгебра називається *асоціативною*. Аналогічно алгебра називається *комутативною*, якщо множення є комутативним, і *алгеброю з одиницею*, якщо для множення існує нейтральний елемент.

Центром алгебри $\mathcal{A}$ називається множина

$$Z(\mathcal{A}) = \{x \mid xa = ax \text{ для всіх } a \in \mathcal{A}\}.$$

Легко перевіряється, що центр асоціативної алгебри є її підалгеброю.

Алгебра $\mathcal{A}$ (не обов'язково асоціативна) називається *алгеброю з діленням*, якщо для довільних $a \neq 0$ і b кожне з рівнянь $ax = b$, $ya = b$ має розв'язок.

Якщо найменша підалгебра алгебри $\mathcal{A}$, яка містить дані елементи $a_1, \ldots, a_k$, збігається з самою $\mathcal{A}$, то набір $a_1, \ldots, a_k$ називається *системою твірних* алгебри $\mathcal{A}$. У випадку алгебр з одиницею додатково вважають, що добуток нульової кількості множників дорівнює одиниці.

Якщо алгебра $\mathcal{A}$ над полем P містить одиницю 1, то відображення $\alpha \mapsto \alpha \cdot 1$ є мономорфізмом поля P в алгебру $\mathcal{A}$. Після ототожнення елементів $\alpha \in P$ з відповідними кратними $\alpha \cdot 1$ одиниці ми можемо вважати, що *алгебра $\mathcal{A}$ з одиницею містить поле P*. При такому ототожненні "зовнішнє" множення на елементи з P як на скаляри збігається із "внутрішнім" множенням в алгебрі $\mathcal{A}$.

Вправа 4.1. *Перевірте, що в алгебрі з одиницею $P \subseteq Z(\mathcal{A})$.*

Поширеним способом перетворення векторного простору A над полем P в алгебру над P є задання множення в A за допомогою так званих *структурних констант*. Нехай $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ — фіксована база

простору A. Для кожної пари індексів (i,j), $1 \le i,j \le n$, задамо деякий вектор $\boldsymbol{v}_{ij} = \alpha_{ij}^1 \boldsymbol{e}_1 + \cdots + \alpha_{ij}^n \boldsymbol{e}_n$. Тоді для довільних векторів

$$\boldsymbol{x} = a_1 \boldsymbol{e}_1 + \cdots + a_n \boldsymbol{e}_n, \qquad \boldsymbol{y} = b_1 \boldsymbol{e}_1 + \cdots + b_n \boldsymbol{e}_n$$

з простору A їх добуток $\boldsymbol{xy}$ можна визначити правилом

$$\boldsymbol{xy} = \sum_{i,j=1}^{n} a_i b_j \boldsymbol{v}_{ij} = \sum_{i,j,k=1}^{n} a_i b_j \alpha_{ij}^k \boldsymbol{e}_k$$

(із однозначності розкладу векторів за векторами бази випливає коректність цього правила). Це перетворює A в алгебру над P (перевірте дистрибутивні закони!).

Зауважимо, що коефіцієнти α_{ij}^k, які називаються *структурними константами* алгебри A, можна вибирати довільно.

Приклади. 7. Поле комплексних чисел $\mathbb{C}$ (як алгебра над полем $\mathbb{R}$) у базі $1, i$ задається таблицею множення

$\times$	1	i
1	1	i
i	i	-1

8. Алгебра векторів простору V_3 (див. приклад **1**) в ортонормованій базі $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ задається таблицею множення

$\times$	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}$	0	$\boldsymbol{k}$	$-\boldsymbol{j}$
$\boldsymbol{j}$	$-\boldsymbol{k}$	0	$\boldsymbol{i}$
$\boldsymbol{k}$	$\boldsymbol{j}$	$-\boldsymbol{i}$	0

9. Нехай $S = \{a_1, a_2, \ldots, a_n\}$ — скінченна напівгрупа порядку n. Виберемо в n-вимірному просторі A над полем P базу, елементи якої проіндексуємо елементами напівгрупи S: $\boldsymbol{e}_{a_1}$, $\boldsymbol{e}_{a_2}$, …, $\boldsymbol{e}_{a_n}$. Множення елементів бази визначимо так:

$$\boldsymbol{e}_a \cdot \boldsymbol{e}_b = \boldsymbol{e}_{ab} \quad \text{для довільних} \quad a, b \in S.$$

Отримана таким чином алгебра називається *напівгруповою алгеброю* над полем P і позначається $P[S]$. Замість $\boldsymbol{e}_{a_1}$, $\boldsymbol{e}_{a_2}$, …, $\boldsymbol{e}_{a_n}$ часто пишуть просто a_1, a_2, …, a_n.

Якщо S — група, то алгебра $P[S]$ називається *груповою*.

10. Частковим випадком напігрупової алгебри над полем P є *тензорна алгебра* $P\langle x_1, \ldots, x_n\rangle$ над полем P — напігрупова алгебра вільного моноїда X^* із множиною твірних $X = \{x_1, \ldots, x_n\}$. Її ще називають *алгеброю многочленів від "некомутуючих" змінних* $x_1, \ldots, x_n$.

Задача 4.1. *Нехай* $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ *— фіксована база алгебри* $\mathcal{A}$ *як векторного простору.*

1. *Доведіть, що* $\mathcal{A}$ *комутативна тоді й лише тоді, коли комутативним є множення базисних векторів, тобто* $\boldsymbol{e}_i\boldsymbol{e}_j = \boldsymbol{e}_j\boldsymbol{e}_i$ *для довільних векторів* e_i, e_j *бази.*

2. *Доведіть, що* $\mathcal{A}$ *асоціативна тоді й лише тоді, коли асоціативним є множення базисних векторів, тобто* $\boldsymbol{e}_i(\boldsymbol{e}_j\boldsymbol{e}_k) = (\boldsymbol{e}_i\boldsymbol{e}_j)\boldsymbol{e}_k$ *для довільних векторів* $\boldsymbol{e}_i$, $\boldsymbol{e}_j$, $\boldsymbol{e}_k$ *бази.*

Із цієї задачі одразу випливає, що групові та напівгрупові алгебри є асоціативними.

Означення 4.3. *Відображення* $\varphi : \mathcal{A} \to \mathcal{B}$ *лінійних алгебр над полем* P *називається* ***гомоморфізмом****, якщо воно одночасно є гомоморфізмом алгебр як векторних просторів* (тобто лінійним відображенням) *і гомоморфізмом алгебр як кілець. Ін'єктивний гомоморфізм називається* ***мономорфізмом****, а сюр'єктивний —* ***епіморфізмом*** *Взаємно однозначний гомоморфізм називається* ***ізоморфізмом****.*

Під *ядром* $\operatorname{Ker}\varphi$ гомоморфізму $\varphi : \mathcal{A} \to \mathcal{B}$ розуміють ядро φ як лінійного відображення (тобто повний прообраз нульового елемента з $\mathcal{B}$).

Задача 4.2. *Нехай* $\mathcal{A}$ *— асоціативна алгебра з одиницею та системою твірних* $a_1, \ldots, a_k$*. Доведіть, що відображення* $x_1 \mapsto a_1, \ldots, x_k \mapsto a_k$ *можна продовжити, причому єдиним способом, до епіморфізму* $\varphi : P\langle x_1, \ldots, x_k\rangle \to \mathcal{A}$*.*

Нехай $\mathcal{A}_1, \ldots, \mathcal{A}_n$ — набір алгебр над даним полем P. На множині

$$\mathcal{A} = \{(a_1, \ldots, a_n) \mid a_i \in \mathcal{A}_i,\ i = 1, \ldots, n\}$$

можна "покомпонентно" визначити додавання, множення та множення на скаляри:

$$\begin{gathered}(a'_1, \ldots, a'_n) + (a''_1, \ldots, a''_n) := (a'_1 + a''_1, \ldots, a'_n + a''_n),\\ (a'_1, \ldots, a'_n) \cdot (a''_1, \ldots, a''_n) := (a'_1a''_1, \ldots, a'_na''_n),\\ \alpha(a_1, \ldots, a_n) := (\alpha a_1, \ldots, \alpha a_n).\end{gathered}$$

Легко перевірити, що множина $\mathcal{A}$ з так визначеними операціями також є алгеброю над полем P. Вона називається *прямою сумою* алгебр $\mathcal{A}_1$, $\ldots$, $\mathcal{A}_n$ і позначається $\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$.

Якщо елемент $a \in \mathcal{A}_k$ ототожнити з набором $(0, \ldots, 0, a, 0, \ldots, 0)$ (у якому всі компоненти, крім k-ї, дорівнюють 0), то множник $\mathcal{A}_k$ можна розглядати як підмножину прямої суми $\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$. Зрозуміло, що $\mathcal{A}_k$ буде навіть підалгеброю в $\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$.

Твердження 4.1. *Пряма сума алгебр з одиницею є алгеброю з одиницею.*

Доведення. Якщо e_k є одиницею алгебри $\mathcal{A}_k$, то елемент $e = e_1 + \cdots + e_n$ є одиницею алгебри $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$. □

Підалгебра I алгебри $\mathcal{A}$ називається *лівим* (відповідно *правим*, *двостороннім*) *ідеалом* алгебри $\mathcal{A}$, якщо вона витримує множення на елементи алгебри $\mathcal{A}$ зліва (відповідно справа, з обох сторін), тобто $\mathcal{A}I \subseteq I$ (відповідно $I\mathcal{A} \subseteq I$, $\mathcal{A}I\mathcal{A} \subseteq I$). Двосторонні ідеали часто називають просто *ідеалами*.

Вправа 4.2. *Доведіть, що підалгебра I алгебри $\mathcal{A}$ буде ідеалом тоді й лише тоді, коли вона є ядром деякого гомоморфізму $\varphi : \mathcal{A} \to \mathcal{B}$.*

Твердження 4.2. *Якщо двосторонній ідеал I асоціативної алгебри $\mathcal{A}$ є алгеброю з одиницею, то для нього існує доповняльний двосторонній ідеал* (тобто такий ідеал J, що $\mathcal{A} = I \oplus J$).

Доведення. Нехай e — одиниця ідеалу I. Покладемо $J = \{a \in A \mid ae = 0\}$. Очевидно, що J — лівий ідеал алгебри $\mathcal{A}$.

Враховуючи, що для довільних $a \in \mathcal{A}$ і $b \in J$ буде $be = 0$ і $ae \in I$, маємо

$$ba \cdot e = b \cdot ae = b \cdot eae = be \cdot ae = 0 \cdot ae = 0.$$

Отже, ba також належить J, а тому J є і правим ідеалом алгебри $\mathcal{A}$.

Із рівності $a = ae + (a - ae)$ з урахуванням того, що $ae \in I$ та $a - ae \in J$, випливає, що кожен елемент $a \in \mathcal{A}$ розкладається в суму елементів з I та J, тобто що $\mathcal{A} = I + J$. Нарешті, для довільного $c \in I \cap J$ маємо $ce = c$ (тому що $c \in I$) і $ce = 0$ (тому що $c \in J$). Отже, $I \cap J = 0$ і сума $I + J$ є прямою. □

Теорема 4.1. *Кожну* (*асоціативну*) *алгебру можна розширити до* (*асоціативної*) *алгебри з одиницею.*

Доведення. Нехай $\mathcal{A}$ — алгебра над полем P. Розглянемо пряму суму (як векторних просторів) $\mathcal{A}_1 = \mathcal{A} \oplus P$ і визначимо множення в $\mathcal{A}_1$:

$$(a, \alpha) \cdot (b, \beta) := (ab + \alpha b + \beta a, \alpha\beta)\,.$$

Легко перевіряється, що $\mathcal{A}_1$ — алгебра з одиницею $(0, 1)$ (причому асоціативна, якщо такою є $\mathcal{A}$), а відображення $a \mapsto (a, 0)$ є мономорфізмом. □

4.2 Кватерніони

Важливу роль у математиці відіграє чотиривимірна дійсна *алгебра кватерніонів* $\mathbb{H}$. У базі, елементи якої зазвичай позначають $1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$, вона задається таблицею множення

$\times$	1	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
1	1	$\boldsymbol{i}$	$\boldsymbol{j}$	$\boldsymbol{k}$
$\boldsymbol{i}$	$\boldsymbol{i}$	-1	$\boldsymbol{k}$	$-\boldsymbol{j}$
$\boldsymbol{j}$	$\boldsymbol{j}$	$-\boldsymbol{k}$	-1	$\boldsymbol{i}$
$\boldsymbol{k}$	$\boldsymbol{k}$	$\boldsymbol{j}$	$-\boldsymbol{i}$	-1

(4.1)

Вправа 4.3. *Доведіть, що алгебра кватерніонів є асоціативною.*

Кватерніон $x = x_0 \cdot 1 + x_1 \cdot \boldsymbol{i} + x_2 \cdot \boldsymbol{j} + x_3 \cdot \boldsymbol{k}$ часто записують у вигляді $x = x_0 + \widehat{x}$. Доданок x_0 називають *дійсною* або *скалярною* частиною кватерніона x, а доданок $\widehat{x} = x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$ — *уявною* або *векторною* частиною. Кватерніон, дійсна частина якого дорівнює 0, називають *чисто уявним*.

Оскільки для ненульового кватерніона $x = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$ маємо

$$x^2 = x_0^2 - x_1^2 - x_2^2 - x_3^2 + 2x_0(x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k})\,,$$

то легко бачити, що квадрат x^2 буде дійсним тоді й лише тоді, коли або $x_0 = 0$ (і тоді x є чисто уявним та $x^2 < 0$), або $x_1 = x_2 = x_3 = 0$ (і тоді x є дійсним і $x^2 > 0$). Якщо врахувати, що $\mathbb{R}$ виділяється в $\mathbb{H}$ як центр, то звідси випливає, що розклад $x = x_0 + \widehat{x}$ кватерніона на скалярну й векторну частини можна описати внутрішнім чином (тобто не використовуючи базу $1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$, а спираючись лише на властивості множення).

Кватерніон $\overline{x} = x_0 - \widehat{x}$ називається *спряженим* до кватерніона $x = x_0 + \widehat{x}$. Легко перевіряється (зробіть це!), що для довільного кватерніона $x = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$ маємо

$$x \cdot \overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2\,. \tag{4.2}$$

Зокрема, $x \cdot \overline{x} = \overline{x} \cdot x$. Число $N(x) = x \cdot \overline{x}$ називається *нормою* кватерніона x.

Вправа 4.4. *Доведіть, що* $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$.

Алгебру кватерніонів можна розглядати як чотиривимірний евклідів простір, якщо вважати базу $1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ ортонормованою. Тоді для довжини $|x|$ кватерніона x матимемо $|x| = \sqrt{N(x)}$.

Із правила множення кватерніонів стає зрозумілим походження термінів *скалярний добуток векторів* і *векторний добуток векторів*[10]. Справді, якщо розглядати чисто уявний кватерніон $\widehat{x} = x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$ як вектор звичайного тривимірного простору простору V_3 з ортонормованою базою $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$, то для чисто уявних кватерніонів $\widehat{x}$ і $\widehat{y}$ матимемо

$$\widehat{x} \cdot \widehat{y} = -(\widehat{x}, \widehat{y}) + [\widehat{x}, \widehat{y}],$$

де $(\widehat{x}, \widehat{y})$ і $[\widehat{x}, \widehat{y}]$ — відповідно скалярний і векторний добутки векторів $\widehat{x}$ та $\widehat{y}$.

Для кватерніонів існує аналог тригонометричної форми запису комплексних чисел. Справді, позаяк

$$x = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k} = |x| \cdot \left(\frac{x_0}{|x|} + \frac{q}{|x|} \left(\frac{x_1}{q}\boldsymbol{i} + \frac{x_2}{q}\boldsymbol{j} + \frac{x_3}{q}\boldsymbol{k} \right) \right),$$

де $q = \sqrt{x_1^2 + x_2^2 + x_3^2}$, то кожен кватерніон x записується у вигляді

$$x = r(\cos\varphi + \boldsymbol{v} \cdot \sin\varphi),$$

де $r \geq 0$ і $\boldsymbol{v} = \frac{x_1}{q}\boldsymbol{i} + \frac{x_2}{q}\boldsymbol{j} + \frac{x_3}{q}\boldsymbol{k}$ — вектор довжини 1, причому $0 \leq \varphi \leq \pi$. Якщо $x \neq 0$, то такий запис однозначний.

Вправа 4.5. *Якщо* $x = r(\cos\varphi + \boldsymbol{v} \cdot \sin\varphi) \neq 0$, *то існує обернений елемент* $x^{-1} = \frac{1}{r}(\cos\varphi - \boldsymbol{v} \cdot \sin\varphi)$.

Із цієї вправи, зокрема, випливає, що алгебра кватерніонів є тілом.

Безпосередньо перевіряється (зробіть це!), що для кожного ненульового кватерніона a відображення

$$\varphi_a : \mathbb{H} \to \mathbb{H}, \quad x \mapsto a^{-1}xa,$$

[10] Правило множення кватерніонів ірландський математики Гамільтон відкрив у 1843 р. Згодом — у 50-х рр. XIX ст. — Гамільтон розробив теорію кватерніонів досить глибоко. Ця теорія стала одним із поштовхів до створення векторної алгебри, основи якої заклав у 80-х рр. XIX ст. американський математик і фізик Гіббс.

є автоморфізмом $\mathbb{H}$ як тіла. Зокрема, φ_a є автоморфізмом $\mathbb{H}$ як алгебри над $\mathbb{R}$, а тому φ_a є лінійним перетворенням $\mathbb{H}$ як векторного простору над $\mathbb{R}$.

Твердження 4.3. *a) Для автоморфізму φ_a кожен із підпросторів $\langle 1\rangle$ і $\langle \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\rangle$ є інваріантним.*

b) $\varphi_a(\overline{x}) = \overline{\varphi_a(x)}$.

Доведення. a) Інваріантність підпростору $\langle 1\rangle$ очевидна. Нехай тепер кватерніон x є чисто уявним. Ми вже встановили, що кватерніон буде чисто уявним тоді й лише тоді, коли його квадрат є від'ємним дійсним число. Але

$$\varphi_a(x)\varphi_a(x) = a^{-1}xaa^{-1}xa = a^{-1}xxa = xxa^{-1}a = xx.$$

b) Нехай $x = x_0 + \widehat{x}$. Тоді $\varphi_a(x) = \varphi_a(x_0) + \varphi_a(\widehat{x})$ і за доведеним у попередньому пункті $\overline{\varphi_a(x)} = \varphi_a(x_0) - \varphi_a(\widehat{x})$. З іншого боку, $\varphi_a(\overline{x}) = \varphi_a(x_0 - \widehat{x}) = \varphi_a(x_0) - \varphi_a(\widehat{x})$. □

Теорема 4.2. *Відображення $\Phi : a \mapsto \varphi_a$ є гомоморфізмом мультиплікативної групи $\mathbb{H}^*$ у групу ізометрій алгебри $\mathbb{H}$ як евклідового простору. Ядром цього гомоморфізму є $\mathbb{R}^*$.*

Доведення. Позаяк φ_a є лінійним перетворенням простору $\mathbb{H}$, то щоб показати, що φ_a є ізометрією, досить показати, що φ_a зберігає довжини векторів. Це справді так:

$$\begin{aligned} N(\varphi_a(x)) = \varphi_a(x)\cdot\overline{\varphi_a(x)} = \varphi_a(x)\cdot\varphi_a(\overline{x}) = a^{-1}xa\cdot a^{-1}\overline{x}a = \\ = a^{-1}x\cdot\overline{x}a = a^{-1}N(x)a = N(x)a^{-1}a = N(x)\,. \end{aligned}$$

Гомоморфність відображення Φ очевидна:

$$\varphi_{ab}(x) = (ab)^{-1}xab = b^{-1}a^{-1}xab = b^{-1}(a^{-1}xa)b = \varphi_b(\varphi_a(x)) = (\varphi_a\varphi_b)(x).$$

Зрозуміло також, що для кожного $a \in \mathbb{R}^*$ відображення φ_a є тотожним автоморфізмом алгебри $\mathbb{H}$. Тому $\mathbb{R}^* \subseteq \operatorname{Ker}\Phi$. Навпаки, нехай $a \notin \mathbb{R}^*$. Без обмеження загальності можна вважати, що $a = \alpha + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ і $\beta \neq 0$. Тоді $a\boldsymbol{j} \neq \boldsymbol{j}a$ і $\boldsymbol{j} = a^{-1}a\boldsymbol{j} \neq a^{-1}\boldsymbol{j}a = \varphi_a(\boldsymbol{j})$, а тому $a \notin \operatorname{Ker}\Phi$. Отже, $\mathbb{R}^* = \operatorname{Ker}\Phi$. □

Із теореми 4.2 випливає, що при вивченні автоморфізмів вигляду φ_a можна обмежитися лише тими $a \in \mathbb{H}$, для яких $N(a) = 1$, тобто тривимірною сферою S радіуса 1 у чотиривимірному евклідовому просторі $\mathbb{H}$. При цьому вектори, які відрізняються знаком, дають один і

той самий автоморфізм (тобто діаметрально протилежні точки сфери треба ототожнити). Таким чином, групу внутрішніх автоморфізмів тіла $\mathbb{H}$ (тобто автоморфізмів вигляду φ_a) можна ототожнити із тривимірним проективним дійсним простором $P\mathbb{R}^3$.

Через некомутативність множення теорія рівнянь над тілом кватерніонів набагато складніша від такої теорії над полями $\mathbb{R}$ або $\mathbb{C}$. Труднощі з'являються вже при розв'язуванні лінійного рівняння з одним невідомим. Загальний вигляд такого рівняння

$$axb + cx + xd + e = 0\,. \tag{4.3}$$

Якщо записати невідоме й коефіцієнти в алгебричній формі, то рівняння (4.3) зведеться до дійсної квадратної системи лінійних рівнянь відносно координат x_0, x_1, x_2, x_3 невідомого $x = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$. Але виразити x у безкоординатній формі — безпосередньо через коефіцієнти a, b, c, d, e (або хоча б через їх скалярні й векторні частини) — дуже складно.

Ще заплутаніша ситуація із системами лінійних рівнянь і рівняннями вищих степенів.

Твердження 4.4. *Кожен кватерніон є коренем деякого квадратного рівняння з дійсними коефіцієнтами.*

Доведення. Кожен кватерніон $a = a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}$ є коренем квадратного рівняння $(x - a)(x - \overline{a}) = 0$. Але з рівності (4.2) випливає, що

$$(x - a)(x - \overline{a}) = x^2 - 2a_0x + N(a). \tag{4.4}$$

Отже, коефіцієнти цього рівняння є дійсними.

Доведення ще не можна вважати завершеним, бо рівність (4.4) отримана за припущення, що x комутує з $\widehat{a}$. Але те, що a справді є коренем многочлена $x^2 - 2a_0x + N(a)$, можна вже перевірити безпосередньо. $\square$

Із доведення твердження 4.4 випливає, що для довільних дійсних чисел a_0 і $b > a_0^2$ кватерніон a буде коренем квадратного рівняння $x^2 - 2a_0x + b = 0$ тоді й лише тоді, коли він має вигляд $a = a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}$, де $a_1^2 + a_2^2 + a_3^2 = b - a_0^2$. Отже, векторні частини коренів цього рівняння утворюють у тривимірному евклідовому просторі сферу радіуса $\sqrt{b - a_0^2}$. Зокрема, при $b > a_0^2$ рівняння $x^2 - 2a_0x + b = 0$ матиме в тілі $\mathbb{H}$ нескінченно багато коренів (на відміну від поля $\mathbb{R}$, де квадратне рівняння має щонайбільше 2 корені).

На закінчення розділу зауважимо, що аналог алгебри кватерніонів можна визначити для довільного поля P. Для цього в чотиривимірному векторному просторі V над P елементи певної бази треба позначити 1, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ і визначити множення за допомогою таблиці 4.1. Відповідну алгебру позначають $\mathbb{H}(P)$.

Задача 4.3. *Доведіть, що алгебра $\mathbb{H}(P)$ буде тілом тоді й лише тоді, коли для довільних x_0, x_1, x_2, x_3 із P з рівності $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ випливає рівність $x_0 = x_1 = x_2 = x_3 = 0$.*

4.3 Тіла

Твердження 4.5. *Асоціативна алгебра $\mathcal{A}$ з діленням є тілом.*

Доведення. Виберемо довільний $a \neq 0$. Нехай e_a — розв'язок рівняння $ax = a$. Позаяк довільний елемент b можемо записати у вигляді $b = ca$, то

$$b \cdot e_a = ca \cdot e_a = c \cdot ae_a = ca = b\,.$$

Отже, e_a є правою одиницею алгебри $\mathcal{A}$. Аналогічно доводиться існування в $\mathcal{A}$ лівої одиниці. Але тоді в $\mathcal{A}$ існує просто одиниця e. Існування обернених елементів тепер випливає з розв'язності рівнянь $ax = e$ і $ya = e$. □

Над полем $\mathbb{R}$ дійсних чисел є три класичні скінченновимірні алгебри з діленням — це самé поле $\mathbb{R}$, поле комплексних чисел $\mathbb{C}$ і тіло кватерніонів $\mathbb{H}$. Виявляється, що цими алгебрами вичерпуються всі скінченновимірні асоціативні алгебри з діленням над $\mathbb{R}$.

Теорема 4.3 (Фробеніус, 1903)**.** *Кожна скінченновимірна асоціативна алгебра $\mathcal{A}$ з діленням над полем $\mathbb{R}$ ізоморфна або полю $\mathbb{R}$, або полю комплексних чисел $\mathbb{C}$, або тілу кватерніонів $\mathbb{H}$.*

Доведення. За твердженням 4.5 алгебра $\mathcal{A}$ є тілом, а тому не містить дільників нуля. Поле $\mathbb{R}$ природно ототожнюється з його образом при зануренні $\mathbb{R} \hookrightarrow \mathcal{A}$, $x \mapsto x \cdot 1$. Тоді $\mathcal{A}$ можна розглядати як скінченне розширення $\mathbb{R}$. Якщо $[\mathcal{A} : \mathbb{R}] = 1$, то $\mathcal{A} = \mathbb{R}$. Тому далі вважаємо, що $[\mathcal{A} : \mathbb{R}] = n > 1$.

Лема 4.1. *Для кожного елемента $a \in \mathcal{A} \setminus \mathbb{R}$ просте розширення $\mathbb{R}(a)$ ізоморфне полю $\mathbb{C}$.*

Доведення. Позаяк $[\mathcal{A} : \mathbb{R}] = n$, то елементи 1, a, $\ldots$, a^n — лінійно залежні над $\mathbb{R}$. Тому в $\mathbb{R}[x]$ для a існує анулюючий многочлен. Але тоді для a існує й мінімальний многочлен $m_a(x)$, причому він буде незвідним в $\mathbb{R}[x]$, бо інакше в $\mathcal{A}$ були б дільники нуля. Оскільки $a \notin \mathbb{R}$ і кожен незвідний над $\mathbb{R}$ многочлен із $\mathbb{R}[x]$ має степінь ≤ 2, то

$$m_a(x) = x^2 + \alpha x + \beta, \quad \text{де} \quad \alpha^2 - 4\beta < 0\,.$$

Тоді $\left(a + \frac{\alpha}{2}\right)^2 = \frac{\alpha^2}{4} - \beta < 0$, і для елемента $b = \left(a + \frac{\alpha}{2}\right) \Big/ \sqrt{\beta - \frac{\alpha^2}{4}}$ маємо

$$\mathbb{R}(b) = \mathbb{R}(a) \quad \text{і} \quad b^2 = -1\,.$$

Тому $\mathbb{R}(b) \simeq \mathbb{C}$. □

Лема 4.2. *Якщо алгебра $\mathcal{A}$ — комутативна, то вона ізоморфна полю $\mathbb{C}$.*

Доведення. Справді, у цьому випадку алгебра $\mathcal{A}$ є полем, а тому, за теоремою про примітивний елемент, вона є простим алгебричним розширенням поля $\mathbb{R}$. Але тоді з леми 4.1 випливає, що $\mathcal{A} \simeq \mathbb{C}$. □

Лема 4.3. *Нехай $a, b \in \mathcal{A} \setminus \mathbb{R}$ і $\mathbb{R}(b) \neq \mathbb{R}(a)$. Тоді $ab \neq ba$.*

Доведення. Якби було $ab = ba$, то алгебра $\mathbb{R}(a, b)$ була б комутативною і, за лемою 4.2, ізоморфною полю $\mathbb{C}$. Зокрема, було б $[\mathbb{R}(a, b) : \mathbb{R}] = 2$. Але з умови і леми 4.1 випливає, що $a \notin \mathbb{R}(b)$ і $b \notin \mathbb{R}(a)$. Тому $[\mathbb{R}(a, b) : \mathbb{R}] \geq 3$. Отримана суперечність доводить лему. □

Оскільки $\mathbb{R}$ лежить у центрі алгебри $\mathcal{A}$, то з леми 4.3, зокрема, випливає, що коли $[\mathcal{A} : \mathbb{R}] \geq 3$, то центр $\mathcal{A}$ збігається з $\mathbb{R}$. Легко перевіряється, що для кожного ненульового елемента a відображення $\varphi_a : x \mapsto a^{-1}xa$ буде автоморфізмом тіла $\mathcal{A}$. Із леми 4.3 також випливає, що коли $[\mathcal{A} : \mathbb{R}] \geq 3$ і $a \notin \mathbb{R}$, то автоморфізм φ_a буде нетривіальним, а його полем нерухомих точок буде $\mathbb{R}(a)$.

Лема 4.4. *Нехай тіло $\mathcal{A}$ — не комутативне. Тоді для кожного $a \in \mathcal{A} \setminus \mathbb{R}$ існують такі елементи $b \in \mathbb{R}(a)$ та $c \notin \mathbb{R}(a)$, що $b^2 = c^2 = -1$ і $\varphi_b(c) = -c$. Зокрема, $\varphi_b(c)$ є автоморфізмом поля $\mathbb{R}(c)$ із полем нерухомих точок $\mathbb{R}$.*

Доведення. За лемою 4.1 у полі $\mathbb{R}(a)$ існує такий елемент b, що $b^2 = -1$ і $\mathbb{R}(b) = \mathbb{R}(a)$. Виберемо довільний елемент $d \notin \mathbb{R}(a)$. Позначимо $d' = \varphi_b(d)$. Зауважимо, що $d' \neq d$. Оскільки

$$\varphi_b(d') = b^{-1} \cdot b^{-1} db \cdot b = (-1) \cdot d \cdot (-1) = d,$$

то для елемента $c = d - d'$ маємо $\varphi_b(c) = d' - d = -c$. Звідси випливає, по-перше, що $c \notin \mathbb{R}(a)$, а по-друге, що $\varphi_b(\mathbb{R}(c)) = \mathbb{R}(c)$, тобто що φ_b є автоморфізмом поля $\mathbb{R}(c)$. Нехай $m_c(x) = x^2 + \alpha x + \beta$ — мінімальний многочлен для c, як елемента розширення $\mathbb{R} \subset \mathbb{R}(c)$. Тоді

$$0 = \varphi_b(0) = \varphi_b(c^2 + \alpha c + \beta) = (-c)^2 + \alpha(-c) + \beta.$$

Отже, $-c$ також є коренем многочлена $m_c(x)$. Але тоді $\alpha = c + (-c) = 0$ і $c^2 = -\beta < 0$. Перейшовши, у разі потреби, до $c/\sqrt{\beta}$, можемо вважати, що $c^2 = -1$.

Остання частина твердження випливає з того, що полем нерухомих точок автоморфізму φ_b є $\mathbb{R}(a)$ і $\mathbb{R}(a) \cap \mathbb{R}(c) = \mathbb{R}$. □

Лема 4.5. *Нехай $[\mathcal{A} : \mathbb{R}] > 2$, а елементи b і c такі, як у попередній лемі. Тоді підалгебра $\mathbb{R}(b, c)$ ізоморфна тілу кватерніонів $\mathbb{H}$.*

Доведення. Покажемо, що елементи 1, b, c і bc лінійно незалежні над $\mathbb{R}$. Справді, нехай для деяких $x, y, z \in \mathbb{R}$ буде

$$bc = x + yb + zc\,. \tag{4.5}$$

Помноживши цю рівність один раз на z, а другий раз — зліва на b, одержуємо, що

$$zbc = zx + zyb + z^2 c = y - xb - c\,.$$

Із лінійної незалежності 1, b і c випливає, що $z^2 = -1$. Але це суперечить тому, що $z \in \mathbb{R}$. Отже, рівність (4.5) неможлива, що й доводить лінійну незалежність 1, b, c і bc.

Оскільки $b^{-1}cb = \varphi_b(c) = -c$, то $-bc = cb$. Тому елементи 1, b, c і bc утворюють базу алгебри $\mathbb{R}(b, c)$ як векторного простору над $\mathbb{R}$. Легко перевіряється, що структурні константи алгебри $\mathbb{R}(b, c)$ у цій базі збігаються зі структурними константами алгебри $\mathbb{H} = \mathbb{R}(1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$. Тому $\mathbb{R}(b, c) \simeq \mathbb{H}$. □

Припустимо тепер, що алгебра $\mathcal{A}$ не збігається з побудованою в лемі 4.5 підалгеброю $\mathbb{R}(b, c)$. Тоді існує елемент $g \notin \mathbb{R}(b, c)$. Нехай $g' = \varphi_b(g)$.

Тоді $\varphi_b(g') = g$ і $\varphi_b(g+g') = g+g'$. Отже, $g+g' \in \mathbb{R}(b) \subset \mathbb{R}(b,c)$. Тому елемент $p = g - g' = 2g - (g+g')$ не належить $\mathbb{R}(b,c)$. Крім того, $\varphi_b(p) = -p$. Далі, як і в лемі 4.5, будуємо підалгебру $\mathbb{R}(b,p)$, ізоморфну тілу $\mathbb{H}$. Зауважимо, що $\mathbb{R}(b,c) \cap \mathbb{R}(b,p) = \mathbb{R}(b)$.

Позаяк

$$\varphi_b(cp) = \varphi_b(c)\varphi_b(p) = (-c)(-p) = cp,$$

то $cp \in \mathbb{R}(b)$. Але тоді $p = (-c)\cdot cp \in \mathbb{R}(b,c)$, усупереч вибору p. Отже, $\mathcal{A} = \mathbb{R}(b,c) \simeq \mathbb{H}$. □

У теоремі Фробеніуса на скінченновимірну алгебру $\mathcal{A}$ накладаються два обмеження: бути асоціативною й бути алгеброю з діленням. Виникає природне питання: що буде, коли послабити обмеження? Виявляється, що відмова від асоціативності не дуже розширює принаймні список розмірностей таких алгебр. Справді, у 1958 р. Мілнор довів таку теорему:

Теорема 4.4 (Мілнор)**.** *Над полем* $\mathbb{R}$ *кожна скінченновимірна алгебра з діленням має розмірність* 1, 2, 4 *або* 8.

Доведення цієї теореми вимагає досить тонких топологічних міркувань, тому ми його не наводимо[11].

Серед 8-вимірних дійсних алгебр із діленням особливу роль відіграє *алгебра октав Келі*. Це множина виразів вигляду $\boldsymbol{x}+\boldsymbol{y}\boldsymbol{e}$, де $\boldsymbol{x}$ і $\boldsymbol{y}$ — кватерніони, а $\boldsymbol{e}$ — новий символ. Додавання таких виразів і їх множення на скаляри з $\mathbb{R}$ визначаються природно:

$$(\boldsymbol{x}_1 + \boldsymbol{y}_1\boldsymbol{e}) + (\boldsymbol{x}_2 + \boldsymbol{y}_2\boldsymbol{e}) = (\boldsymbol{x}_1 + \boldsymbol{x}_2) + (\boldsymbol{y}_1 + \boldsymbol{y}_2)\boldsymbol{e},$$
$$\alpha(\boldsymbol{x}+\boldsymbol{y}\boldsymbol{e}) = \alpha\boldsymbol{x} + (\alpha\boldsymbol{y})\boldsymbol{e}.$$

Із цих правил бачимо, що елементи 1, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$, $\boldsymbol{e}$, $\boldsymbol{i}\boldsymbol{e}$, $\boldsymbol{j}\boldsymbol{e}$, $\boldsymbol{k}\boldsymbol{e}$ утворюють базу алгебри Келі як векторного простору над $\mathbb{R}$.

Множення октав визначається правилом[12]

$$(\boldsymbol{x}_1 + \boldsymbol{y}_1\boldsymbol{e})\cdot(\boldsymbol{x}_2 + \boldsymbol{y}_2\boldsymbol{e}) = (\boldsymbol{x}_1\boldsymbol{x}_2 - \overline{\boldsymbol{y}_2}\boldsymbol{y}_1) + (\boldsymbol{y}_2\boldsymbol{x}_1 + \boldsymbol{y}_1\overline{\boldsymbol{x}_2})\boldsymbol{e}\,.$$

[11] Позаяк скінченновимірна лінійна алгебра (не обов'язково асоціативна) є алгеброю з діленням тоді й лише тоді, коли вона не містить дільників нуля (див. задачу 7), то в теоремі Мілнора алгебру з діленням можна замінити на *алгебру без дільників нуля*.

[12] Якщо ототожнити кватерніон $x_0 + x_1\boldsymbol{i}$ з відповідним комплексним числом, то довільний кватерніон $x = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$ можна записати у вигляді $x = z + u\boldsymbol{j}$, де $z = x_0 + x_1\boldsymbol{i}$ та $u = x_2 + x_3\boldsymbol{i}$ — комплексні числа. Тоді правило множення кватерніонів набуває вигляду $(z_1 + u_1\boldsymbol{j})(z_2 + u_2\boldsymbol{j}) = (z_1z_2 - \overline{u_2}u_1) + (u_2z_1 + u_1\overline{z_2})\boldsymbol{j}$. Тому правило множення октав є аналогом правила множення кватерніонів.

Перевірку дистрибутивності цього множення відносно додавання октав та умови 3) із означення алгебри залишаємо читачеві як вправу.

Теорема 4.5 (Веддербарн). *Скінченне тіло є полем.*

Доведення. Нехай K — скінченне тіло і $Z(K) = P$. Тоді P — поле і $|P| = p^m$ для деякого простого числа p. Нехай K як векторний простір над P має розмірність n. Тоді $|K| = q^n$, де $q = p^m$. Крім того, $P^* = Z(K^*)$.

Нехай $\overline{g}_1, \ldots, \overline{g}_r$ — усі неодноелементні класи спряженості групи K^*, а $g_1, \ldots, g_r$ — їх представники. Якщо $C(g_i)$ — централізатор елемента g_i, то $q^n - 1 = |C(g_i)| \cdot |\overline{g}_i|$. За формулою класів

$$q^n - 1 = |Z(K^*)| + |\overline{g}_1| + \cdots + |\overline{g}_r| = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{|C(g_i)|}\,. \tag{4.6}$$

З іншого боку, для кожного $1 \le i \le r$ множина $C_i = C(g_i) \cup \{0\}$ утворює тіло, причому $P \subseteq C_i \subseteq K$. Тому $|C_i| = q^{m_i}$ і $|C(g_i)| = q^{m_i} - 1$. Оскільки K є розширенням C_i, то існує таке t_i, що $|K| = |C_i|^{t_i}$. Отже, $q^n = (q^{m_i})^{t_i}$, а тому $m_i | n$.

Нехай $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ — всі первісні корені степеня n з одиниці, а $\Phi_n(x) = (x - \varepsilon_1) \cdots (x - \varepsilon_{\varphi(n)})$ — n-й многочлен поділу круга. Використовуючи рівність

$$x^n - 1 = \prod_{d|n} \Phi_d(x)\,, \tag{4.7}$$

за допомогою індукції легко доводиться, що многочлен $\Phi_n(x) = x^{\varphi(n)} + \cdots$ має цілі коефіцієнти. Справді, нехай всі многочлени $\Phi_d(x)$ при $d < n$ мають цілі коефіцієнти, а для

$$\Phi_n(x) = x^{\varphi(n)} + \cdots + a_k x^k + \cdots$$

це не так, причому a_k є першим нецілим коефіцієнтом. Тоді коефіцієнт при $x^{n-\varphi(n)+k}$ у лівій частині рівності (4.7) буде цілим, а відповідний коефіцієнт у правій частині дорівнюватиме $l + a_k$, де l — якесь ціле число, що неможливо.

Оскільки m_i ділить n, то $x^{m_i} - 1$ ділить $x^n - 1$ і

$$\frac{x^n - 1}{x^{m_i} - 1} = \frac{\prod_{d|n} \Phi_d(x)}{\prod_{d|m_i} \Phi_d(x)} = \Phi_n(x) \cdot \Psi_i(x)\,,$$

де многочлен $\Psi_i(n)$ також має цілі коефіцієнти. Із рівностей (4.7) і (4.6) тепер випливає, що

$$\Phi_n(q) \cdot \prod_{d|n,\, d\neq n} \Phi_d(q) = q^n - 1 = q - 1 + \sum_{i=1}^{r} \Phi_n(q) \cdot \Psi_i(q)\,,$$

звідки

$$q - 1 = \Phi_n(q) \cdot \left(\prod_{d|n,\, d\neq n} \Phi_d(q) - \sum_{i=1}^{r} \Phi_n(q) \cdot \Psi_i(q) \right).$$

Отже, $\Phi_n(q) \mid (q-1)$, а тому $|\Phi_n(q)| \leq q - 1$. З іншого боку, якщо $n > 1$, то $\Phi_n(q)$ розкладається в добуток $\Phi_n(q) = \prod\limits_{\varepsilon}(q - \varepsilon)$, де ε пробігає всі первісні корені степеня з 1.

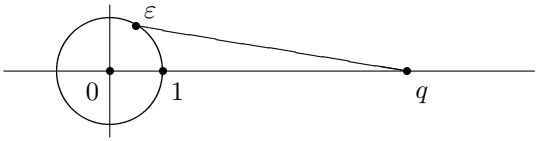


Рис. 6

Але $|q - \varepsilon| > q - 1$ (рис. 6), тому при $n > 1$ маємо $|\Phi_n(q)| > q - 1$. Отже, $n = 1$ і $K = Z(K)$ — поле. □

4.4 Зображення алгебр

Далі до кінця цієї глави розглядаються лише скінченновимірні асоціативні алгебри.

Означення 4.4. ***Лінійним зображенням*** (*або просто* ***зображенням***) *P-алгебри $\mathcal{A}$ називається довільний гомоморфізм вигляду $\varphi : \mathcal{A} \to \operatorname{End} V$, $a \mapsto \varphi_a$, де V — скінченновимірний*[13] *векторний простір над полем P. Розмірність простору V називається* ***розмірністю*** *або* ***степенем*** *зображення φ.*

Сукупність $\operatorname{Ker}\varphi$ тих елементів алгебри $\mathcal{A}$, які при зображенні φ переходять у нульове перетворення простору V, називається *ядром* зображення φ. Очевидно, що $\operatorname{Ker}\varphi$ є двостороннім ідеалом алгебри $\mathcal{A}$.

[13] Для нескінченновимірних алгебр розглядають і *нескінченновимірні* зображення, для яких простір V є нескінченновимірним.

Зображення, при якому кожен елемент алгебри $\mathcal{A}$ переходить у нульове перетворення простору V, називається *тривіальним* або *нульовим*. Зображення називається *точним*, якщо воно ін'єктивне.

Якщо у просторі V зафіксувати деяку базу $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$, то кожному елементу a алгебри $\mathcal{A}$ природно зіставляється матриця M_a перетворення φ_a у цій базі. Оскільки при цьому $M_a M_b = M_{ba}$, то відображення $\widehat{\varphi} : \mathcal{A} \to M_n(P)$, $a \mapsto M_a$, буде антигомоморфізмом алгебри $\mathcal{A}$ у повну матричну алгебру $M_n(P)$. Відображення $\widehat{\varphi}$ називається *матричним зображенням* алгебри $\mathcal{A}$. Із другого боку, від матричного зображення алгебри завжди можна перейти до лінійного, якщо зафіксувати деяку базу і дивитися на матрицю M_a як на матрицю в цій базі певного лінійного перетворення φ_a.

Зауваження. **1**. Таким чином, лінійні й матричні зображення — це два боки однієї медалі, залежно від того, чи ми описуємо лінійні перетворення простору V у безкоординатній формі, чи прив'язуємося до конкретної бази. Матричний підхід зручніший з обчислювального погляду, але він позбавлений геометричної наочності й менш інваріантний. Тому важливо навчитись вільно переходити, залежно від конкретної мети, від одного типу зображень до іншого.

2. Те, що матричне зображення є не гомоморфізмом, а антигомоморфізмом, не є істотним, оскільки замінивши матриці M_a транспонованими, одержимо вже гомоморфізм. Тому часто матричними зображеннями алгебри $\mathcal{A}$ часто називають саме гомоморфізми вигляду $\mathcal{A} \to M_n(P)$.

Вибираючи у просторі V різні бази, ми для одного й того самого лінійного зображення $\varphi : \mathcal{A} \to \operatorname{End} V$ будемо отримувати різні матричні зображення $\widehat{\varphi} : \mathcal{A} \to M_n(P)$. Із другого боку, одна й та сама матриця в різних базах простору V відповідає різним лінійним перетворенням. Зрозуміло, що зображення, які розрізняються лише вибором бази простору V, треба в певному сенсі вважати однаковими. Це приводить до такого означення.

Означення 4.5. *Два зображення $\varphi' : \mathcal{A} \to \operatorname{End} V'$ і $\varphi'' : \mathcal{A} \to \operatorname{End} V''$ алгебри $\mathcal{A}$ називаються* ***еквівалентними*** *або* ***подібними****, якщо існує такий ізоморфізм $\psi : V' \to V''$ векторних просторів, що $\varphi'_a \psi = \psi \varphi''_a$ для довільного $a \in \mathcal{A}$.*

Для відповідних матричних зображень це означає, що для кожного $a \in \mathcal{A}$ виконується рівність $S \cdot M'_a = M''_a \cdot S$, де S — матриця відображення ψ у відповідних базах. Таким чином, еквівалентність лінійних

зображень φ' і φ'' означає, що коли бази просторів V' і V'' вибрати узгодженими в тому сенсі, що база простору V'' є образом при ізоморфізмі ψ бази простору V', то для кожного $a \in \mathcal{A}$ перетворення φ'_a і φ''_a будуть записуватися в цих базах однаковими матрицями.

Підпростір $U \subseteq V$ називається *інваріантним* відносно лінійного зображення $\varphi : \mathcal{A} \to \operatorname{End} V$, якщо $\varphi_a(U) \subseteq U$ для всіх $a \in \mathcal{A}$. Якщо $U \neq V$, то говорять про *власний* інваріантний підпростір.

Якщо $U \subseteq V$ — інваріантний підпростір, то для кожного $a \in \mathcal{A}$ можна розглянути обмеження $\varphi_a|_U$ перетворення φ_a на підпростір U. Це дає лінійне зображення $\varphi|_U : \mathcal{A} \to \operatorname{End} U$ алгебри $\mathcal{A}$, яке називається *звуженням* зображення φ на підпростір U або *підзображенням* зображення φ.

Якщо простір V розкладається у пряму суму $V = U \oplus W$ інваріантних підпросторів U та W, то кажуть, що зображення $\varphi : \mathcal{A} \to \operatorname{End} V$ розкладається у *пряму суму* зображень $\varphi|_U$ та $\varphi|_W$, і записують $\varphi = \varphi|_U \dot{+} \varphi|_W$.

Серед усіх зображень алгебри $\mathcal{A}$ особливу роль відіграє зображення, яке називається *правим регулярним* або просто *регулярним*. Для цього розглянемо $\mathcal{A}$ як векторний простір і кожному $a \in \mathcal{A}$ поставимо у відповідність так званий правий зсув за допомогою елемента a: $\lambda_a : x \mapsto xa$. Легко перевіряється, що λ_a є лінійним перетворенням простору $\mathcal{A}$, а відображення $a \mapsto \lambda_a$ — лінійним зображенням алгебри $\mathcal{A}$.

Вправа 4.6. *Доведіть, що підпростір $U \subseteq \mathcal{A}$ асоціативної алгебри $\mathcal{A}$ буде інваріантним відносно регулярного зображення тоді й лише тоді, коли U є правим ідеалом алгебри $\mathcal{A}$.*

Твердження 4.6. *Регулярне зображення алгебри з одиницею є точним.*

Доведення. Якщо $a \neq b$, то

$$\lambda_a(1) = 1 \cdot a = a \neq b = 1 \cdot b = \lambda_b(1)\,,$$

а тому $\lambda_a \neq \lambda_b$. □

Наслідок 4.1. *Для кожної асоціативної алгебри існує точне зображення.*

Доведення. За теоремою 4.1 кожну асоціативну алгебру $\mathcal{A}$ можна розширити до алгебри $\mathcal{A}_1$ з одиницею. Розглянемо регулярне зображення

λ алгебри $\mathcal{A}_1$. За твердженням 4.6 воно є точним. Якщо тепер зображення λ обмежити на підалгебру $\mathcal{A}$, то одержимо точне зображення $\lambda|_{\mathcal{A}} : \mathcal{A} \to \mathrm{End}A_1$ алгебри $\mathcal{A}$. □

Наслідку 4.1 можна, враховуючи його доведення, надати такого вигляду.

Теорема 4.6 (Келі). *Кожна n-вимірна асоціативна алгебра $\mathcal{A}$ над полем P ізоморфна деякій підалгебрі з $M_k(P)$, де $k \leq n+1$.*

Таким чином, повні матричні алгебри відіграють у теорії алгебр роль, аналогічну ролі симетричних груп у теорії груп. Крім усього, після занурення даної алгебри $\mathcal{A}$ в алгебру $M_k(P)$ для дослідження $\mathcal{A}$ можна використати потужний апарат числення матриць.

Означення 4.6. *Зображення $\varphi : \mathcal{A} \to \mathrm{End}\, V$ називається **незвідним**, якщо простір V не має нетривіальних інваріантних підпросторів.*

Нехай $\varphi : \mathcal{A} \to \mathrm{End}\, V$ — зображення алгебри $\mathcal{A}$. Для довільного вектора $v \in V$ множина $U_v = \{\varphi_a(v) \mid a \in \mathcal{A}\}$ буде інваріантним підпростором зображення φ. Якщо $U_v = V$, то вектор v називається *циклічним* (відносно зображення φ). Із означення одразу випливає

Твердження 4.7. *Зображення $\varphi : \mathcal{A} \to \mathrm{End}\, V$ буде незвідним тоді й лише тоді, коли кожен ненульовий вектор є циклічним.*

Нагадаємо, що кратні $c\cdot\varepsilon$ тотожного перетворення ε називаються *гомотетіями* простору V. В основі багатьох міркувань теорії зображень лежить

Лема 4.6 (Шур). *Нехай $\varphi : \mathcal{A} \to \mathrm{End}\, V$ — незвідне зображення комплексної алгебри $\mathcal{A}$. Перетворення $\psi \in \mathrm{End}V$ комутує з усіма перетвореннями φ_a тоді й лише тоді, коли ψ — гомотетія.*

Доведення. Очевидно, що гомотетія комутує з довільним лінійним перетворенням простору. Тому доведення вимагає лише необхідність умови.

Нехай лінійне перетворення ψ комутує з усіма φ_a. Лінійне перетворення комплексного простору завжди має власні вектори. Нехай $\boldsymbol{v} \neq \mathbf{0}$ — один із власних векторів перетворення ψ, а c — відповідне власне число. Перетворення $\mu = \psi - c\varepsilon$ також комутує з усіма φ_a. Тому для довільних $\boldsymbol{u} \in \mathrm{Ker}\,\mu$ та $a \in \mathcal{A}$ маємо

$$\mu(\varphi_a(\boldsymbol{u})) = (\varphi_a \cdot \mu)(\boldsymbol{u}) = (\mu \cdot \varphi_a)(\boldsymbol{u}) = \varphi_a(\mu(\boldsymbol{u})) = \varphi_a(\mathbf{0}) = \mathbf{0}\,.$$

Отже, $\varphi_a(\boldsymbol{u}) \in \mathrm{Ker}\,\mu$, а тому $\mathrm{Ker}\,\mu$ є інваріантним підпростором зображення φ. Позаяк це зображення незвідне і $\mathrm{Ker}\,\mu \neq 0$ (бо $\boldsymbol{v} \in \mathrm{Ker}\,\mu$), то $\mathrm{Ker}\,\mu = V$. Тому $\psi - c\varepsilon = 0$ і $\psi = c\varepsilon$. □

4.5 Прості алгебри

Якщо алгебра $\mathcal{A}$ має власний двосторонній ідеал I, то в певному сенсі її вивчення можна звести до вивчення двох "менших" алгебр: підалгебри I та факторалгебри $\mathcal{A}/I$. Тому зрозумілою є важливість такого поняття:

Означення 4.7. *Нетривіальна алгебра, яка не має нетривіальних двосторонніх ідеалів, називається* ***простою****.*

Очевидно, що кожна алгебра з діленням є простою. Менш тривіальний приклад дає

Теорема 4.7. *Алгебра $M_n(P)$ є простою.*

Доведення. Нехай $I \subseteq M_n(P)$ — ненульовий ідеал і $A = (a_{ij})$ — ненульова матриця з I. Через E_{ij} позначимо матричну одиницю — матрицю, у якій на перетині i-го рядка і j-го стовпця стоїть 1, а решта елементів — нулі. Нехай $a_{kl} \neq 0$. Із рівностей

$$\frac{1}{a_{kl}} E_{kk} A E_{ll} = E_{kl} \quad \text{і} \quad E_{ik} E_{kl} E_{lj} = E_{ij}$$

випливає, що ідеал J містить усі матричні одиниці. Позаяк кожна матриця $B = (b_{ij})$ розкладається в лінійну комбінацію $B = \sum_{ij} b_{ij} E_{ij}$ матричних одиниць, то J містить усі матриці, а тому збігається з $M_n(P)$. □

Пізніше ми побачимо (теорема 4.11), що у випадку поля комплексних чисел цим прикладом (із точністю до ізоморфізму) вичерпуються всі скінченновимірні прості алгебри.

Вправа 4.7. *Кожне ненульове зображення простої алгебри є точним.* (*Вказівка.* Ядро зображення є ідеалом.)

Теорема 4.8. *Для кожної простої скінченновимірної алгебри $\mathcal{A}$ існує точне незвідне зображення.*

Доведення. Зі скінченновимірності регулярного зображення випливає існування для такого зображення мінімальних інваріантних підпросторів. Нехай $\varphi : \mathcal{A} \to \operatorname{End} V$ — звуження регулярного зображення на один із таких підпросторів. Згідно із вправою 4.7 досить показати, що зображення φ є ненульовим. А для цього, у свою чергу, досить показати, що $b\mathcal{A} = \{ba \mid a \in \mathcal{A}\} \neq 0$ для кожного ненульового $b \in V$.

Припустимо, що $b\mathcal{A} = 0$. Тоді $\mathcal{A}b$ є двостороннім ідеалом. Із простоти $\mathcal{A}$ випливає, що або $\mathcal{A}b = 0$, або $\mathcal{A}b = \mathcal{A}$. У першому випадку множина

$I = \{\alpha b \mid \alpha \in P\}$ є двостороннім ідеалом, а тому, унаслідок простоти $\mathcal{A}$, $I = \mathcal{A}$. Але тоді $\mathcal{A}^2 = 0$, тобто алгебра $\mathcal{A}$ є тривіальною. Якщо ж $\mathcal{A}b = \mathcal{A}$, то для довільних $x, y \in \mathcal{A}$ маємо

$$xy = x_1 b \cdot y_1 b = x_1 \cdot by_1 \cdot b = x_1 \cdot 0 \cdot b = 0\,.$$

Отже, і в цьому випадку $\mathcal{A}^2 = 0$. Таким чином, в обох випадках приходимо до суперечності з простотою алгебри $\mathcal{A}$. □

Зауваження. Для довільних алгебр точних незвідних зображень може й не існувати. Більше того, у найважливішому випадку поля комплексних чисел точні незвідні зображення мають лише прості алгебри (див. далі наслідок 4.4).

Зафіксуємо деяке точне незвідне зображення $\widetilde{\varphi} : \mathcal{A} \to \operatorname{End} V$ простої алгебри $\mathcal{A}$.

Теорема 4.9. *Нехай $\Phi : \mathcal{A} \to \operatorname{End} A$ — праве регулярне зображення простої алгебри $\mathcal{A}$, а I — його мінімальний інваріантний підпростір. Тоді*

a) звуження $\Phi^{(I)}$ зображення Φ на підпростір I еквівалентне зображенню $\widetilde{\varphi}$;

b) підпростір I (якщо його розглядати як підалгебру алгебри $\mathcal{A}$) містить ліву одиницю.

Доведення. Розглянемо довільний ненульовий елемент $a \in I$. Позаяк зображення $\widetilde{\varphi}$ точне, то $\widetilde{\varphi}_a \neq 0$. Тому існує такий елемент $w \in \mathcal{A}$, що $\widetilde{\varphi}_a(w) \neq 0$. Розглянемо відображення

$$\psi : I \to V, \qquad u \mapsto \widetilde{\varphi}_u(w).$$

Легко перевіряється, що це відображення є лінійним. Якщо $u \in \operatorname{Ker} \psi$, то для довільного $x \in \mathcal{A}$ маємо:

$$\widetilde{\varphi}_{u \cdot x}(w) = \widetilde{\varphi}_x(\widetilde{\varphi}_u(w)) = \widetilde{\varphi}_x(0) = 0.$$

А тому елемент $u \cdot x = \Phi_x(u)$ також належить $\operatorname{Ker} \psi$. Отже, $\operatorname{Ker} \psi$ є інваріантним підпростором зображення Φ. Оскільки $a \notin \operatorname{Ker} \psi$, $\operatorname{Ker} \psi \subset I$ і I є мінімальним інваріантним підпростором, то $\operatorname{Ker} \psi = \{0\}$. З іншого боку, позаяк для довільного $b \in \mathcal{A}$

$$\widetilde{\varphi}_b(\widetilde{\varphi}_a(w)) = \widetilde{\varphi}_{ab}(w) = \widetilde{\varphi}_{\Phi_b(a)}(w),$$

то $\psi(I)$ є інваріантним підпростором зображення $\widetilde{\varphi}$, причому ненульовим. Із незвідності $\widetilde{\varphi}$ випливає, що $\psi(I) = V$.

Отже, відображення $\psi : I \to V$ є ізоморфізмом. Крім того, для довільного $b \in \mathcal{A}$ діаграма

$$\begin{array}{ccc} I & \xrightarrow{\Phi_b^{(I)}} & I \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ V & \xrightarrow{\widetilde{\varphi}_b} & V \end{array}$$

комутативна, бо для довільного $u \in I$

$$\psi(\Phi_b^{(I)}(u)) = \psi(ub) = \widetilde{\varphi}_{ub}(w) = \widetilde{\varphi}_b(\widetilde{\varphi}_u(w)) = \widetilde{\varphi}_b(\psi(u)).$$

Таким чином, перша частина теореми доведена. Для доведення другої частини зауважимо, що із сюр'єктивності відображення ψ випливає існування такого елемента $e \in I$, що $\psi(e) = \widetilde{\varphi}_e(w) = w$. Тоді для довільного $u \in I$

$$\psi(eu) = \widetilde{\varphi}_{eu}(w) = \widetilde{\varphi}_u(\widetilde{\varphi}_e(w)) = \widetilde{\varphi}_u(w) = \psi(u).$$

Позаяк ψ — ізоморфізм, то $eu = u$. Отже, e є лівою одиницею підалгебри I. □

Із першої частини теореми 4.9 одразу випливає

Наслідок 4.2. *Усі точні незвідні зображення простої алгебри еквівалентні.*

Теорема 4.10. *Праве регулярне зображення простої алгебри A є прямим кратним її точного незвідного зображення.*

Доведення. Ураховуючи теорему 4.9 і наслідок з неї, досить показати, що алгебра $\mathcal{A}$ розкладається в пряму суму $I_1 \oplus \cdots \oplus I_m$ мінімальних інваріантних підпросторів правого регулярного зображення $\Phi : \mathcal{A} \to \operatorname{End} A$.

За перший доданок I_1 можемо взяти довільний мінімальний інваріантний підпростір алгебри $\mathcal{A}$. За теоремою 4.9 він (як підалгебра алгебри $\mathcal{A}$) містить принаймні одну ліву одиницю e_1.

Припустимо тепер, що вже знайдені такі мінімальні інваріантні підпростори $I_1, \ldots, I_k$, що їх сума $J_k = I_1 + \cdots + I_k$ є прямою. Якщо $J_k = \mathcal{A}$, то теорему вже доведено. У противному разі зауважимо, що J_k є правим ідеалом алгебри $\mathcal{A}$ (вправа 4.6), і припустимо, що цей ідеал містить ліву одиницю e_k. Множина $J_k' = \{a \in \mathcal{A} \mid e_k a = 0\}$ є інваріантним підпростором зображення Φ і має з J_k нульовий перетин. Крім

того, для довільного $a \in \mathcal{A}$ маємо $(a - e_k a) \in J'_k$, причому якщо $a \notin J_k$, то й $(a - e_k a) \notin J_k$. Зокрема, $a - e_k a \neq 0$.

Отже, підпростір J'_k є ненульовим. Тому в ньому можна вибрати мінімальний інваріантний підпростір I_{k+1}. Позаяк $J_k \cap I_{k+1} = 0$, то сума

$$J_{k+1} = J_k + I_{k+1} = I_1 + \cdots + I_k + I_{k+1}$$

буде прямою. Крім того, ідеал J_{k+1} також містить ліву одиницю. Справді, нехай e' — ліва одиниця ідеалу I_{k+1} (вона існує за теоремою 4.9). Розглянемо елемент $e_{k+1} = e_k + e' - e'e_k$. Зауважимо, що $e_k b = 0$ для довільного $b \in I_{k+1}$. Тому для довільного $a_1 + a_2$, де $a_1 \in J_k$, $a_{\in} I_{k+1}$, маємо

$$e_{k+1}(a_1 + a_2) = (e_k + e' - e'e_k)(a_1 + a_2) =$$
$$= e_k a_1 + e_k a_2 + e' a_1 + e' a_2 - e'e_k a_1 - e'e_k a_2 = a_1 + a_2.$$

Таким чином, до суми $J_{k+1} = I_1 \oplus \cdots \oplus I_k \oplus I_{k+1}$ ми знову можемо застосувати нашу конструкцію. Оскільки алгебра $\mathcal{A}$ є скінченновимірною, то на якомусь кроці процес завершиться й одержимо розклад $A = I_1 \oplus \cdots \oplus I_m$ алгебри $\mathcal{A}$ в пряму суму мінімальних інваріантних підпросторів. □

Твердження 4.8. *Кожна проста алгебра має одиницю.*

Доведення. Нехай $\mathcal{A}$ — проста алгебра. Із доведення теореми 4.10 випливає, що $\mathcal{A}$ має ліву одиницю e. Розглянемо точне незвідне зображення $\varphi : \mathcal{A} \to \operatorname{End} V$ алгебри $\mathcal{A}$. Тоді для довільних $a \in \mathcal{A}$ і $\boldsymbol{v} \in V$ маємо:

$$\varphi_a(\varphi_e(\boldsymbol{v}) - \boldsymbol{v}) = \varphi_{ea}(\boldsymbol{v}) - \varphi_a(\boldsymbol{v}) = \varphi_{ea-a}(\boldsymbol{v}) = \varphi_0(\boldsymbol{v}) = \boldsymbol{0}.$$

Таким чином, множина $U = \{\varphi_e(\boldsymbol{v}) - \boldsymbol{v} \mid \boldsymbol{v} \in V\}$ є інваріантним підпростором, на якому алгебра $\mathcal{A}$ діє тривіально. Із незвідності зображення φ випливає, що $U = 0$. Але тоді φ_e є тотожним перетворенням простору і для довільного $a \in \mathcal{A}$ буде

$$\varphi_a = \varphi_a \varphi_e = \varphi_{ea} = \varphi_e \varphi_a = \varphi_{ae}.$$

Із точності зображення φ тепер випливає, що $a = ea = ae$. Отже, e є двосторонньою одиницею. □

Теорема 4.11. *Кожна скінченновимірна проста алгебра над полем $\mathbb{C}$ ізоморфна алгебрі всіх лінійних перетворень деякого скінченновимірного простору над $\mathbb{C}$.*

Доведення. Нехай $\varphi : \mathcal{A} \to \operatorname{End} V$ — деяке точне незвідне зображення простої комплексної алгебри $\mathcal{A}$. Розглянемо образ $\widetilde{\mathcal{A}} = \{\varphi_a \mid a \in \mathcal{A}\}$ алгебри $\mathcal{A}$ при цьому зображенні. Із незвідності зображення φ і леми Шура випливає, що комутатор

$$\widetilde{\mathcal{A}}' = \{\psi \in \operatorname{End} V \mid \psi\varphi_a = \varphi_a\psi \text{ для всіх } a \in \mathcal{A}\}$$

алгебри $\widetilde{\mathcal{A}}$ збігається з множиною всіх гомотетій $c\varepsilon : \boldsymbol{v} \mapsto c\boldsymbol{v}$ простору V. Позаяк гомотетії комутують з усіма перетвореннями, то другий комутатор

$$\widetilde{\mathcal{A}}'' = \{\mu \in \operatorname{End} V \mid \psi\mu = \mu\psi \text{ для всіх } \psi \in \widetilde{\mathcal{A}}'\}$$

збігається з $\operatorname{End} V$. Тому для доведення теореми досить показати, що $\widetilde{\mathcal{A}}''$ збігається з $\widetilde{\mathcal{A}}$.

Лема 4.7. *Нехай $\mathcal{A}$ — алгебра з одиницею e і $\mathcal{A}_r$ та $\mathcal{A}_l$ — образи $\mathcal{A}$ відповідно при правому $a \mapsto \lambda_a$ (де $\lambda_a : x \mapsto xa$) та лівому $a \mapsto {}_a\lambda$ (де ${}_a\lambda : x \mapsto ax$) регулярних зображеннях, а $\mathcal{A}'_r$ і $\mathcal{A}'_l$ — комутатори цих алгебр як підалгебр алгебри* $\operatorname{End}\mathcal{A}$. *Тоді $\mathcal{A}'_l = \mathcal{A}_r$ і $\mathcal{A}'_r = \mathcal{A}_l$.*

Доведення. Позаяк для довільних $a, b, x \in \mathcal{A}$ маємо

$$({}_a\lambda \cdot \lambda_b)(x) = (ax)b = a(xb) = (\lambda_b \cdot {}_a\lambda)(x)\,,$$

то $\mathcal{A}'_l \supseteq \mathcal{A}_r$ і $\mathcal{A}'_r \supseteq \mathcal{A}_l$. Доведемо тепер включення $\mathcal{A}'_l \subseteq \mathcal{A}_r$ (включення $\mathcal{A}'_r \subseteq \mathcal{A}_l$ доводиться аналогічно).

Розглянемо довільні $\psi \in \mathcal{A}'_l$ та $a, x \in \mathcal{A}$. Тоді

$$\psi(ax) = \psi({}_a\lambda(x)) = {}_a\lambda(\psi(x)) = a \cdot \psi(x).$$

Поклавши в цій рівності $x = e$, отримаємо $\psi(a) = a \cdot \psi(e)$. Оскільки елемент a довільний, то $\psi = \lambda_{\psi(e)}$. Отже, $\psi \in \mathcal{A}_r$ і $\mathcal{A}'_l \subseteq \mathcal{A}_r$. □

Виберемо в просторі V базу $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ і позначимо через T_a матрицю перетворення $\lambda_a : x \mapsto xa$ в цій базі. За теоремою 4.10 можна вважати, що праве регулярне зображення алгебри $\mathcal{A}$ є прямим кратним її зображення $\varphi : \mathcal{A} \to \operatorname{End} V$. Нехай $\mathcal{A} = I_1 \oplus \cdots \oplus I_m$ — розклад алгебри $\mathcal{A}$ в пряму суму мінімальних інваріантних підпросторів правого регулярного зображення. Тоді в кожному з підпросторів I_k, $1 \le k \le m$, можна вибрати таку базу $\boldsymbol{f}_1^{(k)}, \ldots, \boldsymbol{f}_n^{(k)}$, що перетворення $\lambda_a : x \mapsto xa$ матиме в базі

$$\boldsymbol{f}_1^{(1)},\ \boldsymbol{f}_2^{(1)},\ \ldots,\ \boldsymbol{f}_n^{(1)},\ \boldsymbol{f}_1^{(2)},\ \ldots,\ \boldsymbol{f}_n^{(m)} \tag{4.8}$$

матрицю

$$M_a = \begin{pmatrix} T_a & 0 & \cdots & 0 \\ 0 & T_a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & T_a \end{pmatrix}.$$

Легко бачити, що матриця

$$P = \begin{pmatrix} P_{11} & \cdots & P_{1m} \\ \vdots & \ddots & \vdots \\ P_{m1} & \dots & P_{mm} \end{pmatrix} \tag{4.9}$$

буде комутувати з матрицею M_a тоді й лише тоді, коли кожен блок P_{ij} буде комутувати з матрицею T_a. Тому P буде комутувати з усіма матрицями M_a (тобто перетворення з матрицею P буде належати $\mathcal{A}'_r$) тоді й лише тоді, коли кожен блок P_{ij} буде комутувати з усіма матрицями T_a.

Розглянемо тепер перетворення $\mu \in \widetilde{\mathcal{A}}''$. Нехай Q — його матриця в базі $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$. Якщо матриця (4.9) є матрицею перетворення з $\mathcal{A}'_r$, то Q буде комутувати з усіма її блоками P_{ij}. А тому матриця

$$Q^* = \begin{pmatrix} Q & 0 & \cdots & 0 \\ 0 & Q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & Q \end{pmatrix}$$

буде комутувати з P, тобто Q^* є матрицею в базі (4.8) деякого перетворення μ^* із другого комутатора $\mathcal{A}''_r$ алгебри $\mathcal{A}_r$. Позаяк за твердженням 4.8 алгебра $\mathcal{A}$ має одиницю, то з леми випливає, що $\mathcal{A}'_r = \mathcal{A}_l$ і $\mathcal{A}''_r = \mathcal{A}'_l = \mathcal{A}_r$. Тому μ^* збігається з λ_b для деякого $b \in \mathcal{A}$. Але тоді Q є матрицею (в базі $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$) перетворення φ_b для цього ж елемента b. Отже, $\mu = \varphi_b$.

Таким чином, $\widetilde{\mathcal{A}}'' \subseteq \widetilde{\mathcal{A}}$. Оскільки $\widetilde{\mathcal{A}} \subseteq \operatorname{End} V$, а $\widetilde{\mathcal{A}}'' = \operatorname{End} V$, то $\widetilde{\mathcal{A}} = \operatorname{End} V$, що завершує доведення. □

Позаяк алгебра всіх лінійних перетворень n-вимірного простору над $\mathbb{C}$ ізоморфна повній матричній алгебрі $M_n(\mathbb{C})$, то з теорем 4.7 і 4.11 одразу випливає такий

Наслідок 4.3. Комплексна скінченновимірна алгебра буде простою тоді й лише тоді, коли вона ізоморфна деякій повній матричній алгебрі $M_n(\mathbb{C})$.

Зауважимо, що в доведеннях теорем 4.9, 4.10, 4.11 і твердження 4.8 фактично використовувалась не простота алгебри $\mathcal{A}$, а лише той факт, що $\mathcal{A}$ мала точне незвідне зображення. Разом із теоремою 4.7 це одразу дає

Наслідок 4.4. *Кожна комплексна скінченновимірна алгебра, яка має точне незвідне зображення, є простою.*

Таким чином, у випадку поля $\mathbb{C}$ існування точного незвідного зображення є характеристичною властивістю простих алгебр.

Теорема 4.11 була доведена в кінці XIX ст. незалежно Моліним, Фробеніусом та Е.Картаном. У 1907 р. Веддербарн узагальнив її на скінченновимірні асоціативні алгебри над довільним полем.

Теорема 4.12 (Веддербарн)**.** *Кожна скінченновимірна асоціативна проста алгебра над полем P ізоморфна алгебрі всіх лінійних перетворень деякого скінченновимірного простору V над деяким тілом D. При цьому тіло D є скінченновимірною алгеброю над полем P і визначене з точністю до ізоморфізму, а розмірність простору V над D визначена однозначно.*

Позаяк єдиною скінченновимірною алгеброю з діленням над полем $\mathbb{C}$ є самé поле $\mathbb{C}$ (див. задачу 22), то теорема 4.11 є частковим випадком теореми Веддербарна.

4.6 Напівпрості алгебри

Означення 4.8. *Алгебра $\mathcal{A}$ називається* ***напівпростою****, якщо для кожного $0 \neq a \in \mathcal{A}$ існує таке незвідне зображення $\varphi : \mathcal{A} \to \operatorname{End} V$ алгебри $\mathcal{A}$, що $\varphi_a \neq 0$.*

Вправа 4.8. *Доведіть, що алгебра $\mathcal{A}$ буде напівпростою тоді й лише тоді, коли перетин усіх максимальних двосторонніх ідеалів буде нульовим.*

Очевидно, що кожна проста алгебра є напівпростою.

Твердження 4.9. *Пряма сума $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_k$ простих алгебр $\mathcal{A}_1$, $\ldots$, $\mathcal{A}_k$ є напівпростою алгеброю.*

Доведення. За теоремою 4.8 для кожної простої алгебри існує точне незвідне зображення. Нехай $\varphi^{(i)} : \mathcal{A}_i \to \operatorname{End} V_i$ — точне незвідне зображення алгебри $\mathcal{A}_i$, $i = 1, \ldots, k$. Розглянемо відображення

$$\widetilde{\varphi}^{(i)} : \mathcal{A} \to \operatorname{End} V_i\,, \quad (a_1, \ldots, a_k) \mapsto \varphi^{(i)}_{a_i} \quad (i = 1, \ldots, k)\,.$$

Очевидно, що кожне з відображень $\widetilde{\varphi}^{(i)}$ є зображенням алгебри $\mathcal{A}$, причому незвідним. Крім того, якщо $a = (a_1, \ldots, a_k) \neq 0$, то існує таке i, що $a_i \neq 0$. Але тоді $\widetilde{\varphi}^{(i)}(a) = \varphi^{(i)}_{a_i} \neq 0$. □

Виявляється, що з точністю до ізоморфізму алгебрами з твердження 4.9 вичерпуються всі напівпрості алгебрі. Доведення цього важливого факту і є метою цього розділу.

Ряд підалгебр

$$0 = \mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \cdots \subseteq \mathcal{A}_{n-1} \subseteq \mathcal{A}_n = \mathcal{A} \tag{4.10}$$

алгебри $\mathcal{A}$ називається *нормальним рядом* алгебри A, якщо для кожного $n > k \geq 0$ підалгебра $\mathcal{A}_k$ є двостороннім ідеалом підалгебри $\mathcal{A}_{k+1}$. Нормальний ряд, у якому для кожного $n > k \geq 0$ підалгебра $\mathcal{A}_k$ є максимальним двостороннім ідеалом підалгебри $\mathcal{A}_{k+1}$, називається *композиційним*. Зауважимо, що для композиційного ряду всі включення в (4.10) є строгими[14].

Елемент a називається *нільпотентним* (або *нільелементом*), якщо для деякого натурального k $a^k = 0$.

Твердження 4.10. *У напівпростій алгебрі $\mathcal{A}$ для кожного ненульового елемента a існує такий елемент b, що добуток ab не є нільелементом.*

Доведення. Якщо $a \neq 0$, то існує таке незвідне зображення $\varphi : \mathcal{A} \to \operatorname{End} V$, що $\varphi_a \neq 0$. Візьмемо вектор $\boldsymbol{v} \neq 0$, для якого $\varphi_a(\boldsymbol{v}) = \boldsymbol{u} \neq 0$. Позаяк $U = \{\varphi_a(\boldsymbol{u}) \mid a \in \mathcal{A}\}$ є інваріантним підпростором зображення φ, то $U = V$. Отже, існує такий елемент $b \in \mathcal{A}$, що $\varphi_b(\boldsymbol{u}) = \boldsymbol{v}$. Але тоді $\varphi_{ab}(\boldsymbol{v}) = \boldsymbol{v}$ і для довільного k $\varphi_{(ab)^k}(\boldsymbol{v}) = \boldsymbol{v}$. Тому $(ab)^k \neq 0$ для всіх k. □

Теорема 4.13. *Нормальний ряд напівпростої алгебри не містить ненульових тривіальних алгебр.*

Доведення. Нехай

$$0 = \mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \cdots \subseteq \mathcal{A}_{n-1} \subseteq \mathcal{A}_n = \mathcal{A}$$

— нормальний ряд напівпростої алгебри $\mathcal{A}$. Можна вважати, що $\mathcal{A}_1 \neq 0$, і досить показати, що алгебра $\mathcal{A}_1$ є нетривіальною. Нехай $a \in \mathcal{A}_1 \setminus \{0\}$,

[14] Очевидно, що в скінченновимірних алгебрах композиційні ряди існують завжди. Для нескінченновимірних алгебр це не так.

а елемент $b \in \mathcal{A}$ такий, що добуток ab не є нільелементом (такий b існує за твердженням 4.10). Позаяк a належить усім підалгебрам $\mathcal{A}_k$ $(k > 0)$ і $\mathcal{A}_k$ є ідеалом в $\mathcal{A}_{k+1}$, то для кожного $c \in \mathcal{A}_{k+1}$ елемент cac належить $\mathcal{A}_k$. Звідси одразу випливає, що

$$b \cdot a \cdot b \in \mathcal{A}_{n-1}, \quad (ba)^3 b = bab \cdot a \cdot bab \in \mathcal{A}_{n-2},$$
$$(ba)^7 b = (ba)^3 b \cdot a \cdot (ba)^3 b \in \mathcal{A}_{n-3}, \quad \ldots$$
$$\ldots, \quad (ba)^{2^{n-1}-1} b = (ba)^{2^{n-2}-1} b \cdot a \cdot (ba)^{2^{n-2}-1} b \in \mathcal{A}_1 .$$

Але $a \cdot (ba)^{2^{n-1}-1} b = (ab)^{2^{n-1}} \neq 0$. □

Наслідок 4.5. *Кожен ненульовий ідеал напівпростої алгебри $\mathcal{A}$ є нетривіальною алгеброю.*

Доведення. Це випливає з теореми 4.9 і того, що кожен ідеал I є членом нормального ряду $0 \subseteq I \subseteq \mathcal{A}$. □

Теорема 4.14. *Кожна напівпроста алгебра $\mathcal{A}$ містить одиницю і розкладається в пряму суму своїх двосторонніх ідеалів, кожен із яких є простою алгеброю.*

Для доведення теореми нам знадобляться дві леми.

Лема 4.8. *Якщо $0 \subset \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq A$ — нормальний ряд і підалгебра $\mathcal{A}_1$ є простою, то $\mathcal{A}_1$ є двостороннім ідеалом алгебри A.*

Доведення. Нехай e — одиниця алгебри $\mathcal{A}_1$ (вона існує за твердженням 4.8). Позаяк $e \in \mathcal{A}_2$, то $ae \in \mathcal{A}_2$ для довільного $a \in \mathcal{A}$. Тому для довільних $a \in \mathcal{A}$ і $b \in \mathcal{A}_1$ маємо: $a \cdot b = a \cdot eb = ae \cdot b \in \mathcal{A}_1$.

Включення $b \cdot a \in \mathcal{A}_1$ доводиться аналогічно. □

Лема 4.9. *Нехай алгебра $\mathcal{A}$ розкладається в пряму суму двох двосторонніх ідеалів: $\mathcal{A} = I \oplus J$. Якщо ідеал I — максимальний, то алгебра J не має нетривіальних двосторонніх ідеалів.*

Доведення. Нехай J_1 — нетривіальний двосторонній ідеал у J. Тоді $I + J_1$ буде двостороннім ідеалом алгебри $\mathcal{A}$, який задовольняє строгі включення $\mathcal{A} \supset I + J_1 \supset I$. Справді, для довільних $a + b \in I \oplus J$ та $a_1 + b_1 \in I + J_1$

$$(a + b)(a_1 + b_1) = (aa_1 + ab_1 + ba_1) + bb_1 \in I + J_1 ,$$

і, аналогічно, $(a_1 + b_1)(a + b) \in I + J_1$. А це суперечить максимальності ідеалу I. □

Доведення теореми 4.14. Нехай

$$0 = \mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{n-1} \subset \mathcal{A}_n = \mathcal{A}$$

— композиційний ряд алгебри $\mathcal{A}$. Індукцією за k доведемо, що для кожного k алгебра $\mathcal{A}_k$ містить одиницю й розкладається в пряму суму своїх двосторонніх ідеалів, кожен із яких є простою алгеброю (при $k = n$ це дасть твердження теореми).

За означенням композиційного ряду алгебра $\mathcal{A}_1$ не має власних двосторонніх ідеалів, а за теоремою 4.13 вона є нетривіальною. Отже, вона є простою і (як проста алгебра) містить одиницю. Це дає базу індукції.

Припустимо, що для деякого $k < n$ твердження вже доведене. Тоді підалгебра $\mathcal{A}_k$ містить одиницю. За твердженням 4.2 існує такий двосторонній ідеал J алгебри $\mathcal{A}_{k+1}$, що $\mathcal{A}_{k+1} = \mathcal{A}_k \oplus J$. Позаяк $\mathcal{A}_k$ є максимальним ідеалом в $\mathcal{A}_{k+1}$, то за лемою 4.9 алгебра J не має нетривіальних двосторонніх ідеалів. З іншого боку, алгебра J є членом нормального ряду $0 \subset J \subseteq \mathcal{A}_{k+1} \subseteq \mathcal{A}$, а тому за теоремою 4.13 є нетривіальною. Отже, алгебра J є простою.

За припущенням індукції алгебра $\mathcal{A}_k$ розкладається в пряму суму $\mathcal{A}_k = \bigoplus\limits_m J_m$ своїх двосторонніх ідеалів, кожен із яких є простою алгеброю. Із нормальності ряду $0 \subset J_m \subseteq \mathcal{A}_k \subseteq \mathcal{A}_{k+1}$ і леми 4.8 випливає, що кожна підалгебра J_m буде ідеалом і в $\mathcal{A}_{k+1}$. Це одразу дає й розклад алгебри $\mathcal{A}_{k+1}$ у пряму суму $\mathcal{A}_{k+1} = J \oplus \bigoplus\limits_m J_m$ своїх двосторонніх ідеалів, кожен із яких є простою алгеброю.

Нарешті, із твердження 4.1 і того, що проста алгебра має одиницю, випливає наявність одиниці і в алгебрі $\mathcal{A}_{k+1}$. Це завершує доведення індукційного кроку. □

Із теореми 4.14 і твердження 4.9 одержуємо такий

Наслідок 4.6. *Алгебра буде напівпростою тоді й лише тоді, коли вона розкладається в пряму суму простих алгебр.*

У випадку комплексних алгебр, враховуючи теорему 4.11, наслідок 4.6 можна уточнити.

Наслідок 4.7. *Комплексна алгебра буде напівпростою тоді й лише тоді, коли вона ізоморфна деякій алгебрі вигляду* $M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$.

4.7 Задачі

1. а) Доведіть, що множина 2^M всіх підмножин фіксованої множини M є комутативним асоціативним кільцем з одиницею, якщо за додавання

взяти симетричну різницю $A \triangle B := (A \setminus B) \cup (B \setminus A)$ підмножин, а за множення — перетин підмножин.

b) Доведіть, що кільце 2^M можна перетворити в алгебру над полем $\mathbb{Z}_2$, якщо множення на скаляри визначити правилом $0 \cdot A = \varnothing$, $1 \cdot A = A$.

2. Доведіть, що алгебру матриць можна задавати в базі з матричних "одиничок" e_{ij} таким правилом множення: $e_{ij} \cdot e_{kl} = \delta_{jk} e_{il}$.

3. Доведіть, що алгебра $P[x]$ многочленів ізоморфна напівгруповій алгебрі $P[S]$ вільного моноїда $S = \{x\}^*$.

4. Доведіть, що в алгебрі $P[[x]]$ формальних степеневих рядів від змінної x елемент буде оборотним тоді й лише тоді, коли його вільний член не дорівнює 0.

5. Які серед наступних $\mathbb{C}$-алгебр будуть ізоморфними: $\mathcal{A}_1 = \mathbb{C} \oplus \mathbb{C}$, $\mathcal{A}_2 = \mathbb{C}[x]$, $\mathcal{A}_3 = \mathbb{C}[x, y]$, $\mathcal{A}_4 = \mathbb{C}[x]/\langle x^2 \rangle$, $\mathcal{A}_5 = \mathbb{C}[x]/\langle (x-1)^2 \rangle$, $\mathcal{A}_6 = \mathbb{C}[x]/\langle x^2 - 1 \rangle$, $\mathcal{A}_7 = \mathbb{C}[x, y]/\langle x^2 - y^2 \rangle$, $\mathcal{A}_8 = \mathbb{C}[x, y]/\langle (x-y)^2 \rangle$?

6. Доведіть, що для кожної комутативної скінченнопородженої P-алгебри $\mathcal{A}$ існує таке натуральне число n, що $\mathcal{A}$ ізоморфна деякій факторалгебрі алгебри $P[x_1, \ldots, x_n]$.

7. Доведіть, що скінченновимірна лінійна (не обов'язково асоціативна) буде алгеброю з діленням тоді й лише тоді, коли вона не містить дільників нуля.

8. Доведіть, що в скінченновимірній асоціативній алгебрі з одиницею кожен елемент, який не є дільником нуля, є оборотним.

9. Доведіть, що нетривіальна асоціативна алгебра буде тілом тоді й лише тоді, коли вона не має нетривіальних односторонніх ідеалів.

10. Нехай $\mathcal{A}$ — n-вимірна асоціативна алгебра з одиницею й мінімальний многочлен елемента a має степінь n. Доведіть, що елемент a породжує алгебру $\mathcal{A}$.

11. Доведіть, що кожне тіло є алгеброю або над полем $\mathbb{Q}$, або над деяким полем лишків $\mathbb{Z}_p$.

12. Нехай D — тіло, $K = Z(D)$ і $[D : K] < \infty$. Доведіть, що для кожного максимального підполя $P \subseteq D$ виконується рівність $[D : K] = [D : P]^2$.

13. Нехай P — алгебрично замкнене поле, а скінченновимірна P-алгебра $\mathcal{A}$ є тілом. Доведіть, що $\mathcal{A} = P$.

14. Чи буде алгебра кватерніонів груповою алгеброю групи кватерніонів Q_8?

15. Чи буде тіло кватерніонів алгеброю над полем комплексних чисел при природному зануренні $\mathbb{C}$ в $\mathbb{H}$?

16. Доведіть, що відображення $1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\boldsymbol{i} \mapsto \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $\boldsymbol{j} \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\boldsymbol{k} \mapsto \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$ індукує мономорфізм $\mathbb{R}$-алгебри $\mathbb{H}$ у $\mathbb{R}$-алгебру $M_2(\mathbb{C})$.

17. Доведіть, що в алгебрі кватерніонів перетворення $\psi : x \mapsto \overline{x}$ є інволютивним антиавтоморфізмом (тобто $\psi^2 = \mathrm{id}$, $\psi(x+y) = \psi(x) + \psi(y)$ і $\psi(xy) = \psi(y)\psi(x)$), який комутує з кожним автоморфізмом вигляду $\varphi_a : x \mapsto a^{-1}xa$.

18. Доведіть, що для кожного кватерніона z існує єдиний розклад вигляду $z = z_1 + z_2$, де $z_1^2, z_2^2 \in \mathbb{R}$ і $z_1^2 \geq 0$, $z_2^2 \leq 0$.

19. Доведіть, що чисто уявні кватерніони u і v антикомутують (тобто $uv = -vu$) тоді й лише тоді, коли u і v ортогональні як вектори.

20. Доведіть, що в тілі кватерніонів рівняння $x^2 = 1$ має лише 2 роз'язки, а рівняння $x^3 = 1$ — нескінченно багато.

21. Доведіть, що для кватерніонів виконується аналог формули Муавра: якщо $z = r(\cos\varphi + \boldsymbol{v} \cdot \sin\varphi)$, то $z^n = r^n(\cos n\varphi + \boldsymbol{v} \cdot \sin n\varphi)$.

22. Доведіть, що з точністю до ізоморфізму існує тільки одна скінченновимірна комплексна алгебра з діленням — поле $\mathbb{C}$.

23. Нехай P — довільне поле, $a, b \in P^*$. Через $\mathbb{H}(a,b)$ позначимо P-алгебру з одиницею 1 і базою 1, $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$, де $\boldsymbol{u}^2 = a$, $\boldsymbol{v}^2 = b$, $\boldsymbol{w}^2 = -ab$, $\boldsymbol{uv} = -\boldsymbol{vu} = \boldsymbol{w}$, $\boldsymbol{vw} = -\boldsymbol{wv} = -b\boldsymbol{u}$, $\boldsymbol{wu} = -\boldsymbol{uw} = -a\boldsymbol{v}$. Доведіть, що

    a) алгебра $\mathbb{H}(a,b)$ є асоціативною;

    b) алгебра $\mathbb{H}(a,b)$ буде тілом тоді й лише тоді, коли для довільних x_0, x_1, x_2, x_3 із P з рівності $x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = 0$ випливає рівність $x_0 = x_1 = x_2 = x_3 = 0$.

24. Доведіть, що кожен елемент алгебри $\mathbb{H}(a,b)$ із задачі 23 є коренем деякого квадратного тричлена з $P[x]$.

25. Нехай $\mathcal{A}$ — 4-вимірна алгебра над $\mathbb{Q}$ з одиницею 1 і базою 1, $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$, причому $\boldsymbol{u}^2 = -1$, $\boldsymbol{v}^2 = 2$, $\boldsymbol{w}^2 = 2$, $\boldsymbol{uv} = -\boldsymbol{vu} = \boldsymbol{w}$, $\boldsymbol{vw} = -\boldsymbol{wv} = -2\boldsymbol{u}$, $\boldsymbol{wu} = -\boldsymbol{uw} = \boldsymbol{v}$. Доведіть, що $\mathcal{A}$ — тіло і що $\mathbb{Q}(\boldsymbol{u})$ та $\mathbb{Q}(\boldsymbol{v})$ — неізоморфні максимальні підполя цього тіла.

26. Нехай $\mathcal{A}$ — 4-вимірна алгебра над $\mathbb{C}$ з одиницею 1, базою 1, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ і такою самою таблицею множення, як в алгебрі кватерніонів. Доведіть, що $\mathcal{A}$ ізоморфна алгебрі $M_2(\mathbb{C})$.

27. Побудуйте для алгебри октав Келі таблицю множення в базі 1, $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$, $\boldsymbol{e}$, $\boldsymbol{ie}$, $\boldsymbol{je}$, $\boldsymbol{ke}$.

28. Нормою $N(\boldsymbol{z})$ октави $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{ye}$ називається сума $N(\boldsymbol{x}) + N(\boldsymbol{y})$ норм кватерніонів $\boldsymbol{x}$ і $\boldsymbol{y}$. Доведіть, що $N(\boldsymbol{z}) = (\boldsymbol{x} + \boldsymbol{ye})(\overline{\boldsymbol{x}} - \boldsymbol{ye})$ і що $N(\boldsymbol{zu}) = N(\boldsymbol{z})N(\boldsymbol{u})$.

29. Доведіть, що алгебра октав Келі не містить дільників нуля.

30. Доведіть, що алгебра октав є *альтернативною*, тобто що для довільних октав $\boldsymbol{v}$ і $\boldsymbol{u}$ виконуються рівності $(\boldsymbol{vv})\boldsymbol{u} = \boldsymbol{v}(\boldsymbol{vu})$ і $(\boldsymbol{vu})\boldsymbol{u} = \boldsymbol{v}(\boldsymbol{uu})$.

31. Доведіть, що над полем кожна двовимірна лінійна алгебра з одиницею буде комутативною й асоціативною.

32. Доведіть, що над полем $\mathbb{R}$ кожна 2-вимірна лінійна алгебра з одиницею ізоморфна одній з таких алгебр: 1) $\mathbb{C}$; 2) $\langle 1, b\rangle$, $b^2 = 1$ (так звані *подвійні* числа); 3) $\langle 1, b\rangle$, $b^2 = 0$ (так звані *дуальні* числа).

33. Опишіть із точністю до ізоморфізму всі двовимірні лінійні алгебри з одиницею над полем $\mathbb{C}$.

34. Доведіть, що існує нескінченно багато попарно неізоморфних 2-вимірних лінійних алгебр з одиницею над полем $\mathbb{Q}$.

35. Доведіть, що лінійна алгебра $L = \langle a, b : a^2 = b^2 = a, ab = -ba = b\rangle$ над $\mathbb{R}$ є неасоціативною алгеброю з діленням, але без одиниці.

36. Нехай група H ізоморфна деякій факторгрупі групи G. Доведіть, що групова алгебра $P[H]$ ізоморфна деякій факторалгебрі групової алгебри $P[G]$.

37. Доведіть, що коли група G містить неодиничні елементи скінченного порядку, то групова алгебра $P[G]$ містить дільники нуля.

38.* Доведіть, що коли групова алгебра $\mathbb{C}[G]$ скінченної групи G не містить нільпотентних елементів, то група G — абелева.

39.* Доведіть, що коли скінченні абелеві групи G і H мають однаковий порядок, то їх групові алгебри $\mathbb{C}[G]$ і $\mathbb{C}[H]$ — ізоморфні.

40. Знайдіть розмірність центру групової алгебри: a) $\mathbb{C}[S_3]$; b) $\mathbb{C}[Q_8]$; c) $\mathbb{C}[A_4]$.

41. Доведіть, що групові алгебри $\mathbb{C}[D_4]$ і $\mathbb{C}[Q_8]$ — ізоморфні.

42. Для яких скінченних груп G групова алгебра $\mathbb{C}[G]$ буде простою?

43. Знайдіть усі власні ідеали: a) алгебри дуальних чисел (див. задачу 32); b) алгебри подвійних чисел (див. задачу 32).

44. Знайдіть усі ліві ідеали алгебри $M_2(\mathbb{Z}_2)$.

45. Нехай P — поле. Знайдіть усі ідеали алгебри $P \oplus \cdots \oplus P$ (n доданків) і підрахуйте їх кількість.

46. Доведіть, що в таких алгебрах усі двосторонні ідеали є головними:
a) алгебра $P[[x]]$ формальних степеневих рядів від змінної x;
b) * групова алгебра $\mathbb{C}[\mathbb{Z}]$.

47. Підрахуйте кількість двосторонніх ідеалів у груповій алгебрі: a) $\mathbb{C}[S_3]$; b) $\mathbb{C}[Q_8]$.

48. Доведіть, що центр повної матричної алгебри $M_n(P)$ збігається з множиною скалярних матриць.

49. Нехай U — фіксований підпростір простору P^n. Доведіть, що
a) множина $I_U^l = \{\varphi \in \operatorname{End} P^n \mid \operatorname{Im}\varphi \subseteq U\}$ буде лівим ідеалом алгебри $\operatorname{End} P^n$ і кожен лівий ідеал алгебри $\operatorname{End} P^n$ має такий вигляд;
b) множина $I_U^r = \{\varphi \in \operatorname{End} P^n \mid \operatorname{Ker}\varphi \supseteq U\}$ буде правим ідеалом алгебри $\operatorname{End} P^n$ і кожен правий ідеал алгебри $\operatorname{End} P^n$ має такий вигляд.

50. Нехай I_U^l та I_U^r — такі, як в задачі 49. Доведіть, що: a) $I_U^l \subseteq I_W^l$ тоді й лише тоді, коли $U \subseteq W$; b) $I_U^r \subseteq I_W^r$ тоді й лише тоді, коли $U \supseteq W$.

51. Опишіть максимальні й мінімальні односторонні ідеали алгебри $\operatorname{End} P^n$.

52. Нехай U — фіксований підпростір простору P^n. Доведіть, що

    a) Множина $I_U^l = \{A \in M_n(P) \mid Ax = 0$ для всіх векторів-стовпців $x \in U\}$ буде лівим ідеалом алгебри $M_n(P)$ і всі ліві ідеали з $M_n(P)$ мають такий вигляд.

    b) Множина $I_U^r = \{A \in M_n(P) \mid xA = 0$ для всіх векторів-рядків $x \in U\}$ буде правим ідеалом алгебри $M_n(P)$ і всі праві ідеали з $M_n(P)$ мають такий вигляд.

53. Опишіть із точністю до ізоморфізму всі комплексні комутативні напівпрості алгебри.

54. Нехай V — векторний простір над полем $\mathbb{C}$. Опишіть усі комутативні напівпрості підалгебри алгебри $\operatorname{End} V$.

55. Нехай для алгебри $\mathcal{A}$ лінійних перетворень простору $\mathbb{C}^n$ можна визначити на $\mathbb{C}^n$ скалярний добуток таким чином, щоб $\mathcal{A}$ була замкненою відносно взяття спряженого перетворення. Доведіть, що алгебра $\mathcal{A}$ є напівпростою.

56. Опишіть усі напівпрості підалгебри матричної алгебри $M_n(\mathbb{C})$.

57. Нехай $\varphi : \mathcal{A} \to \operatorname{End} V$ — зображення алгебри $\mathcal{A}$, а $V_1, \ldots, V_n$ — такий набір мінімальних інваріантних підпросторів цього зображення, що $V = V_1 + \cdots + V_n$. Доведіть, що V є прямою сумою якихось підпросторів із цього набору.

58. Доведіть, що підмножина I алгебри $\mathcal{A} = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$ буде двостороннім ідеалом тоді й лише тоді, коли вона є сумою певної кількості прямих доданків $M_{n_1}(\mathbb{C}) \ldots, M_{n_k}(\mathbb{C})$ алгебри A.

5 Многовиди

5.1 Означення та приклади

Нехай Ω — деяка сигнатура, а $\{x_1, x_2, \ldots, x_n, \ldots, \}$ — зліченний алфавіт, елементи якого назвемо *змінними*. *Ω-тотожністю* називається формальна рівність $u = v$, де u і v — два якихось Ω-терми над алфавітом змінних.

Нехай $x_{i_1}, \ldots, x_{i_n}$ — список усіх змінних, які зустрічаються в термах u або v. Кажуть, що тотожність $u(x_{i_1}, \ldots, x_{i_n}) = v(x_{i_1}, \ldots, x_{i_n})$ виконується в універсальній алгебрі $\langle A; \Omega\rangle$, якщо $u(a_1, \ldots, a_n) = v(a_1, \ldots, a_n)$ для довільних елементів $a_1, \ldots, a_n \in A$.

Означення 5.1. *Клас (Ω, Λ) всіх алгебр сигнатури Ω, в яких виконуються всі тотожності з даної множини Λ Ω-тотожностей, називається* ***многовидом*** *алгебр сигнатури Ω, що визначається тотожностями Λ.*

Зауважимо, що многовид (Ω, Λ) завжди непорожній, бо містить, зокрема, усі одноелементні алгебри сигнатури Ω.

Множину Λ Ω-тотожностей, якою задається даний многовид (Ω, Λ), часто зручно вважати *симетризованою* (тобто якщо Λ містить рівність $u = v$, то містить і рівність $v = u$).

Для довільної сигнатури Ω многовидами будуть клас усіх алгебр цієї сигнатури (він визначається порожньою множиною тотожностей; можна також взяти тотожність $x = x$) і клас одноелементних алгебр сигнатури Ω (так званий *абсолютно вироджений* многовид; він визначається тотожністю $x = y$). Крім того, перетин довільної родини також є многовидом:

$$\bigcap_{i\in I}(\Omega, \Lambda_i) = (\Omega, \bigcup_i \Lambda_i)\,. \tag{5.1}$$

Твердження 5.1. *Для кожного класу $\mathfrak{K}$ алгебр сигнатури Ω існує найменший многовид $\mathfrak{M}$, який містить $\mathfrak{K}$.*

Доведення. Множина многовидів, які містять клас $\mathfrak{K}$, не є порожньою: туди потрапляє многовид усіх алгебр сигнатури Ω. Крім того, перетин многовидів є многовидом. Тому найменшим многовидом, який містить $\mathfrak{K}$, буде перетин усіх многовидів, які містять $\mathfrak{K}$. □

Твердження 5.2. *Якщо многовид (Ω, Λ) містить алгебру $\mathcal{A}$, то він містить і всі підалгебри та гомоморфні образи алгебри $\mathcal{A}$.*

Доведення. Перше твердження випливає з того, що коли рівність $u = v$ виконується для всіх елементів алгебри $\mathcal{A}$, то вона тим більше виконується для всіх елементів її підалгебри.

Нехай тепер $\varphi : \mathcal{A} \to \mathcal{B}$ — епіморфізм, $u = v$ — Ω-тотожність із Λ, а $x_1, \ldots, x_n$ — список усіх змінних, які в ній зустрічаються. Візьмемо в $\mathcal{B}$ довільні елементи $b_1, \ldots, b_n$ і для кожного b_i виберемо якийсь його прообраз в $\mathcal{A}$ (тобто такий елемент $a_i \in \mathcal{A}$, що $\varphi(a_i) = b_i$). Тоді

$$u(b_1, \ldots, b_n) = u(\varphi(a_1), \ldots, \varphi(a_n)) = \varphi(u(a_1, \ldots, a_n)), \tag{5.2}$$

$$v(b_1, \ldots, b_n) = v(\varphi(a_1), \ldots, \varphi(a_n)) = \varphi(v(a_1, \ldots, a_n)). \tag{5.3}$$

А позаяк праві частини рівностей (5.2) і (5.3) збігаються, то ліві також збігаються. □

Із цього твердження одразу випливає, що довільний многовид (Ω, Λ) є абстрактним класом алгебр, бо разом із кожною алгеброю містить і всі алгебри, їй ізоморфні.

Вправа 5.1. *Доведіть, що коли кожна з алгебр $\mathcal{A}_i$, $i \in I$, належить многовиду (Ω, Λ), то прямий добуток $\prod\limits_{i \in I} \mathcal{A}_i$ також належить цьому многовиду.*

Нехай $\mathcal{A}$ — алгебра сигнатури Ω. Для довільної непорожньої множини M множина $\mathrm{Map}(M, A)$ всіх відображень $\varphi : M \to A$ перетворюється в алгебру сигнатури Ω, якщо для кожної n-арної операції $\omega \in \Omega$ ($n \geq 0$) покласти

$$\omega(\varphi_1, \ldots, \varphi_n)(x) := \omega(\varphi_1(x), \ldots, \varphi_n(x)) \tag{5.4}$$

(тобто операції з Ω визначаються на $\mathrm{Map}(M, A)$ поточково). Легко бачити, що $\mathrm{Map}(M, A) \simeq \prod_{m \in M} \mathcal{A}$. Тому з вправи 5.1 і твердження 5.2 одразу випливає, що кожен многовид, який містить алгебру $\mathcal{A}$, містить і алгебру $\mathrm{Map}(M, A)$.

Приклади многовидів:

1. У класі алгебр, сигнатура яких містить єдину (бінарну) операцію $\cdot$, многовид напівгруп визначається тотожністю $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

2. У класі алгебр сигнатури $(\cdot, 1)$ моноїди утворюють многовид, визначений тотожностями $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot 1 = x$, $1 \cdot x = x$.

3. Якщо групу розглядати як алгебру сигнатури $(\cdot, ^{-1}, 1)$, то клас груп є многовидом, визначеним тотожностями

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad x \cdot x^{-1} = 1, \quad x \cdot 1 = x. \tag{5.5}$$

Зауважимо, що клас груп не є ні многовидом напівгруп, ні многовидом моноїдів.

4. Якщо до тотожностей (5.5) долучити $x \cdot y = y \cdot x$, отримаємо многовид абелевих груп.

5. У класі алгебр сигнатури $(+, -, 0, \cdot)$ тотожності

$$(x+y)+z = x+(y+z), \quad x+(-x) = 0, \quad x+0 = x, \quad x+y = y+x,$$
$$x \cdot (y+z) = x \cdot z + y \cdot z, \quad (y+z) \cdot x = y \cdot x + z \cdot x$$

визначають многовид кілець. Якщо долучити до цих тотожностей ще $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, то отримаємо многовид асоціативних кілець.

6. У класі алгебр сигнатури $(\vee, \wedge)$ шість тотожностей

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a, \quad a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a,$$
$$a \vee (b \vee c) = (a \vee b) \vee c, \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

визначають многовид решіток.

7. Якщо до тотожностей із попереднього прикладу долучити якусь із тотожностей $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ чи $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, то отримаємо многовид дистрибутивних решіток.

Ми вже бачили на прикладі груп, що відповідь на питання, чи утворює даний клас алгебр многовид, залежить і від вибору сигнатури. На багатьох алгебрах можна природно визначити деякі додаткові операції, що дозволяє розширити сигнатуру, а за рахунок цього — і набір потенційних тотожностей. Ми розглянемо два приклади, коли розширення сигнатури дозволяє перетворити даний клас алгебр у многовид: регулярні та інверсні напівгрупи.

На кожній регулярній напівгрупі можна визначити (взагалі кажучи, багатьма способами) унарну операцію $x \mapsto x^*$, яка кожному елементу ставить у відповідність який-небудь інверсний до нього елемент. Тоді *клас регулярних напівгруп є многовидом алгебр сигнатури* $(\cdot, ^*)$, *визначеним тотожностями*

$$x(yz) = (xy)z, \quad xx^*x = x, \quad x^*xx^* = x^*.$$

Теорема 5.1 (Шайн)**.** *Нехай у напівгрупі S додатково визначена унарна дія a^{-1}, яка задовольняє тотожності*

$$(i)\ (a^{-1})^{-1} = a, \quad (ii)\ (ab)^{-1} = b^{-1}a^{-1},$$
$$(iii)\ \ aa^{-1} \cdot bb^{-1} = bb^{-1} \cdot aa^{-1}, \quad (iv)\ \ aa^{-1}a = a.$$

Тоді S — інверсна напівгрупа.

Доведення. Із (iv) одразу випливає, що напівгрупа S є регулярною. Припустимо тепер, що елемент e є ідемпотентом, тобто $ee = e$. Застосовуючи послідовно (iv), рівність $ee = e$, (ii), (i), (iii), (i), знову рівність $ee = e$, (i), (iv), отримуємо:

$$e = ee^{-1}e = e(ee)^{-1}e = ee^{-1}e^{-1}e = ee^{-1} \cdot e^{-1}(e^{-1})^{-1} =$$
$$= e^{-1}(e^{-1})^{-1} \cdot ee^{-1} = e^{-1}eee^{-1} = e^{-1}ee^{-1} = e^{-1}(e^{-1})^{-1}e^{-1} = e^{-1}.$$

Отже, кожний ідемпотент із S має вигляд $e = ee = ee^{-1}$. Але тоді з (iii) та критерію інверсності (теорема 2.14) випливає, що напівгрупа S є інверсною. □

Наслідок 5.1. *Інверсні напівгрупи утворюють многовид алгебр сигнатури* $(\cdot, {}^{-1})$.

Доведення. Якщо в інверсній напівгрупі через $^{-1}$ позначити операцію взяття інверсного елемента, то всі тотожності з теореми Шайна виконуються. Тому многовид, породжений тотожностями (i)–(iv) і $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, містить усі інверсні напівгрупи. Із другого боку, з теореми Шайна випливає, що нічого іншого він не містить. □

Теорема 5.2. *Гомоморфний образ інверсної напівгрупи також є інверсною напівгрупою.*

Доведення. Нехай S — інверсна напівгрупа і $\varphi : S \to T$ — епіморфізм напівгруп. Покажемо, що коли $\varphi(a_1) = \varphi(a_2)$, то образи інверсних елементів a_1^{-1} і a_2^{-1} також збігаються. Справді, в інверсній напівгрупі елементи $a_1^{-1}a_1$ $a_1a_1^{-1}$ $a_2^{-1}a_2$ і $a_2a_2^{-1}$ є ідемпотентами, а тому вони комутують (теорема 2.14). Тоді

$$\varphi(a_1^{-1}a_2) = \varphi(a_1^{-1}a_2a_2^{-1}a_2) = \varphi(a_1^{-1}a_1a_2^{-1}a_2) =$$
$$= \varphi(a_2^{-1}a_2a_1^{-1}a_1) = \varphi(a_2^{-1}a_1a_1^{-1}a_1) = \varphi(a_2^{-1}a_1).$$

Аналогічно показується, що $\varphi(a_2a_1^{-1}) = \varphi(a_1a_2^{-1})$. Звідси отримуємо:

$$\varphi(a_1^{-1}) = \varphi(a_1^{-1}a_1a_1^{-1}) = \varphi(a_1^{-1}a_2a_1^{-1}) = \varphi(a_2^{-1}a_1a_1^{-1}) =$$
$$= \varphi(a_2^{-1}a_2a_1^{-1}) = \varphi(a_2^{-1}a_1a_2^{-1}) = \varphi(a_2^{-1}a_2a_2^{-1}) = \varphi(a_2^{-1}).$$

Це дозволяє визначити на T унарну операцію $^{-1}$, якщо для кожного $b \in T$ взяти в S довільний прообраз a і покласти $b^{-1} = \varphi(a)^{-1}$. Тобто $\varphi(a)^{-1} = \varphi(a)^{-1}$. Отже, при такому визначенні операції $^{-1}$ на T відображення φ стає гомоморфізмом алгебр сигнатури $(\cdot, {}^{-1})$.

Позаяк інверсні напівгрупи як алгебри сигнатури $(\cdot,^{-1})$ утворюють многовид, а за твердженням 5.2 многовид замкнений відносно гомоморфних образів, то напівгрупа T також буде інверсною. $\square$

Зауваження. Безпосередньо з твердження 5.2 теорема 5.2 не випливає: інверсні напівгрупи утворюють не многовид напівгруп, а многовид алгебр сигнатури $(\cdot,^{-1})$. Саме з цієї причини піднапівгрупа інверсної напівгрупи не зобов'язана бути інверсною: вона може бути не замкненою відносно операції $^{-1}$. Зокрема, не будуть інверсними всі циклічні піднапівгрупи, породжені негруповими елементами.

5.2 Вільні алгебри многовидів

Нехай $\mathfrak{M}$ — непорожній клас універсальних алгебр даної сигнатури Ω. Алгебра $F \in \mathfrak{M}$ називається *вільною алгеброю* класу $\mathfrak{M}$ із вільною системою твірних X, якщо існує відображення $\mu : X \to F$, яке задовольняє такі дві умови:

1) алгебра F породжується множиною $\mu(X)$;

2) (*властивість універсальності*) для довільних алгебри $A \in \mathfrak{M}$ та відображення $\nu : X \to A$ існує такий гомоморфізм $\varphi : F \to A$, що $\mu \circ \varphi = \nu$.

Приклад. Із теореми 1.1 випливає, що в класі всіх алгебр даної сигнатури Ω алгебра термів $F(\Omega, X)$ є вільною.

Хоча в загальному випадку й не вимагається, щоб відображення $\mu : X \to F$ було ін'єктивним, зазвичай буде саме так:

Твердження 5.3. *Якщо F — вільна алгебра класу $\mathfrak{M}$, який містить не тільки одноелементні алгебри, то відображення $\mu : X \to F$ є ін'єктивним.*

Доведення. Нехай a, b — різні елементи алгебри $A \in \mathfrak{M}$, x, y — різні елементи множини X. Розглянемо довільне відображення $\nu : X \to A$, для якого $\nu(x) = a$, $\nu(y) = b$. Тоді з рівностей $(\mu\circ\varphi)(x) = a$ і $(\mu\circ\varphi)(y) = b$ випливає, що $\mu(x) \neq \mu(y)$. $\square$

Теорема 5.3. *Якщо непорожній клас $\mathfrak{M}$ універсальних алгебр даної сигнатури Ω замкнений відносно взяття підалгебр і прямих добутків, то для довільної непорожньої множини X клас $\mathfrak{M}$ містить вільну алгебру з вільною системою твірних X.*

Доведення. Обмежимося лише випадком, коли множина X і сигнатура Ω не більше ніж зліченні. Нехай M — множина всіх попарно неізоморфних алгебр із $\mathfrak{M}$ не більше ніж зліченної потужності. Розглянемо прямий добуток

$$B = \prod_{(A,\alpha_A)} A\,,$$

де A пробігає всі алгебри з M, а α_A — всі відображення вигляду $\alpha_A : X \to A$. Розглянемо також відображення

$$\mu : X \to B, \qquad x \mapsto \big(\alpha_A(x)\big)_{(A,\alpha_A)}\,,$$

і алгебру $F(X)$, породжену образом $\mu(X)$ цього відображення.

Очевидно, що $F(X)$ належить класу $\mathfrak{M}$ і задовольняє умову 1) з означення вільної алгебри. Перевіримо виконання умови 2). Нехай $A' \in \mathfrak{M}$ і $\nu : X \to A'$ — довільне відображення. Оскільки множина $\nu(X)$ і сигнатура Ω не більше ніж зліченні, то множина $\nu(X)$ породжує в A' підалгебру A, потужність якої не більше ніж зліченна. Тому можна вважати, що $A \in M$ і що відображення $\nu : X \to A'$ збігається з деяким α_A. Тоді для гомоморфізму $\varphi : F(X) \to A'$, індукованого канонічним епіморфізмом прямого добутку B на множник з індексом (A, α_A), для всіх $x \in X$ маємо:

$$(\mu \circ \varphi)(x) = \varphi(\mu(x)) = \varphi\big((\alpha_A(x))_{(A,\alpha_A)}\big) = \alpha_A(x) = \nu(x).$$

Отже $\mu \circ \varphi = \nu$. □

Теорема 5.4 (Біркгоф)**.** *Непорожній клас $\mathfrak{M}$ універсальних алгебр даної сигнатури Ω буде многовидом тоді й тільки тоді, коли він замкнений відносно взяття підалгебр, гомоморфних образів і прямих добутків.*

Доведення. Необхідність цих умов випливає з твердження 5.2 і вправи 5.1.

Достатність. Це очевидно, якщо клас $\mathfrak{M}$ містить лише одноелементні алгебри (можна взяти тотожність $x = y$). Тому далі вважатимемо, що $\mathfrak{M}$ містить не тільки одноелементні алгебри. За теоремою 5.3 клас $\mathfrak{M}$ містить вільну алгебру $F_{\mathfrak{M}}(X)$ зі зліченною множиною твірних $X = \{x_1, x_2, \ldots\}$, причому на підставі твердження 5.3 можна вважати, що $X \subseteq F_{\mathfrak{M}}(X)$. Нехай $F(\Omega, X)$ — вільна алгебра сигнатури Ω. Тоді тотожне відображення $\mathrm{id} : X \to X$ індукує гомоморфізм $\varphi : F(\Omega, X) \to F_{\mathfrak{M}}(X)$. Нехай $\mathfrak{R}$ — многовид алгебр сигнатури Ω, визначений системою тотожностей $\Sigma = \{u = v \mid \varphi(u) = \varphi(v)\}$. Доведемо, що $\mathfrak{M} = \mathfrak{R}$.

Нехай $u(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)$ — тотожність із Σ, $A \in \mathfrak{M}$ і $a_1, \ldots, a_n$ — довільні елементи з A. Існує такий гомоморфізм $\psi : F_{\mathfrak{M}}(X) \to A$, що $\psi(x_1) = a_1, \ldots, \psi(x_n) = a_n$. Тоді

$$u(a_1, \ldots, a_n) = u\big(\psi(x_1), \ldots, \psi(x_n)\big) = \psi(u(x_1, \ldots, x_n)) =$$
$$= \psi(v(x_1, \ldots, x_n)) = v\big(\psi(x_1), \ldots, \psi(x_n)\big) = v(a_1, \ldots, a_n).$$

Отже, $A \in \mathfrak{R}$ і $\mathfrak{M} \subseteq \mathfrak{R}$.

Для доведення зворотного включення розглянемо довільну алгебру $A \in \mathfrak{R}$. Нехай Y — система твірних A. За теоремою 1.1 існує епіморфізм π вільної алгебри $F(\Omega, Y)$ сигнатури Ω на алгебру A, який на множині Y діє тотожно. Крім того, існує аналогічний епіморфізм ψ алгебри $F(\Omega, Y)$ на вільну алгебру $F_{\mathfrak{M}}(Y)$ класу $\mathfrak{M}$. Розглянемо довільний елемент

$$\big(u(y_1, \ldots, y_k), v(y_1, \ldots, y_k)\big) \in \operatorname{Ker} \psi.$$

Із властивостей вільних алгебр випливає, що існують такі гомоморфізми $\chi : F(\Omega, Y) \to F(\Omega, X)$, $\varphi : F(\Omega, X) \to F_{\mathfrak{M}}(X)$ і $\rho : F_{\mathfrak{M}}(Y) \to F_{\mathfrak{M}}(X)$, що $\chi(y_i) = \rho(y_i) = \varphi(x_i) = x_i$ для всіх $i = 1, \ldots, k$.

$$\begin{array}{ccccc} & & F(\Omega, Y) & \xrightarrow{\chi} & F(\Omega, X) \\ & \swarrow \pi & \downarrow \psi & & \varphi \downarrow \\ A & \underset{\delta}{\leftarrow} & F_{\mathfrak{M}}(Y) & \underset{\rho}{\rightarrow} & F_{\mathfrak{M}}(X) \end{array}$$

Рис. 6.

Тому в алгебрі $F_{\mathfrak{M}}(X)$ маємо:

$$u(x_1, \ldots, x_k) = u(\rho(y_1), \ldots, \rho(y_k)) = \rho(u(y_1, \ldots, y_k)) =$$
$$= \rho\big(u(\psi(y_1), \ldots, \psi(y_k))\big) = \rho\big(\psi(u(y_1, \ldots, y_k))\big) =$$
$$= \rho\big(\psi(v(y_1, \ldots, y_k))\big) = \cdots = v(x_1, \ldots, x_k).$$

Отже, тотожність $u(x_1, \ldots, x_k) = v(x_1, \ldots, x_k)$ належить системі Σ. Але тоді в алгебрі A повинна виконуватися рівність

$$u(\pi(y_1), \ldots, \pi(y_k)) = v(\pi(y_1), \ldots, \pi(y_k)),$$

звідки

$$\pi(u(y_1, \ldots, y_k)) = \pi(v(y_1, \ldots, y_k)).$$

Отже,

$$\big(u(y_1, \ldots, y_k), v(y_1, \ldots, y_k)\big) \in \operatorname{Ker} \pi.$$

Таким чином, $\operatorname{Ker}\psi \subseteq \operatorname{Ker}\pi$. Але тоді існує такий гомоморфізм $\delta : F_{\mathfrak{M}}(Y) \to A$, що $\pi = \varphi\delta$, причому із сюр'єктивності π випливає, що гомоморфізм δ також буде сюр'єктивним. Позаяк клас $\mathfrak{M}$ замкнений відносно гомоморфних образів, то $A \in \mathfrak{M}$ і $\mathfrak{R} \subseteq \mathfrak{M}$. □

Наслідок 5.2. *Для кожної непорожньої множини X многовид $\mathfrak{M}$ містить вільну алгебру з вільною системою твірних X.*

Доведення. Це випливає з теорем 5.4 і 5.3. □

Наслідок 5.3. *Кожна алгебра $\mathcal{A}$ многовиду $\mathfrak{M}$ є гомоморфним образом деякої вільної алгебри цього многовиду.*

Доведення. Нехай X — довільна система твірних алгебри $\mathcal{A}$. Візьмемо в $\mathfrak{M}$ вільну алгебру $F(X)$ із вільною системою твірних X. За означенням вільної алгебри занурення $X \hookrightarrow F(X)$ можна продовжити до гомоморфізму $\varphi : F(X) \to \mathcal{A}$, який, очевидно, буде епіморфізмом. □

Наслідок 5.4. *Поля не утворюють многовид.*

Доведення. Клас полів не є замкненим відносно прямих добутків. □

Будову вільних алгебр многовиду (Ω, Λ) можна описати за допомогою такої конструкції. Будемо казати, що Ω-терм p *безпосередньо виводиться* з Ω-терма q за допомогою Λ, якщо p одержується з q заміною деякого підтерма u термом v, причому Λ містить рівність $u = v$. Транзитивне замикання відношення безпосередньої вивідності позначимо $\underset{\Lambda}{\sim}$.

Вправа 5.2. *Доведіть, що відношення $\underset{\Lambda}{\sim}$ є конгруенцією на абсолютно вільній алгебрі $F(\Omega, X)$.*

Теорема 5.5. *Факторалгебра $F_\Lambda(\Omega, X) := F(\Omega, X)/\underset{\Lambda}{\sim}$ є вільною алгеброю многовиду (Ω, Λ) із вільною системою твірних X.*

Доведення. Відображення $\mu : X \to F_\Lambda(\Omega, X)$ визначається природно: кожен елемент із X переходить у відповідний клас еквівалентності конгруенції $\underset{\Lambda}{\sim}$ (тобто μ є обмеженням на X канонічного епіморфізму $F(\Omega, X) \to F(\Omega, X)/\underset{\Lambda}{\sim}$). Оскільки при епіморфізмі система твірних переходить у систему твірних, то алгебра $F(\Omega, X)/\underset{\Lambda}{\sim}$ породжується множиною $\mu(X)$.

Лишилося перевірити властивість універсальності. Нехай для деякої алгебри $\mathcal{A} \in (\Omega, \Lambda)$ задано відображення $\nu : X \to \mathcal{A}$. Відображення $\varphi : F(\Omega, X)/\underset{\Lambda}{\sim} \to \mathcal{A}$ визначимо так:

для елементів із X покладемо $\varphi(\mu(x)) = \nu(x)$ (що буде гарантувати виконання рівності $\mu \circ \varphi = \nu$);

якщо o є символом нульарної операції, то для елемента $\overline{o}$ з $F(\Omega, X)/\underset{\Lambda}{\sim}$ його образом буде відповідна константа $c_{\overline{o}}$ з $\mathcal{A}$;

далі значення відображення φ визначаємо рекурентно: якщо для термів $v_1, \ldots, v_n \in F(\Omega, X)$ образи елементів $\overline{v_1}$, $\ldots$, $\overline{v_n}$ фактор-алгебри $F(\Omega, X)/\underset{\Lambda}{\sim}$ вже визначені, а ω — операція арності n, то

$$\varphi(\overline{\omega(v_1, \ldots, v_n)}) = \omega(\varphi(\overline{v_1}), \ldots, \varphi(\overline{v_n}))\,. \tag{5.6}$$

За означенням Ω-термів кожен терм, відмінний від елемента з X, починається символом деякої операції. Звідси випливає, що кожний власний підтерм терма $\omega(v_1, \ldots, v_n)$ повинен бути підтермом одного з термів v_1, $\ldots$, v_n. Але тоді з означення конгруенції $\underset{\Lambda}{\sim}$ випливає, що рівність

$$\overline{\omega(v_1, \ldots, v_n)} = \overline{\omega(u_1, \ldots, u_n)}$$

тягне за собою рівності $\overline{v_1} = \overline{u_1}$, $\ldots$, $\overline{v_n} = \overline{u_n}$. А це означає, що задання відображення φ правилом (5.6) є коректним, бо не залежить від вибору представника $\omega(v_1, \ldots, v_n)$ класу $\overline{\omega(v_1, \ldots, v_n)}$.

Гомоморфність відображення φ безпосередньо випливає з правила (5.6). □

На завершення цього параграфу розглянемо будову вільних алгебр деяких важливих многовидів. Згідно з теоремою 5.5 для цього досить у кожному класі конгруенції $\underset{\Lambda}{\sim}$ на абсолютно вільній алгебрі $F(\Omega, X)$ виділити конкретного представника.

Групоїдом називається непорожня множина з визначеною на ній бінарною операцією. Жодних обмежень на цю операцію не накладається, тому многовид групоїдів збігається з множиною всіх алгебр сигнатури $\Omega = (\cdot)$. Позаяк множина Λ тотожностей є порожньою, то конгруенція $\underset{\Lambda}{\sim}$ збігається з відношенням рівності. Тому вільними алгебрами многовиду групоїдів (їх називають *вільними групоїдами*) будуть абсолютно вільні алгебри сигнатури $\Omega = (\cdot)$. Елементами вільного групоїда з вільною системою твірних X будуть послідовності $x_1 x_2 \ldots x_n$ $(n > 0)$ елементів із X, у яких додатково розставлені дужки, що вказують порядок виконання дій. Оскільки в послідовності $x_1 x_2 \ldots x_n$ дужки можна розставити c_{n-1} способами, де $c_n = \frac{1}{n+1}\binom{2n}{n}$ — n-те число Каталана, то кожна така послідовність породжує c_{n-1} елементів вільного групоїда.

Напівгрупи утворюють підмноговид класу групоїдів, визначений тотожністю $x\cdot(y\cdot z)=(x\cdot y)\cdot z$. Зрозуміло, що два елементи вільного групоїда будуть належати до одного класу еквівалентності породженої цією тотожністю конгруенції $\underset{\Lambda}{\sim}$ тоді й лише тоді, коли розрізняються щонайбільше порядком дужок. Отже, дужки можна проігнорувати, а класи еквівалентності конгруенції $\underset{\Lambda}{\sim}$ ототожнити із словами над алфавітом X. Із теореми 5.5 тоді випливає, що в многовиді напівгруп вільною алгеброю з вільною системою твірних X буде описана на початку розділу 2.2 вільна напівгрупа X^+.

Переходячи від напівгруп до моноїдів, нам треба додати константу 1 і тотожності $x\cdot 1=x,\ \ 1\cdot x=x$. Якщо ототожнити цю константу з пустим словом, то аналогічно попередньому отримаємо, що в многовиді моноїдів вільною алгеброю з вільною системою твірних X буде вільний моноїд X^*.

Трохи складніше описуються вільні алгебри в многовиді груп як алгебр сигнатури $(\cdot,^{-1},1)$. Нехай X — непорожня множина. Розглянемо множину

$$X\cup X^{-1}=\{x^{\varepsilon}\mid x\in X,\ \varepsilon=\pm 1\},$$

причому елементи x і x^1 не будемо розрізняти. Для слів із $(X\cup X^{-1})^*$ будемо говорити, що слово u одержується *редукцією* слова v, якщо u одержується з v викиданням деякого підслова вигляду $x^{\varepsilon}x^{-\varepsilon}$, де $x\in X$ і $\varepsilon=\pm 1$. Слово, яке не містить підслів вигляду $x^{\varepsilon}x^{-\varepsilon}$, назвемо *нескоротним*. Позаяк при редукції довжина слова зменшується, то в результаті редукцій з даного слова рано чи пізно отримається нескоротне.

Якщо початкове слово містить кілька підслів вигляду $x^{\varepsilon}x^{-\varepsilon}$, то процес зведення до нескоротного слова визначений неоднозначно. Однак результат цього процесу є однозначним.

Лема 5.1. *Нескоротне слово, яке отримується з даного за допомогою редукцій, визначене однозначно.*

Доведення. Будемо доводити за довжиною $l(\omega)$ початкового слова ω. Для слів довжини ≤ 2 твердження леми очевидне, що дає базу індукції. Припустимо тепер, що для слів довжини, меншої ніж $l(\omega)$, твердження вже доведене. Очевидно, що коли слово ω містить не більше одного підслова вигляду $x^{\varepsilon}x^{-\varepsilon}$, то процес його зведення до нескоротного слова є однозначним. Тому різні послідовності редукцій можливі лише тоді, коли слово ω містить кілька підслів вигляду $x^{\varepsilon}x^{-\varepsilon}$.

Отже, нехай маємо дві різні послідовності редукцій. Якщо перша редукція обох послідовностей стосувалася того самого підслова, то однозначність відповідного нескоротного слова випливає з припущення індукції. Тому лишилося розглянути випадок, коли перша редукція стосується різних підслів. Тут можливі два підвипадки.

I. Перші редукції двох різних послідовностей стосуються слів, які перетинаються. Це можливе, якщо слово ω має вигляд $\omega = ux^{\varepsilon}x^{-\varepsilon}x^{\varepsilon}v$ і в одному випадку перша редукція знищує підслово $x^{\varepsilon}x^{-\varepsilon}$, а в другому — підслово $x^{-\varepsilon}x^{\varepsilon}$. В обох випадках після першої редукції отримуємо слово $w = ux^{\varepsilon}v$ і однозначність відповідного нескоротного слова випливає з припущення індукції.

II. Перші редукції стосуються слів, які не перетинаються. У цьому випадку слово ω має вигляд $\omega = w_1x^{\varepsilon}x^{-\varepsilon}w_2y^{\varepsilon'}y^{-\varepsilon'}w_3$ і перша редукція першої послідовності редукцій знищує підслово $x^{\varepsilon}x^{-\varepsilon}$, а другої послідовності — підслово $y^{\varepsilon'}y^{-\varepsilon'}$. Припустимо, що в результаті першої послідовності редукцій отримуємо нескоротне слово v, а в результаті другої — нескоротне слово u. Із рис. 7 видно, що з кожного із слів $w_1w_2y^{\varepsilon'}y^{-\varepsilon'}w_3$ і $w_1x^{\varepsilon}x^{-\varepsilon}w_2w_3$ редукцією можно отримати слово $w_1w_2w_3$.

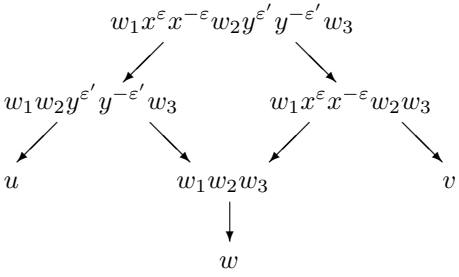


Рис. 7

Нехай w — нескоротне слово, яке отримується з $w_1w_2w_3$. Позаяк кожне із слів $w_1w_2y^{\varepsilon'}y^{-\varepsilon'}w_3$ і $w_1x^{\varepsilon}x^{-\varepsilon}w_2w_3$ має меншу довжину, ніж ω, то, за припущенням індукції, $u = w$ і $w = v$. Отже, $u = v$. □

Нехай $(X \cup X^{-1})^*$ — вільний моноїд над алфавітом $X \cup X^{-1}$, а $\overline{w}$ — нескоротне слово, яке отримується із слова w.

Лема 5.2. *Відношення* $\rho = \{(u, v) \mid \overline{u} = \overline{v}\}$ *є конгруенцією на* $(X \cup X^{-1})^*$.

Доведення. Справді, нехай $\overline{u_1} = \overline{u_2}$ і $\overline{v_1} = \overline{v_2}$. Тоді, використовуючи лему 5.1, отримуємо:

$$\overline{u_1 v_1} = \overline{\overline{u_1}\,\overline{v_1}} = \overline{\overline{u_2}\,\overline{v_2}} = \overline{u_2 v_2}.$$

□

Теорема 5.6. *Факторнапівгрупа $G(X) = (X \cup X^{-1})^*/\rho$ є вільною групою із системою твірних X.*

Доведення. Оскільки для кожного слова $x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \in (X \cup X^{-1})^*$ маємо

$$(x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \cdot x_k^{-\varepsilon_1} \cdots x_1^{-\varepsilon_1}, 1) \in \rho\,,$$

то у факторнапівгрупі $G(X)$ для кожного елемента існує обернений. Тому $G(X)$ є групою. Через π позначимо канонічний епіморфізм $(X \cup X^{-1})^* \to G(X)$.

Відображення $\mu : X \to G(X)$ визначається природно: кожному елементу $x \in X$ ставимо у відповідність той клас еквівалентності конгруенції ρ, який містить слово x. Тобто μ є обмеженням на X канонічного епіморфізму π. Очевидно, що множина $\mu(X)$ породжує $G(X)$ як групу.

Лишилося перевірити властивість універсальності. Нехай задано відображення $\nu : X \to G$ множини X у деяку групу G. Розглянемо відображення $\psi : X \cup X^{-1} \to G$, при якому для довільного $x \in X$ $\psi(x) = \nu(x)$ і $\psi(x^{-1}) = \nu(x)^{-1}$. Позаяк $(X \cup X^{-1})^*$ — вільний моноїд, то це відображення продовжується до гомоморфізму $\widetilde{\psi} : (X \cup X^{-1})^* \to G$ моноїдів. Позаяк для довільного $x \in X$ маємо

$$\widetilde{\psi}(x^{\varepsilon} x^{-\varepsilon}) = \widetilde{\psi}(x^{\varepsilon})\widetilde{\psi}(x^{-\varepsilon}) = \widetilde{\psi}(x^{\varepsilon})\widetilde{\psi}(x^{\varepsilon})^{-1} = 1\,,$$

то для довільного слова $v \in (X \cup X^{-1})^*$ маємо $\widetilde{\psi}(v) = \widetilde{\psi}(\overline{v})$. А це означає, що рівність $\overline{u} = \overline{v}$ тягне за собою рівність $\widetilde{\psi}(u) = \widetilde{\psi}(v)$, тобто що $\rho \subseteq \operatorname{Ker} \widetilde{\psi}$. Але тоді з першої теореми про ізоморфізм (задача 1.3) та основної теореми про гомоморфізми випливає існування такого гомоморфізму $\varphi : G(X) \to G$, що $\widetilde{\psi} = \pi \circ \varphi$.

Тепер для кожного $x \in X$ маємо:

$$\nu(x) = \psi(x) = \widetilde{\psi}(x) = \varphi(\pi(x)) = \varphi(\mu(x))\,.$$

Отже, $\mu \circ \varphi = \nu$, що й доводить універсальність $G(X)$. □

5.3 Еквівалентність многовидів

Нехай $F(\Omega, X)$ — абсолютно вільна алгебра сигнатури Ω. Кожен її елемент — терм $\omega = \omega(x_1, \ldots, x_m)$ сигнатури Ω — індукує на довільній алгебрі $\mathcal{A}$ сигнатури Ω так звану *похідну m-арну операцію*

$$\widetilde{\omega} : (a_1, \ldots, a_m) \mapsto \omega(a_1, \ldots, a_m)\,.$$

Змістовно операція $\widetilde{\omega}$ є результатом підстановки в слово $\omega(x_1,\dots,x_m)$ замість змінних x_i елементів a_i, $i=1,\dots,m$. А формально $\widetilde{\omega}(a_1,\dots,a_m)$ можна визначити так: розглянемо відображення $X\to A$, при якому $x_i\mapsto a_i$, $i=1,\dots,m$. За основною властивістю вільної алгебри це відображення продовжується до гомоморфізму $\varphi : F(\Omega,X)\to\mathcal{A}$. Тоді $\widetilde{\omega}(a_1,\dots,a_m)=\varphi(\omega)$.

Сукупність $W(\Omega)$ похідних операцій утворює так звану *похідну сигнатуру* сигнатури Ω. Із теореми Біркгофа випливає, що коли операції похідної сигнатури $W(\Omega)$ поширити на всі алгебри многовиду $\mathfrak{M}=(\Omega,\Lambda)$, то він стає многовидом алгебр сигнатури $W(\Omega)$. Так утворений многовид позначається $W(\mathfrak{M})$ і називається *похідним многовидом* многовиду $\mathfrak{M}$.

Зазвичай розглядається не вся похідна сигнатура, а лише деякі операції з $W(\Omega)$. Зокрема, для них можуть використовуватися власні позначення.

Приклад 5.1. *Праве $a/b:=ab^{-1}$ та ліве $a\backslash b:=a^{-1}b$ ділення є похідними операціями в групах як універсальних алгебрах сигнатури $(\cdot,^{-1},1)$. Зокрема, у класі груп для цих операцій виконуються тотожності*

$$a/(b/b)=a,\qquad (a\backslash a)\backslash b=b\,.$$

Многовиди $\mathfrak{M}_1=(\Omega_1,\Lambda_1)$ і $\mathfrak{M}_2=(\Omega_2,\Lambda_2)$ називаються *еквівалентними за Мальцевим*, якщо кожну операцію сигнатури Ω_2 можна так записати у вигляді похідної операції сигнатури Ω_1 (і навпаки), що всі тотожності з Λ_2 стануть наслідками тотожностей із Λ_1 (і навпаки).

Твердження 5.4. *Многовид сигнатури $(-,0)$, визначений тотожностями*

$$x-x=0,\qquad 0-(0-x)=x\quad i\quad (x-y)-z=(x-z)-y\,,\qquad (5.7)$$

еквівалентний за Мальцевим многовиду абелевих груп у сигнатурі $(\cdot,^{-1},e)$.

Доведення. Операціям однієї сигнатури поставимо у відповідність такі похідні операції іншої сигнатури:

$$e\leftrightarrow 0,\quad x^{-1}\leftrightarrow 0-x,\quad xy\leftrightarrow x-(0-y),\quad x-y\leftrightarrow xy^{-1}.$$

Тепер покажемо, що з тотожностей (5.5) і $x\cdot y=y\cdot x$ випливають тотожності (5.7):

$$x-x=x\cdot x^{-1}=e=0;\qquad 0-(0-x)=e\cdot(x^{-1})^{-1}=e\cdot x=x;$$
$$(x-y)-z=(xy^{-1})\cdot z^{-1}=(xz^{-1})\cdot y^{-1}=(x-z)-y\,.$$

Із тотожностей (5.7), у свою чергу, випливають (5.5) і $x \cdot y = y \cdot x$. Справді,

$$\begin{gathered} x^{-1} \cdot x = (0 - x) - (0 - x) = 0 = e; \\ e \cdot x = 0 - (0 - x) = x; \\ x \cdot y = x - (0 - y) = \big(0 - (0 - x)\big) - (0 - y) = \\ = \big(0 - (0 - y)\big) - (0 - x) = y - (0 - x) = y \cdot x; \\ (x \cdot y) \cdot z = (y \cdot x) \cdot z = \big(y - (0 - x)\big) - (0 - z) = \\ = \big(y - (0 - z)\big) - (0 - x) = (y \cdot z) \cdot x = x \cdot (y \cdot z). \end{gathered}$$

□

Інші приклади еквівалентності многовидів є в задачах 3.44–45 і 3.18–20.

5.4 Теорема Мальцева

Теорема 3.4 стверджує, що для модулярності решітки $\mathrm{Con}\,(\mathcal{A})$ конгруенцій алгебри $\mathcal{A}$ достатньо, щоб конгруенції комутували як бінарні відношення. Хороший критерій комутування конгруенцій дає така

Теорема 5.7 (Мальцев)**.** *У кожній алгебрі многовиду* (Ω, Λ) *конгруенції будуть попарно переставними тоді й лише тоді, коли існує такий* Ω*-терм* $\omega(x, y, z)$ *від змінних* x, y, z*, що в усіх алгебрах із* (Ω, Λ) *виконуються тотожності* $\omega(x, x, z) = z$ *і* $\omega(x, z, z) = x$*.*

Доведення. Необхідність. Нехай у кожній алгебрі многовиду (Ω, Λ) усі конгруенції попарно переставні. Досить показати, що існує такий Ω-терм $\omega(x, y, z)$, що у вільній алгебрі $F = F(x, y, z)$ многовиду (Ω, Λ) виконуються рівності $\omega(x, x, z) = z$ і $\omega(x, z, z) = x$. Для цього розглянемо ще вільну алгебру $G = G(u, v)$ і такі гомоморфізми $\varphi_1, \varphi_2 : F \to G$, що

$$\varphi_1(x) = \varphi_1(y) = \varphi_2(x) = u, \qquad \varphi_1(z) = \varphi_2(y) = \varphi_2(z) = v.$$

Позаяк $(x, z) \in \mathrm{Ker}\,\varphi_1 \circ \mathrm{Ker}\,\varphi_2$ і $\mathrm{Ker}\,\varphi_1 \circ \mathrm{Ker}\,\varphi_2 = \mathrm{Ker}\,\varphi_2 \circ \mathrm{Ker}\,\varphi_1$, то існує таке слово $\omega = \omega(x, y, z)$, що

$$(x, \omega) \in \mathrm{Ker}\,\varphi_2 \quad \text{і} \quad (\omega, z) \in \mathrm{Ker}\,\varphi_1\,.$$

Тому

$$\begin{aligned} \omega(u, u, v) &= \omega(\varphi_1(x), \varphi_1(y), \varphi_1(z)) = \varphi_1(\omega(x, y, z)) = \varphi_1(z) = v\,, \\ \omega(u, v, v) &= \omega(\varphi_2(x), \varphi_2(y), \varphi_2(z)) = \varphi_2(\omega(x, y, z)) = \varphi_2(x) = u\,. \end{aligned}$$

Розглянемо тепер гомоморфізм $\psi : G \to F$, для якого $\psi(u) = x$, $\psi(v) = z$. Тоді

$$\omega(x,x,z) = \omega(\psi(u),\psi(u),\psi(v)) = \psi(\omega(u,u,v)) = \psi(v) = z,$$
$$\omega(x,z,z) = \omega(\psi(u),\psi(v),\psi(v)) = \psi(\omega(u,v,v)) = \psi(u) = x.$$

Достатність. Нехай тепер $A \in (\Omega,\Lambda)$, ρ_1, ρ_2 — конгруенції на A і $(a,b) \in \rho_1 \circ \rho_2$. Тоді існує такий елемент $c \in A$, що $a,c) \in \rho_1$ і $(c,b) \in \rho_2$. Оскільки $a = \omega(a,b,b)$ і $(\omega(a,b,b),\omega(a,c,b)) \in \rho_2$, то $(a,\omega(a,c,b)) \in \rho_2$. Аналогічно з рівності $b = \omega(a,a,b)$ випливає, що $(\omega(a,c,b),b) \in \rho_1$. Отже, $(a,b) \in \rho_2 \circ \rho_1$ і $\rho_1 \circ \rho_2 \subseteq \rho_2 \circ \rho_1$.

Зворотне включення доводиться аналогічно. □

Наслідок 5.5. *Якщо сигнатура Ω многовиду $\mathfrak{M} = (\Omega,\Lambda)$ містить групові операції $\cdot, ^{-1}$, e* (тобто операції $\cdot, ^{-1}$, e, які задовольняють аксіомам групи)*, то в кожній алгебрі з $\mathfrak{M}$ конгруенції попарно переставні.*

Доведення. Досить зауважити, що групове слово $\omega = xy^{-1}z$ задовольняє умови теореми 5.7. □

5.5 Задачі

1. Чи утворює многовид клас модулярних решіток?
2. Доведіть, що для кожного натурального $n \geq 1$ групи експоненти n утворюють многовид алгебр сигнатури $(\cdot, ^{-1}, 1)$. Випишіть тотожності, які задають цей многовид.
3. Доведіть, що кожен многовид унарів визначається однією тотожністю вигляду або $f^k(x) = f^m(x)$, або $f^k(x) = f^k(y)$.
4. Опишіть вільні алгебри многовиду унарів, який задається тотожністю $f^k(x) = x$.
5. Опишіть найменший многовид унарів, який містить такий унар:
   a) $\langle\{a,b,c\}; f\rangle$, де $f(a) = b$, $f(b) = c$, $f(c) = a$;
   b) $\langle\{a,b\}; f\rangle$, де $f(a) = f(b) = b$;
   c) $\langle\{a_1,a_2,a_3,\ldots\}; f\rangle$, де $f(a_i) = a_{i+1}$ для всіх $i > 0$.
6. Опишіть найменший многовид комутативних асоціативних кілець з одиницею, який містить кільце $\mathbb{Z}_p$.
7. Доведіть, що кожний многовид абелевих груп визначається однією тотожністю вигляду $nx = 0$.
8. Опишіть вільні алгебри многовиду абелевих груп, заданого тотожністю $nx = 0$.

9. Яку необхідну й достатню умову має задовольняти скінченна абелева група, щоб бути вільною алгеброю в якомусь многовиді абелевих груп?

10. Опишіть найменший многовид абелевих груп, який містить: a) групу C_n; b) групи C_n і C_n; c) групу $\mathbb{Z}$.

11. Через $\mathrm{Var}\mathcal{A}$ позначається найменший многовид, який містить дану алгебру $\mathcal{A}$. Доведіть, що коли алгебра $\mathcal{A}$ — скінченна, то кожна скінченнопороджена алгебра з $\mathrm{Var}\mathcal{A}$ також скінченна.

12. Доведіть, що найменший многовид $\mathfrak{M}$, який містить даний клас алгебр $\mathfrak{K}$, складається з усіх ізоморфних образів факторалгебр підалгебр прямих добутків алгебр із $\mathfrak{K}$.

13. Доведіть, що коли множини X і Y рівнопотужні, то вільні алгебри класу $\mathfrak{M}$ із вільними системами твірних X і Y — ізоморфні.

14. Доведіть, що клас усіх нільпотентних напівгруп не є многовидом і в ньому нема вільних алгебр.

15. Доведіть, що клас усіх асоціативних нільпотентних лінійних алгебр над даним полем P a) не є многовидом; b) не містить вільних алгебр.

16. Доведіть, що клас нільпотентних напівгруп ступеня нільпотентності $\leq n$ є многовидом, і опишіть вільні об'єкти цього многовиду.

17. Доведіть, що клас асоціативних нільпотентних лінійних алгебр над даним полем P ступеня нільпотентності $\leq n$ є многовидом, і опишіть вільні алгебри цього многовиду.

18. Доведіть, що коли покласти $a\backslash b = a^{-1}b$, $b/a = ba^{-1}$, то клас груп можна розглядати як многовид алгебр сигнатури $(\cdot, \backslash, /)$, визначений тотожностями $(xy)z = x(yz)$, $x(x\backslash y) = y$, $(y/x)x = y$, $x\backslash xy = y$, $yx/x = y$.

19. Доведіть, що клас груп можна розглядати як многовид алгебр сигнатури, яка містить єдину бінарну дію b/a (див. задачу 18).

20. Доведіть, що визначений тотожністю $a/((b/c)/(b/a)) = c$ многовид алгебр із єдиною бінарною операцією b/a еквівалентний за Мальцевим многовиду груп як алгебр сигнатури $(\cdot, ^{-1}, e)$.

6 Поля p-адичних чисел

6.1 Кільце цілих p-адичних чисел

Нехай $(A,+)$ — записана адитивно абелева група. Для довільних двох ендоморфізмів φ і ψ групи A визначимо їх суму $\varphi+\psi$:

$$(\varphi+\psi)(x) := \varphi(x)+\psi(x)\,. \tag{6.1}$$

Оскільки

$$\begin{gathered}(\varphi+\psi)(x+y)=\varphi(x+y)+\psi(x+y)=(\varphi(x)+\varphi(y))+(\psi(x)+\psi(y))=\\ =(\varphi(x)+\psi(x))+(\varphi(y)+\psi(y))=(\varphi+\psi)(x)+(\varphi+\psi)(y)\,,\end{gathered}$$

то сума двох ендоморфізмів знову є ендорфізмом.

Твердження 6.1. *Множина* $\mathrm{End}A$ *ендоморфізмів абелевої групи* A *із визначеним за допомогою* (6.1) *додаванням і звичайним множенням ендоморфізмів утворює асоціативне кільце з одиницею.*

Доведення зводиться до безпосередньої перевірки аксіом асоціативного кільця. Одиницею буде тотожний автоморфізм. □

Приклад Кільцем ендоморфізмів абелевої групи $\mathbb{Z}_p\oplus\cdots\oplus\mathbb{Z}_p$ є кільце матриць $M_n(\mathbb{Z}_p)$.

Нехай $\mathbb{C}_{p^k}$ — мультиплікативна група всіх комплексних коренів із 1 степеня p^k. Ця група циклічна і твірним елементом можна взяти $a_k=\cos\frac{2\pi}{p^k}+i\sin\frac{2\pi}{p^k}$. Такий вибір твірних елементів у групах $\mathbb{C}_{p^k}$, $k\geq 1$, узгоджений у тому сенсі, що для всіх k буде $a_{k+1}^p=a_k$.

Розглянемо тепер групу $\mathbb{C}_{p^\infty}=\bigcup_k\mathbb{C}_{p^k}$. Оскільки множина $\{a_k\,|\,k\geq 1\}$ є системою твірних групи $\mathbb{C}_{p^\infty}$, то кожен ендоморфізм $\varphi\in\mathrm{End}(\mathbb{C}_{p^\infty})$ повністю визначається своєю дією на елементи a_k. Для опису ендоморфізмів нам буде зручно перейти від мультиплікативного запису групової операції в $\mathbb{C}_{p^\infty}$ до адитивного. Зокрема, рівність $a_{k+1}^p=a_k$ перейде в рівність $pa_{k+1}=a_k$.

Зафіксуємо тепер ендоморфізм φ і нехай $\varphi(a_k)=m_ka_k$, де $0\leq m_k<p^k$. Із узгодженості системи твірних $\{a_k\,|\,k\geq 1\}$ маємо такий ланцюжок імплікацій:

$$\begin{gathered}pa_{k+1}=a_k\ \Rightarrow\ \varphi(pa_{k+1})=\varphi(a_k)\ \Rightarrow\ pm_{k+1}a_{k+1}=m_ka_k\ \Rightarrow\\ \Rightarrow\ m_{k+1}a_k=m_ka_k\ \Rightarrow\ m_{k+1}\equiv m_k\pmod{p^k}.\end{gathered}$$

Таким чином, ендоморфізм φ повністю визначається послідовністю

$$(m_1, m_2, m_3, \ldots), \quad \text{де } 0 \le m_k < p^k,\ m_{k+1} \equiv m_k \pmod{p^k},\ k = 1, 2, \ldots . \tag{6.2}$$

Із другого боку, кожна послідовність вигляду (6.2) визначає певний ендоморфізм групи $\mathbb{C}_{p^\infty}$. Легко перевіряється, що коли ендоморфізми φ і ψ задаються відповідно послідовностями $(m_1, m_2, \ldots)$ і $(n_1, n_2, \ldots)$, то їх сумі $\varphi + \psi$ відповідає послідовність

$$(u_1, u_2, u_3, \ldots), \quad \text{де} \quad u_k = (m_k + n_k) \bmod p^k \quad \text{для всіх } k\,, \tag{6.3}$$

а добуткові $\varphi\psi$ — послідовність

$$(v_1, v_2, v_3, \ldots), \quad \text{де} \quad v_k = m_k n_k \bmod p^k \quad \text{для всіх } k\,. \tag{6.4}$$

Звідси, зокрема, випливає, що кільце $\mathrm{End}(\mathbb{C}_{p^\infty})$ буде комутативним.

Елементи кільця $\mathrm{End}(\mathbb{C}_{p^\infty})$ зручно задавати у трохи інший спосіб. Оскільки $m_{k+1} \equiv m_k (\mathrm{mod}\ p^k)$ і $0 \le m_{k+1} < p^{k+1}$, то m_{k+1} можна записати у вигляді $m_{k+1} = m_k + \alpha_k p^k$, де $0 \le \alpha_k < p$. Якщо додатково позначити $m_1 = \alpha_0$, то маємо:

$$m_1 = \alpha_0,\ m_2 = \alpha_0 + \alpha_1 p,\ m_3 = \alpha_0 + \alpha_1 p + \alpha_2 p^2,\ m_4 = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3, \ldots$$

Тому послідовності (6.2) можна поставити у відповідність нескінченну формальну суму

$$\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 + \cdots\,, \quad 0 \le \alpha_i < p,\ i = 0, 1, 2, \ldots\ . \tag{6.5}$$

Сума (6.5) дуже нагадує запис натурального числа в системі числення з основою p. Додавання й множення елементів кільця $\mathrm{End}(\mathbb{C}_{p^\infty})$, заданих такими сумами, також подібне до додавання і множення натуральних чисел й виконується "порозрядно": додаємо чи перемножуємо дві такі суми формально, потім збираємо збираємо коефіцієнти при даному розряді p^k, остачу від ділення суми цих коефіцієнтів на p пишемо при p^k, а частку переносимо в наступний розряд (тобто при "переповненні" розряду відбувається "перенесення" в наступний розряд). Наприклад, при $p = 7$:

$$(2 + 1 \cdot 7 + 3 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4 + \cdots) + (4 + 1 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^4 + \cdots) =$$
$$= 6 + 2 \cdot 7 + 2 \cdot 7^2 + 3 \cdot 7^3 + 1 \cdot 7^4 + \cdots\ ;$$
$$(2 + 1 \cdot 7 + 3 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4 + \cdots) \cdot (4 + 1 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^4 + \cdots) =$$
$$= 1 + 0 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + 6 \cdot 7^4 + \cdots\,.$$

Якщо елементи кільця $\mathrm{End}(\mathbb{C}_{p^\infty})$ задаються у вигляді сум (6.5), то їх зазвичай називають *цілими p-адичними числами*, а саме кільце позначають $\mathbb{Z}_{(p)}$ і називають *кільцем цілих p-адичних чисел*.

Вправа 6.1. *Нехай α_k — це перший ненульовий коефіцієнт елемента $a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 + \cdots$ із $\mathbb{Z}_{(p)}$. Перевірте, що елемент*

$$-a = (p - \alpha_k)p^k + (p - 1 - \alpha_{k+1})p^{k+1} + \\ + (p - 1 - \alpha_{k+2})p^{k+2} + \cdots + (p - 1 - \alpha_{k+m})p^{k+m} + \cdots$$

буде протилежним до a.

Якщо записане в системі числення з основою p натуральне число $n = \alpha_0 + \alpha_1 p + \cdots + \alpha_k p^k$ ототожнити з сумою

$$\alpha_0 + \alpha_1 p + \cdots + \alpha_k p^k + 0 \cdot p^{k+1} + 0 \cdot p^{k+2} + 0 \cdot p^{k+3} + \cdots ,$$

то одержимо природне занурення множини $\mathbb{N}$ натуральних чисел в $\mathbb{Z}_{(p)}$, яке зберігає додавання й множення. Це занурення можна природно продовжити до занурення $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)}$ (із вправи 6.1 випливає, що від'ємним цілим числам будуть відповідати суми вигляду (6.5), у яких із певного місця всі коефіцієнти дорівнюють $p - 1$).

Теорема 6.1. *Кільце $\mathbb{Z}_{(p)}$ є кільцем без дільників 0.*

Доведення. Нехай $a \neq 0$ і $b \neq 0$. Якщо α_k — перший ненульовий коефіцієнт числа $a = \alpha_0 + \alpha_1 p + \cdots$, а β_l — перший ненульовий коефіцієнт числа $b = \beta_0 + \beta_1 p + \cdots$, то $\gamma_{k+l} = \alpha_k \beta_l \bmod p$ — перший ненульовий коефіцієнт числа $ab = \gamma_0 + \gamma_1 p + \cdots$. Отже, $ab \neq 0$. □

Зауваження. Інше доведення твердження 6.1 можна одержати із задачі 1.

Твердження 6.2. *Елемент $a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$ кільця $\mathbb{Z}_{(p)}$ буде оборотним тоді й лише тоді, коли $\alpha_0 \neq 0$*

Доведення. Необхідність умови очевидна. Для доведення достатності вкажемо алгоритм обчислення оберненого елемента. Отже, нехай $\alpha_0 \neq 0$. Коефіцієнти елемента $b = \beta_0 + \beta_1 p + \beta_2 p^2 + \cdots$, оберненого до a, будемо шукати послідовно, виходячи з рівності

$$(\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots) \cdot (\beta_0 + \beta_1 p + \beta_2 p^2 + \cdots) = 1 + 0 \cdot p + 0 \cdot p^2 + \cdots .$$

Коефіцієнт β_0 можна знайти з конгруенції

$$\alpha_0 \beta_0 \equiv 1 \pmod{p},$$

бо α_0 є оборотним елементом за модулем p. Далі з конгруенції

$$\alpha_0\beta_1 + \alpha_1\beta_0 + \delta_1 \equiv 0 \pmod{p},$$

де $\delta_1 = \frac{\alpha_0\beta_0 - 1}{p}$, знаходимо β_1. І т. д. Черговий коефіцієнт β_k знаходимо з конгруенції

$$\alpha_0\beta_k + \alpha_1\beta_{k-1} + \cdots + \alpha_k\beta_0 + \delta_k \equiv 0 \pmod{p},$$

де $\delta_k = \frac{\alpha_0\beta_{k-1} + \alpha_1\beta_{k-2} + \cdots + \alpha_{k-1}\beta_0 + \delta_{k-1}}{p}$. Отже, таким чином можна знайти всі коефіцієнти елемента b. □

Із твердження 6.2 випливає, що кожен ненульовий елемент b кільця $\mathbb{Z}_{(p)}$ однозначно записується у вигляді $b = p^k a$, де елемент a є оборотним. Справді, якщо β_k — перший ненульовий коефіцієнт елемента $b = \beta_0 + \beta_1 p + \cdots$, то

$$b = p^k \cdot (\beta_k + \beta_{k+1}p + \beta_{k+2}p^2 + \cdots) \tag{6.6}$$

і елемент $a = \beta_k + \beta_{k+1}p + \beta_{k+2}p^2 + \cdots$ є оборотним. Таким чином, із точністю до асоційованості в кільці $\mathbb{Z}_{(p)}$ є тільки один простий елемент — це p.

Із існування для кожного елемента розкладу (6.6) одразу випливає

Твердження 6.3. *Кожен ідеал кільця $\mathbb{Z}_{(p)}$ має вигляд $p^k\mathbb{Z}_{(p)}$. Зокрема, усі ідеали є головними і утворюють за включенням спадний ланцюг*

$$\mathbb{Z}_{(p)} \supset p\mathbb{Z}_{(p)} \supset p^2\mathbb{Z}_{(p)} \supset p^3\mathbb{Z}_{(p)} \supset \cdots \supset p^n\mathbb{Z}_{(p)} \supset \cdots .$$

6.2 Поле часток

Нехай A — область цілісності (тобто комутативне асоціативне кільце з одиницею і без дільників нуля), а S — підмоноїд моноїда $\langle A; \cdot \rangle$, причому $0 \notin S$. Упорядковану пару (a, u), де $a \in A$ і $u \in S$, будемо називати *дробом* і записувати у вигляді $\frac{a}{u}$. Компоненти a і u називається відповідно *чисельником* і *знаменником* дробу $\frac{a}{u}$. На множині M усіх дробів визначимо дії

$$\frac{a}{u} + \frac{b}{v} := \frac{av + bu}{uv}, \qquad \frac{a}{u} \cdot \frac{b}{v} := \frac{ab}{uv} \tag{6.7}$$

і розглянемо відношення

$$\frac{a}{u} \sim \frac{b}{v} \quad \text{тоді і тільки тоді, коли} \quad av = bu.$$

Це відношення є відношенням еквівалентності. Справді, рефлексивність і симетричність цього відношення очевидні. Для доведення транзитивності припустимо, що $\frac{b}{v} \sim \frac{c}{w}$, тобто що $bw = cv$. Тоді

$$avw = buw = cuv\,.$$

Після скорочення рівності $avw = cuv$ на v отримуємо $aw = cu$. Отже, $\frac{a}{u} \sim \frac{b}{v}$.

Лема 6.1. *Дії* (6.7) *на множині* M *узгоджені з відношенням еквівалентності* $\sim$. *Тобто якщо* $\frac{a_1}{u_1} \sim \frac{a_2}{u_2}$ *і* $\frac{b_1}{v_1} \sim \frac{b_2}{v_2}$, *то*

$$\frac{a_1}{u_1} + \frac{b_1}{v_1} \sim \frac{a_2}{u_2} + \frac{b_2}{v_2} \qquad \text{і} \qquad \frac{a_1}{u_1} \cdot \frac{b_1}{v_1} \sim \frac{a_2}{u_2} \cdot \frac{b_2}{v_2}\,.$$

Доведення. Безпосередня перевірка. □

Узгодженість дій (6.7) із відношенням $\sim$ дозволяє перенести ці дії на фактормножину $M/\sim$, яку будемо позначати символом AS^{-1}. Допускаючи певну вольність, ми позначатимемо однаково дріб і той клас еквівалентності відношення $\sim$, який цей дріб містить. Дроби, які потрапляють в один клас еквівалентності, будемо називати *рівними*, а замість знаку $\sim$ писати знак рівності $=$. Зауважимо, що для довільного $s \in S$ виконується рівність $\frac{a}{u} \sim \frac{as}{us}$, тобто чисельник і знаменник дробу можна скорочувати (домножувати) на спільний множник.

Теорема 6.2. *Множина* AS^{-1} *з діями* (6.7) *є областю цілісності. Відображення* $\varphi : A \to AS^{-1}$, $a \mapsto \frac{a}{1}$, (точніше, a переходить у той клас еквівалентності відношення $\sim$, що містить $\frac{a}{1}$) *є мономорфізмом кілець. Для кожного елемента* $u \in S$ *його образ* $\frac{u}{1}$ *у кільці* AS^{-1} *є оборотним.*

Доведення першої частини теореми зводиться до безпосередньої перевірки аксіом області цілісності. Зауважимо, що одиницею в AS^{-1} буде клас еквівалентності, який містить дріб $\frac{1}{1}$ (туди потрапляють усі дроби вигляду $\frac{u}{u}$ і тільки вони). Нулем буде клас дробів вигляду $\frac{0}{u}$.

Якщо $\frac{a}{1} \sim \frac{b}{1}$, то $a \cdot 1 = b \cdot 1$, тобто $a = b$. Отже, відображення φ є ін'єктивним. Гомоморфність відображення φ випливає з рівностей

$$\varphi(a) + \varphi(b) = \frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = \varphi(a+b);$$
$$\varphi(a) \cdot \varphi(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = \varphi(ab).$$

Якщо $u \in S$, то серед дробів є й дріб $\frac{1}{u}$. З рівності $\frac{u}{1} \cdot \frac{1}{u} = \frac{u \cdot 1}{1 \cdot u} = \frac{1}{1}$ випливає, що дріб $\frac{1}{u}$ є оберненим до $\frac{u}{1}$. □

Кільце AS^{-1} називається *кільцем часток* (або *кільцем відношень*). Ототожнюючи елемент $a \in A$ із дробом $\frac{a}{1}$ (точніше, з класом еквівалентності, що містить цей дріб), можемо вважати A підкільцем кільця AS^{-1}.

Найважливішим є випадок, коли моноїд S збігається з множиною $A \setminus \{0\}$ усіх ненульових елементів з A. Тоді кільце часток AS^{-1} буде полем, яке називається *полем часток* кільця A. Справді, у цьому випадку для кожного ненульового дробу $\frac{a}{u}$ кільце AS^{-1} містить і дріб $\frac{u}{a}$. Оскільки $\frac{a}{u} \cdot \frac{u}{a} = \frac{au}{ua} = \frac{1}{1}$, то елемент $\frac{a}{u}$ є оборотним.

Приклади. 1. Поле $\mathbb{Q}$ раціональних чисел є полем часток кільця $\mathbb{Z}$ цілих чисел.

2. Поле $P(x)$ раціональних функцій є полем часток кільця многочленів $P[x]$ з коефіцієнтами з поля P.

Означення 6.1. *Поле часток кільця $\mathbb{Z}_{(p)}$ цілих p-адичних чисел називається* ***полем p-адичних чисел*** *і позначається символом $\mathbb{Q}_p$.*

Як у кожному полі часток, довільні p-адичні числа можна зображувати у вигляді відношення $\frac{a}{b}$ двох цілих p-адичних чисел. У такого зображення є два недоліки: по-перше, воно дещо громіздке, по-друге, як випливає із зауваження перед теоремою 6.2, не є однозначним. Але для p-адичних чисел можна запропонувати зручніше зображення. Справді, для кожного цілого p-адичного числа існує розклад вигляду (6.6). Нехай тепер

$$a = p^m \cdot (\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots) = p^m \cdot a_1$$

і

$$b = p^l \cdot (\beta_0 + \beta_1 p + \beta_2 p^2 + \cdots) = p^l \cdot b_1,$$

причому $\alpha_0 \neq 0$ і $\beta_0 \neq 0$. Оскільки для b_1 у кільці $\mathbb{Z}_{(p)}$ існує обернений елемент b_1^{-1}, то для дробу $\dfrac{a}{b}$ маємо:

$$\frac{a}{b} = \frac{p^m \cdot a_1}{p^l \cdot b_1} = p^{m-l} \cdot (\gamma_0 + \gamma_1 p + \gamma_2 p^2 + \cdots),$$

де $\gamma_0 + \gamma_1 p + \gamma_2 p^2 + \cdots = a_1 b_1^{-1}$ і $\gamma_0 \neq 0$. Отже, для $\dfrac{a}{b}$ ми теж отримали розклад вигляду (6.6), тільки тепер показник $m - l$ степеня числа p може бути довільним цілим числом.

Таким чином, запис цілих p-адичних чисел у вигляді формальних сум (6.5) узагальнюється на довільні p-адичні числа:

кожне p-адичне число можна записати у вигляді нескінченної формальної суми

$$\alpha_{-k}p^{-k} + \alpha_{-(k-1)}p^{-(k-1)} + \cdots + \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n + \cdots, \quad (6.8)$$

яка містить лише скінченну кількість членів із від'ємними степенями p і коефіцієнти якої для всіх i задовольняють нерівність $0 \leq a_i < p$.

Зрозуміло, що з точністю до кількості нульових членів на початку формальна сума (6.8) визначена однозначно. Правила операцій із записаними у вигляді сум (6.5) цілими p-адичними числами очевидним чином переносяться і на суми (6.8)[15].

Коротко суму (6.8) будемо позначати $\alpha_{-k}\alpha_{-(k-1)}\ldots\alpha_{-1}.\alpha_0\alpha_1\alpha_2\ldots$.

6.3 Побудова поля дійсних чисел за Кантором

Строгу теорію дійсних чисел було створено у третій чверті XIX ст.[16] У 1872 р. одразу три математики — Ріхард Дедекінд, Карл Вайєрштрас і Георг Кантор — опублікували свої варіанти такої теорії. Ще у 1869 р. теорію, аналогічну канторівській, опублікував француз Шарль Мере, який у тому ж 1872 р. опублікував більш повний варіант. У 70-ті рр. XIX ст. свій варіант теорії дійсних чисел запропонував і Едуард Гайне.

[15] Такі нескінченні суми дуже нагадують відомі з теорії функцій комплексної змінної *ряди Лорана*.

[16] Хронологічно перша сучасна теорія дійсних чисел належить чеському математику Бернарду Больцано. Вона створена в 1830-ті рр., однак була опублікована лише через багато років після смерті Больцано.

Найбільш алгебричною з цих теорій є канторівська. До того ж підхід Кантора легко узагальнюється та використовується в алгебрі для побудови інших важливих об'єктів (зокрема, його можна використати для побудови поля p-адичних чисел). Тому ми зупинимося на канторівській теорії докладніше.

Вихідним об'єктом для побудови дійсних чисел у Кантора, як і в більшості інших теорій, є поле $\mathbb{Q}$ раціональних чисел. Крім визначених у полі операцій далі важливу роль буде відігравати природний лінійний порядок $<$ на $\mathbb{Q}$.

Послідовність $(a_n)_{n\in\mathbb{N}}$ раціональних чисел будемо називати *збіжною*, якщо існує таке раціональне число a, що для кожного додатного раціонального числа ε знайдеться таке натуральне число $N(\varepsilon)$, що $|a_i - a| < \varepsilon$ для всіх $i > N(\varepsilon)$. У таких випадках будемо записувати $\lim\limits_{n\to\infty} a_n = a$ і говорити, що послідовність $(a_n)_{n\in\mathbb{N}}$ *збігається* до a.

Послідовність $(a_n)_{n\in\mathbb{N}}$ раціональних чисел називається *фундаментальною* (або *послідовністю Коші*), якщо для кожного додатного раціонального числа ε знайдеться таке натуральне число $N(\varepsilon)$, що $|a_i - a_j| < \varepsilon$ для всіх $i, j > N(\varepsilon)$.

Стандартно доводяться такі властивості фундаментальних послідовностей:

Твердження 6.4. *a) Кожна фундаментальна послідовність є обмеженою.*

b) Кожна збіжна послідовність є фундаментальною.

c) Множина F фундаментальних послідовностей утворює комутативне асоціативне кільце з одиницею відносно звичайних операцій додавання та множення.

Якщо кожному елементу $a \in \mathbb{Q}$ зіставити постійну послідовність $\widehat{a} = (a, a, \ldots, a, \ldots)$, то одержимо природне занурення поля $\mathbb{Q}$ в кільце F фундаментальних послідовностей.

Через I позначимо множину тих послідовностей із F, які збігаються до 0.

Твердження 6.5. *Множина I є ідеалом кільця F.*

Доведення. Очевидно, що множина I замкнена відносно додавання та віднімання послідовностей. Крім того, з обмеженості фундаментальної послідовності випливає, що добуток фундаментальної послідовності на послідовність, збіжну до 0, також буде збігатися до 0. □

Лема 6.2. *Якщо фундаментальна послідовність $(a_n)_{n\in\mathbb{N}}$ не є збіжною до 0, то з певного місця всі її члени мають однаковий знак. Крім того, існує таке раціональне число $d>0$, що для всіх достатньо великих n виконується нерівність $|a_n|>d$.*

Доведення. Із означення збіжності послідовності випливає, що коли $(a_n)_{n\in\mathbb{N}}$ не є збіжною до 0, то

$$\exists\,\varepsilon\in\mathbb{Q}^+\ \forall\,N\ \exists\,n>N\ \ (|a_n|\geq\varepsilon)\,.$$

Отже, у цьому випадку існують члени з як завгодно великими номерами n, для яких виконується нерівність $|a_n|\geq\varepsilon$. Із другого боку, із фундаментальності послідовності $(a_n)_{n\in\mathbb{N}}$ випливає, що існує таке N, що $|a_i-a_j|<\frac{\varepsilon}{2}$ для всіх $i,j>N$.

Виберемо тепер таке n_0, щоб виконувалися нерівності $n_0>N$ і $|a_{n_0}|\geq\varepsilon$. Припустимо спочатку, що $a_{n_0}>0$. Тоді для всіх $i>N$ будемо мати:

$$a_i=a_{n_0}+(a_i-a_{n_0})\geq a_{n_0}-|a_i-a_{n_0}|>\varepsilon-\frac{\varepsilon}{2}=\frac{\varepsilon}{2}\,.$$

У випадку $a_{n_0}<0$ аналогічно доводиться, що для всіх $i>N$ виконується нерівність $a_i<-\frac{\varepsilon}{2}$. □

Теорема 6.3. *Факторкільце $\mathbb{R}=F/I$ є полем.*

Доведення. Оскільки F є комутативним асоціативним кільцем із одиницею, то таким буде і факторкільце $\mathbb{R}=F/I$. Тому досить лише показати, що в цьому факторкільці для кожного ненульового елемента існує обернений.

Отже, нехай клас суміжності $(a_n)_{n\in\mathbb{N}}+I$ не є нулем факторкільця F/I. Тоді послідовність $(a_n)_{n\in\mathbb{N}}$ не є збіжною до 0. Зрозуміло, що коли ми змінимо кілька початкових членів цієї послідовності, то нова послідовність $(a'_n)_{n\in\mathbb{N}}$ також буде фундаментальною, причому обидві послідовності належатимуть до одного класу суміжності за ідеалом I. Тому на підставі леми 6.2 ми, без обмеження загальності, можемо вважати, що існує таке раціональне число $d>0$, що для всіх n виконується нерівність $|a_n|>d$.

Покажемо, що послідовність $(1/a_n)_{n\in\mathbb{N}}$ також є фундаментальною. Справді, для довільних i,j маємо:

$$\Big|\frac{1}{a_i}-\frac{1}{a_j}\Big|=\frac{|a_i-a_j|}{|a_i|\,|a_j|}<\frac{|a_i-a_j|}{d^2}\,.$$

Розглянемо тепер довільне $\varepsilon \in \mathbb{Q}^+$ і виберемо натуральне число N так, щоб для всіх $i, j > N$ виконувалася нерівність $|a_i - a_j| < \varepsilon d^2$. Тоді для всіх $i, j > N$ маємо:

$$\Big|\frac{1}{a_i} - \frac{1}{a_j}\Big| < \frac{|a_i - a_j|}{d^2} < \frac{\varepsilon d^2}{d^2} = \varepsilon\,.$$

Отже, послідовність $(1/a_n)_{n\in\mathbb{N}}$ є фундаментальною. Очевидно, що ця послідовність є оберненою до $(a_n)_{n\in\mathbb{N}}$, бо

$$(a_n)_{n\in\mathbb{N}} \cdot (1/a_n)_{n\in\mathbb{N}} = (1, 1, \ldots, 1, \ldots)\,. \qquad \square$$

Позаяк при зануренні $\mathbb{Q} \hookrightarrow F$ різні раціональні числа переходять у різні класи суміжності за ідеалом I, то це індукує занурення $\mathbb{Q} \hookrightarrow \mathbb{R}$. Тому $\mathbb{R}$ є розширенням поля $\mathbb{Q}$. Лема 6.2 також дозволяє визначити на $\mathbb{R}$ відношення порядку. Справді, на підставі цієї леми всі елементи поля $\mathbb{R}$ можна розбити на три диз'юнктні класи $\mathbb{R}^-$, 0 і $\mathbb{R}^+$ так:

елемент $a = \overline{(a_n)_{n\in\mathbb{N}}}$ *потрапляє в клас* $\mathbb{R}^-$ (*відповідно в клас* $\mathbb{R}^+$) *тоді й лише тоді, коли, починаючи з певного місця, всі члени послідовності* $(a_n)_{n\in\mathbb{N}}$ *менші деякого фіксованого раціонального числа* $d < 0$ (*відповідно більші деякого раціонального числа* $d > 0$).

Для довільних елементів $a, b \in \mathbb{R}$ покладемо $a > b$ тоді й лише тоді, коли $a - b \in \mathbb{R}^+$.

Вправа 6.2. *Доведіть, що визначене таким чином відношення* $>$ *на* $\mathbb{R}$ *є відношенням лінійного порядку, причому обмеження цього порядку на підполе* $\mathbb{Q}$ *збігається із звичайним порядком на* $\mathbb{Q}$.

Нагадаємо, що кільце K із визначеним на ньому лінійним порядком $>$ називається *впорядкованим*, якщо виконуються такі дві умови:
(I) для довільних $a, b, c \in K$ із $a > b$ випливає $a + c > b + c$;
(II) для довільних $a, b, c \in K$ із $a > b$ і $c > 0$ випливає $ac > bc$.

Теорема 6.4. *Поле* $\mathbb{R}$ *є впорядкованим.*

Доведення зводиться до простої перевірки умов (I) і (II), яку залишаємо читачеві.

Твердження 6.6. *Множина* $\mathbb{Q}$ *є скрізь щільною в полі* $\mathbb{R}$ *у тому сенсі, що для довільних* $a > b$ *із* $\mathbb{R}$ *знайдеться таке* $c \in \mathbb{Q}$, *що* $a > c > b$.

Доведення. Нехай $a > b$ і $a = \overline{(a_n)_{n\in\mathbb{N}}}$, $b = \overline{(b_n)_{n\in\mathbb{N}}}$. За лемою 6.2 існують такі натуральне N_1 і раціональне $d > 0$, що $a_n - b_n > d$ для всіх $n > N_1$. Крім того, із фундаментальності послідовностей $(a_n)_{n\in\mathbb{N}}$ і $(b_n)_{n\in\mathbb{N}}$ випливає існування такого натурального числа $N > N_1$, що $|a_n - a_N| < d/4$ і $|b_n - b_N| < d/4$ для всіх $n > N$.

Тоді раціональне число $c = \frac{a_N+b_N}{2}$ задовольняє нерівність $a > c$, бо для всіх $n > N$ маємо:

$$a_n - \frac{a_N + b_N}{2} = \left(\frac{a_n}{2} - \frac{b_n}{2}\right) + \left(\frac{a_n}{2} - \frac{a_N}{2}\right) + \left(\frac{b_n}{2} - \frac{b_N}{2}\right) \geq \frac{d}{2} - 2\,\frac{d}{8} = \frac{d}{4}\,.$$

Аналогічно доводиться нерівність $c > b$. □

Трохи складніше доводиться наступна теорема, яку інколи називають *аксіомою про верхню грань*.

Теорема 6.5. *Кожна обмежена згори непорожня підмножина з* $\mathbb{R}$ *має точну верхню грань.*

Доведення. Нехай непорожня підмножина $A \subset \mathbb{R}$ обмежена згори елементом b. Якщо в A є найбільший елемент a, то він і буде точною верхньою гранню для A. Тому треба розглянути лише випадок, коли в A найбільшого елемента нема. Зауважимо, що в цьому випадку для кожного $a \in A$ множина $\{x \in A \mid a < x\}$ є нескінченною.

Виберемо довільний елемент $a \in A$ і покладемо $a^{(1)} = a$, $b^{(1)} = b$. Далі розглянемо проміжки

$$\left[a^{(1)}, \frac{a^{(1)} + b^{(1)}}{2}\right] \quad \text{і} \quad \left[\frac{a^{(1)} + b^{(1)}}{2}, b^{(1)}\right] \tag{6.9}$$

і позначимо через $[a^{(2)}, b^{(2)}]$ правий із тих проміжків (6.9), які містять елементи з A (із попереднього зауваження випливає, що $[a^{(2)}, b^{(2)}]$ міститиме нескінченно багато елементів з A).

Потім за проміжком $[a^{(2)},b^{(2)}]$ аналогічно будуємо проміжок $[a^{(3)},b^{(3)}]$, і т. д. Зрештою отримуємо такі дві послідовності $(a^{(n)})_{n\in\mathbb{N}}$ і $(b^{(n)})_{n\in\mathbb{N}}$, що

$$a^{(1)} \leq a^{(2)} \leq a^{(3)} \leq \cdots \leq b^{(3)} \leq b^{(2)} \leq b^{(1)}$$

і для кожного n множина $\{a \in A \mid a^{(n)} < a\}$ є нескінченною, а множина $\{a \in A \mid b^{(n)} < a\}$ — порожньою. Зокрема, кожна верхня грань для A буде більшою за всі $a^{(n)}$, а всі $b^{(n)}$ будуть верхніми гранями для A. Крім

того, для всіх натуральних n маємо:

$$b^{(n+1)} - a^{(n+1)} = \frac{b^{(1)} - a^{(1)}}{2^n}\,, \tag{6.10}$$

$$0 \le a^{(n+1)} - a^{(n)} \le \frac{b^{(1)} - a^{(1)}}{2^n}\,, \quad 0 \le b^{(n)} - b^{(n+1)} \le \frac{b^{(1)} - a^{(1)}}{2^n}\,. \tag{6.11}$$

Для кожного натурального n виберемо з інтервалу $(b^{(n)}, b^{(n)} + 1/2^n)$ якесь раціональне число c_n (це можна зробити за твердженням 6.6). Тоді послідовність $(c_n)_{n\in\mathbb{N}}$ є фундаментальною. Справді, для довільних $m > k$ маємо $c_k, c_m \in (b^{(m)}, b^{(k)} + 1/2^k)$, звідки

$$|c_k - c_m| < \Big(b^{(k)} + \frac{1}{2^k}\Big) - b^{(m)} = (b^{(k)} - b^{(m)}) + \frac{1}{2^k} <$$
$$< (b^{(1)} - a^{(1)})\Big(\frac{1}{2^k} + \frac{1}{2^{k+1}} + \cdots + \frac{1}{2^{m-1}}\Big) + \frac{1}{2^k} < \frac{b^{(1)} - a^{(1)}}{2^{k-1}} + \frac{1}{2^k}.$$

Лема 6.3. *Для елемента $c = \overline{(c_n)_{n\in\mathbb{N}}}$ і кожного натурального числа n виконуються нерівності $c \le b^{(n)}$ і $a^{(n)} \le c$.*

Доведення. Справді, нехай для якогось m буде $c > b^{(m)}$. Із цієї нерівності та леми 6.2 випливає, що існують такі N і k, що для всіх $i > N$ виконується нерівність $c_i > b^{(m)} + 1/2^k$. Тоді для довільного $i > \max(N, k, m)$

$$b^{(i)} + \frac{1}{2^i} > c_i > b^{(m)} + \frac{1}{2^k} \ge b^{(i)} + \frac{1}{2^k}\,,$$

звідки $1/2^i > 1/2^k$, що неможливо. Отже, для всіх n маємо $c \le b^{(n)}$.

Аналогічно припустимо, що для якогось m буде $a^{(m)} > c$. Тоді існують такі N і k, що для всіх $i > N$ виконується нерівність $c_i < a^{(m)} - 1/2^k$. Звідси для кожного $i > \max(N, m)$

$$a^{(m)} - \frac{1}{2^k} > c_i > b^{(i)} > a^{(i)} \ge a^{(m)}\,,$$

що знову неможливо. Отже, нерівність $c \le b^{(n)}$ також виконується для всіх n. □

Тепер уже неважко показати, що елемент c є точною верхньою гранню для A. Для цього спочатку покажемо, що для кожної верхньої грані d множини A виконується нерівність $c \le d$. Справді, якщо для якоїсь верхньої грані d маємо $c > d$, то з рівності (6.10) випливає, що існує таке n, що $b^{(n)} - a^{(n)} < c - d$. Звідси і з нерівності $d > a^{(n)}$ отримуємо $c > b^{(n)} - a^{(n)} + d > b^{(n)}$, що суперечить лемі 6.3.

Лишилося показати, що c є верхньою границею для A. Справді, у противному разі існує такий елемент $a \in A$, що $c < a$. Виберемо довільний елемент $a' \in A$, більший за a, і таке натуральне n, що $\frac{b^{(1)}-a^{(1)}}{2^n} < a' - a$. Тоді з рівності (6.10) випливає, що $a < a^{(n)}$, звідки $c < a^{(n)}$. Але це знову суперечить лемі 6.3. □

Теорема 6.6. *У полі $\mathbb{R}$ кожна фундаментальна послідовність є збіжною.*

Доведення. Нам знадобиться така

Лема 6.4. *Нехай $a = \overline{(a_n)_{n\in\mathbb{N}}}$ і $b = \overline{(b_n)_{n\in\mathbb{N}}}$ — такі елементи поля $\mathbb{R}$, що $|a - b| < \varepsilon$. Тоді знайдеться такий номер k, що $|a_n - b_n| < \varepsilon$ для всіх $n > k$.*

Доведення. Нерівність $a - b < \varepsilon$ рівносильна нерівності $a - b - \varepsilon < 0$. З останньої нерівності і леми 6.2 випливає, що для деякого додатного числа d_1 буде, починаючи з певного номера k_1, виконуватися нерівність

$$a_n - b_n - \varepsilon < -d_1\,,$$

звідки

$$a_n - b_n < \varepsilon - d_1 < \varepsilon\,.$$

Аналогічно нерівність $-\varepsilon < a - b$ означає, що для деякого додатного числа d_2 буде, починаючи з певного номера k_2, виконуватися нерівність

$$a_n - b_n + \varepsilon > d_2\,,$$

звідки

$$a_n - b_n > d_2 - \varepsilon > -\varepsilon\,.$$

Якщо тепер покласти $k = \max(k_1, k_2)$, то для всіх $n > k$ маємо $-\varepsilon < a_n - b_n < \varepsilon$, що й треба було довести. □

Нехай тепер $(a^{(j)})_{j\in\mathbb{N}}$, де $a^{(j)} = \overline{(a_n^{(j)})_{n\in\mathbb{N}}}$ — фундаментальна послідовність елементів поля $\mathbb{R}$. Для кожного j виберемо такий номер $n(j)$, що $|a_{n(j)}^{(j)} - a_m^{(j)}| < 1/2^j$ для всіх $m \geq n(j)$. Позначимо $b_j = a_{n(j)}^{(j)}$ і покажемо, що елемент $b = \overline{(b_j)_{j\in\mathbb{N}}}$ є границею послідовності $(a^{(j)})_{j\in\mathbb{N}}$.

Спочатку доведемо, що послідовність $(b_n)_{n\in\mathbb{N}}$ є фундаментальною. Зафіксуємо $\varepsilon > 0$. Із фундаментальності послідовності $(a^{(j)})_{j\in\mathbb{N}}$ випливає існування такого номера n_1, що $|a^{(k)} - a^{(m)}| < \varepsilon$ для довільних $k, m > n_1$. Далі виберемо n_2 так, щоб виконувалася нерівність $1/2^{n_2} < \varepsilon$,

і покладемо $n = \max(n_1, n_2)$. Зафіксуємо довільні $m, l > n$. За лемою 6.4 існує такий номер $q > \max(n(m), n(l))$, що $|a_q^{(m)} - a_q^{(l)}| < \varepsilon$. Тому

$$|b_m - b_l| = |a_{n(m)}^{(m)} - a_{n(l)}^{(l)}| = |a_{n(m)}^{(m)} - a_q^{(m)} + a_q^{(m)} - a_q^{(l)} + a_q^{(l)} - a_{n(l)}^{(l)}| \le$$
$$\le |a_{n(m)}^{(m)} - a_q^{(m)}| + |a_q^{(m)} - a_q^{(l)}| + |a_q^{(l)} - a_{n(l)}^{(l)}| < \frac{1}{2^m} + \varepsilon + \frac{1}{2^l} < 3\varepsilon.$$

Позаяк m і l — довільні, то це доводить фундаментальність послідовності $(b_n)_{n\in\mathbb{N}}$. А тому $b \in \mathbb{R}$.

Покажемо тепер, що b є границею послідовності $(a^{(j)})_{j\in\mathbb{N}}$. Для цього розглянемо довільне $\varepsilon > 0$ і виберемо n_1 так, щоб для всіх $m, l > n_1$ виконувалася нерівність $|b_m - b_l| < \varepsilon$, і n_2 так, щоб виконувалася нерівність $1/2^{n_2} < \varepsilon$. Покладемо $n = \max(n_1, n_2)$. Тоді для кожного $j > n$ для всіх $k > \max(n, n(j))$ маємо:

$$|b_k - a_k^{(j)}| = |b_k - b_j + b_j - a_k^{(j)}| \le |b_k - b_j| + |a_{n(j)}^{(j)} - a_k^{(j)}| < \varepsilon + \frac{1}{2^j} < 2\varepsilon.$$

Отже, $|b - a^{(j)}| < 2\varepsilon$ для всіх $j > n$, що й завершує доведення. □

6.4 Нормовані й топологічні поля

Нехай K — кільце (не обов'язково асоціативне). Відображення $K \to \mathbb{R}_{\ge 0}$, $x \mapsto \|x\|$, кільця K у множину $\mathbb{R}_{\ge 0}$ невід'ємних дійсних чисел називається *нормуванням* кільця K (або *нормою* в кільці K), якщо виконані такі умови:

(N1) $\|x\| = 0$ тоді й лише тоді, коли $x = 0$;
(N2) $\|xy\| = \|x\| \cdot \|y\|$;
(N3) $\|x + y\| \le \|x\| + \|y\|$.

Кільце з визначеною на ньому нормою називається *нормованим*. Із (N1) і (N2) випливає, що нормоване кільце не містить дільників нуля. Навпаки, у кожному кільці без дільників нуля можна визначити так зване *тривіальне* нормування, якщо покласти $\|x\| = 1$ для всіх $x \ne 0$.

Вправа 6.3. *Доведіть, що в кожному нормованому кільці виконуються такі співвідношення*:
a) $\|1\| = \|-1\| = 1$,
b) $\|a\| = \|-a\|$,
c) $\|a\| - \|b\| \le \|a - b\| \le \|a\| + \|b\|$.

Приклади. **1**. Абсолютна величина числа є нормою в кільці $\mathbb{Z}$ і в полях $\mathbb{Q}$ і $\mathbb{R}$.

2. Модуль числа є нормою в полі $\mathbb{C}$.

3. Визначена на стор. 91 норма $N(x)$ кватерніона x не є нормою в тілі $\mathbb{H}$ кватерніонів у сенсі цього розділу. Але якщо покласти $\|x\| = \sqrt{N(x)}$, то $\|\ \|$ уже буде нормою в $\mathbb{H}$. Справді, виконання умови (N2) випливає з вправи 4.4, а умови (N3) — із того, що $\|x\|$ є довжиною кватерніона x як вектора 4-вимірного евклідового простору.

4. Аналогічно за допомогою введеної в задачі 4.28 норми $N(z)$ октави z можна визначити норму $\|z\| = \sqrt{N(z)}$ в алгебрі октав Келі (виконання умови (N2) випливає із задачі 4.28, а умови (N3) — із того, що $\|z\|$ є довжиною октави z як вектора 8-вимірного евклідового простору).

5. У кільці многочленів $P[x]$ можна визначити норму, якщо взяти фіксоване число $\alpha > 1$ і для кожного ненульового многочлена $f(x)$ покласти $\|f(x)\| = \alpha^{\deg f(x)}$.

Нехай X — непорожня множина. Функція $d : X \times X \to \mathbb{R}$ називається *метрикою* на множині X, якщо вона задовольняє такі три умови:

(M1) $d(x, y) = 0$ тоді й лише тоді, коли $x = y$;

(M2) $d(x, y) = d(y, x)$ для довільних x і y;

(M3) $d(x, y) + d(y, z) \geq d(x, z)$ для довільних x, y та z (ця умова називається *нерівністю трикутника*).

Пару (X, d), де d — визначена на множині X метрика, називають *метричним простором*.

Вправа 6.4. *Доведіть, що кожна метрика набуває лише невід'ємних значень.*

Кожна норма $\|\ \|$ на кільці K природно визначає на K метрику, якщо покласти $d(x, y) = \|x - y\|$. Справді, виконання умов (M1) і (M3) випливає відповідно з властивостей (N1) і (N3) норми, а виконання (M2) — із вправи 6.3.

У свою чергу метрика d на множині X стандартно визначає на цій множині топологію, якщо за систему околів кожної точки a взяти сукупність $B(a, r) = \{x \in X \mid d(x, a) < r\}$, $r > 0$, відкритих куль із центром у цій точці. Зокрема, якщо $a \neq b$, то кулі $B\big(a, \frac{d(a,b)}{2}\big)$ і $B\big(b, \frac{d(a,b)}{2}\big)$ не перетинаються. Тому ця топологія буде навіть *гаусдорфовою*.

Поле P із визначеною на ньому топологією називається *топологічним*, якщо в цій топології кожне з відображень

$$(a, b) \mapsto a + b, \qquad (a, b) \mapsto ab, \qquad a \mapsto -a, \qquad a \mapsto a^{-1}$$

є неперервним.

Теорема 6.7. *Кожне нормоване поле P є топологічним у топології, індукованій на ньому нормою.*

Доведення. Якщо $x \in B(a,\varepsilon)$ і $y \in B(b,\varepsilon)$, то $-x \in B(-a,\varepsilon)$ і $x+y \in B(a+b,2\varepsilon)$. Це доводить неперервність відображень $a \mapsto -a$ і $(a,b) \mapsto a+b$. Неперервність відображення $(a,b) \mapsto ab$ випливає з того, що за цих умов

$$\|ab - xy\| = \|ab - xb + xb - xy\| \leq \|ab - xb\| + \|xb - xy\| \leq \varepsilon\|b\| + \varepsilon\|x\|\,.$$

А позаяк $\|x\| < \|a\| + \|\varepsilon\|$, то $\|ab - xy\| < \varepsilon(\|a\| + \|b\|) + \varepsilon^2$, тобто $xy \in B(ab, \varepsilon(\|a\| + \|b\| + \varepsilon))$.

Нарешті, якщо брати ε достатньо малим, щоб виконувалась нерівність $\varepsilon < \frac{\|a\|}{2}$, то з нерівності $\|x\| > \|a\| - \varepsilon > \frac{\|a\|}{2}$ отримуємо:

$$\Big\|\frac{1}{x} - \frac{1}{a}\Big\| = \Big\|\frac{a-x}{ax}\Big\| = \frac{\|a-x\|}{\|a\| \cdot \|x\|} < \frac{2\varepsilon}{\|a\|^2}\,.$$

Отже, $\frac{1}{x} \in B\big(\frac{1}{a}, \frac{2\varepsilon}{\|a\|^2}\big)$, що доводить неперервність відображення $a \mapsto a^{-1}$. □

Послідовність $(a_n)_{n\in\mathbb{N}}$ елементів нормованого поля P називається *фундаментальною* або *послідовністю Коші*, якщо для кожного $\varepsilon > 0$ існує таке натуральне число N, що для всіх $m, k > N$ виконується нерівність $\|a_m - a_k\| < \varepsilon$.

Послідовність $(a_n)_{n\in\mathbb{N}}$ називається *збіжною*, якщо існує такий елемент a, що для кожного $\varepsilon > 0$ існує таке натуральне число N, що для всіх $m > N$ виконується нерівність $\|a_m - a\| < \varepsilon$. Такий елемент a називається *границею* послідовності $(a_n)_{n\in\mathbb{N}}$ і позначається $a = \lim\limits_{n\to\infty} a_n$. Кажуть також, що послідовність $(a_n)_{n\in\mathbb{N}}$ *збігається* до a.

Твердження 6.7. *a) Кожна збіжна послідовність є послідовністю Коші.*

b) Якщо нескінченна підпослідовність послідовності Коші є збіжною, то й сама послідовність Коші є збіжною.

c) Якщо послідовність $(a_n)_{n\in\mathbb{N}}$ збігається до a, то послідовність $(\|a_n\|)_{n\in\mathbb{N}}$ збігається до $\|a\|$.

Доведення. a) Якщо $\|a_m - a\| < \varepsilon$ і $\|a_k - a\| < \varepsilon$, то $\|a_m - a_k\| < 2\varepsilon$.

b) Якщо $\|a_m - a\| < \varepsilon$ і $\|a_m - a_k\| < \varepsilon$, то $\|a_k - a\| < 2\varepsilon$.

c) Із вправи 6.3.c випливає, що коли $\|a_n - a\| < \varepsilon$, то $\big|\|a_n\| - \|a\|\big| \leq \|a_n - a\| < \varepsilon$. □

Вправа 6.5. *Нехай P — нормоване поле і $a = \lim\limits_{n\to\infty} a_n$, $b = \lim\limits_{n\to\infty} b_n$. Доведіть, що $\lim\limits_{n\to\infty}(a_n+b_n) = a+b$, $\lim\limits_{n\to\infty}(a_nb_n) = ab$, $\lim\limits_{n\to\infty}(-a_n) = -a$.*

Нормоване поле називається *повним*, якщо кожна фундаментальна послідовність є збіжною.

Теорему 6.6 тепер можна переформулювати як твердження про те, що *поле $\mathbb{R}$ із звичайною нормою є повним*. Однак важливість уведених понять не стільки в тому, що з'являється інший погляд на теорему 6.6, як у тому, що вони дозволяють узагальнити конструкцію Кантора поля $\mathbb{R}$ із поля раціональних чисел $\mathbb{Q}$ на довільні нормовані поля.

Теорема 6.8. *Кожне нормоване поле P можна розширити до повного нормованого поля $\overline{P}$, причому так, що обмеження норми з поля $\overline{P}$ на підполе P збігається з початковою нормою на P.*

Доведення. Ми не будемо зупинятися на деталях доведення, позаяк вони майже дослівно повторюють відповідні міркування з розділу 6.3. Нагадаємо тільки (з необхідними змінами) основні етапи конструкції.

1) Будуємо кільце F фундаментальних послідовностей елементів поля P.

2) Відображення $\mu : a \mapsto \widehat{a} = (a, a, \ldots, a, \ldots)$ є зануренням поля P у кільце F.

3) Множина I всіх послідовностей, збіжних до 0, утворює ідеал кільця F.

4) Факторкільце $\overline{P} = F/I$ виявляється полем. Канонічний епіморфізм $\pi : F \to F/I$ діє ін'єктивно на образі $\mu(P)$ поля P, а тому композиція μ і π дає занурення поля P у поле $\overline{P}$.

5) Якщо $(a_n)_{n\in\mathbb{N}}$ — фундаментальна послідовність елементів поля P, то послідовність $(\|a_n\|)_{n\in\mathbb{N}}$ норм також виявляється фундаментальною. За теоремою 6.6 послідовність $(\|a_n\|)_{n\in\mathbb{N}}$ має границю, причому для послідовностей з одного класу суміжності за ідеалом I ця границя буде однаковою. Якщо тепер для елемента $a = \overline{(a_n)_{n\in\mathbb{N}}}$ із $\overline{P}$ покласти $\|a\| = \lim\limits_{n\to\infty} \|a_n\|$, то одержимо норму на $\overline{P}$. Очевидно, що обмеження цієї норми на підполе P збігається з початковою нормою на P.

6) Поле $\overline{P}$ із нормою $\|\ \|$ є повним. □

Поле $\overline{P}$, яке будується в доведенні теореми 6.8, називається *поповненням* нормованого поля P. Спосіб, яким будується поле $\overline{P}$, будемо називати *конструкцією Кантора*.

Норми $\|\ \|_1$ і $\|\ \|_2$ на полі P називаються *еквівалентними*, якщо для обох норм фундаментальні послідовності одні й ті самі.

Лема 6.5. *Послідовність $(a^n)_{n\in\mathbb{N}}$ буде фундаментальною тоді й лише тоді, коли $a = 1$ або $\|a\| < 1$.*

Доведення. Достатність умови випливає з того, що коли $\|a\| < 1$ і $n > m$, то $\|a^n - a^m\| \le \|a^n\| + \|a^m\| < 2\|a\|^m$.

Необхідність. Із вправи 6.3.c випливає, що

$$\|a^n - a^m\| \ge \|a^n\| - \|a^m\|\,.$$

Але якщо $\|a\| > 1$, то при фіксованому n $\|a^n\| - \|a^m\| \to \infty$. Тому при $\|a\| > 1$ послідовність $(a^n)_{n\in\mathbb{N}}$ не буде фундаментальною.

Нехай тепер $\|a\| = 1$ і послідовність $(a^n)_{n\in\mathbb{N}}$ є фундаментальною. Тоді для кожного $\varepsilon > 0$ для достатньо великих n має виконуватися нерівність

$$\|a^{n+1} - a^n\| = \|a\|^n\|a - 1\| = \|a - 1\| < \varepsilon\,.$$

Отже, $\|a - 1\| = 0$, звідки $a = 1$. □

Наслідок 6.1. *Якщо норми $\|\ \|_1$ і $\|\ \|_2$ еквівалентні, то нерівність $\|x\|_1 < 1$ рівносильна нерівності $\|x\|_2 < 1$, нерівність $\|x\|_1 > 1$ — нерівності $\|x\|_2 > 1$, а рівність $\|x\|_1 = 1$ рівносильна рівності $\|x\|_2 = 1$.*

Доведення. Перше твердження випливає з леми 6.5. Переходячи до обернених елементів, отримуємо рівносильність нерівностей $\|x\|_1 > 1$ і $\|x\|_2 > 1$. Третє твердження випливає з двох перших. □

Твердження 6.8. *Норми $\|\ \|_1$ і $\|\ \|_2$ на полі P будуть еквівалентними тоді й лише тоді, коли існує таке дійсне число $\alpha > 0$, що $\|x\|_2 = \|x\|_1^\alpha$ для всіх $x \in P$.*

Доведення. Достатність. Нехай для деякого дійсного числа $\alpha > 0$ маємо $\|x\|_2 = \|x\|_1^\alpha$ і послідовність $(a_n)_{n\in\mathbb{N}}$ є фундаментальною відносно норми $\|\ \|_1$. Для довільного натурального числа n існують такі натуральні числа m і N, що $1/m^\alpha < 1/n$ і $\|a_k - a_l\|_1 < 1/m$ для всіх $k, l > N$. На проміжку $[0, \infty)$ функція $f(x) = x^\alpha$ є монотонно зростаючою, тому для всіх $k, l > N$ маємо:

$$\|a_k - a_l\|_2 = \|a_k - a_l\|_1^\alpha < 1/m^\alpha < 1/n\,.$$

Оскільки n довільне, то послідовність $(a_n)_{n\in\mathbb{N}}$ є фундаментальною і відносно норми $\|\ \|_2$. Із другого боку, $\|x\|_1 = \|x\|_2^{1/\alpha}$, а тому кожна послідовність, фундаментальна відносно норми $\|\ \|_1$, буде фундаментальною і відносно $\|\ \|_2$. Тому норми $\|\ \|_1$ і $\|\ \|_2$ еквівалентні.

Необхідність. Із наслідку 6.1 випливає, що коли норма $\| \ \|_1$ є тривіальною, то норма $\| \ \|_2$ також буде тривіальною, а тому $\|x\|_2 = \|x\|_1^\alpha$ для довільного $\alpha > 0$. Припустимо тепер, що норма $\| \ \|_1$ не є тривіальною. Виберемо елемент y, для якого $\|y\|_1 > 1$, і розглянемо довільний ненульовий елемент x, для якого $\|x\|_1 \neq 1$. Із наслідку 6.1 тепер випливає, що тоді $\|y\|_2 > 1$ і для довільних цілих чисел m і n нерівності

$$\|x^m y^n\|_1 \geq 1 \quad \text{і} \quad \|x^m y^n\|_2 \geq 1$$

є рівносильними. Але тоді будуть рівносильними й нерівності

$$m \lg \|x\|_1 + n \lg \|y\|_1 \geq 0 \quad \text{і} \quad m \lg \|x\|_2 + n \lg \|y\|_2 \geq 0 \,.$$

Отже, для довільних $m, n \in \mathbb{Z}$, $m > 0$, маємо:

$$\frac{\lg \|x\|_1}{\lg \|y\|_1} \geq -\frac{n}{m} \iff \frac{\lg \|x\|_2}{\lg \|y\|_2} \geq -\frac{n}{m} \,.$$

Це можливо тоді й лише тоді, коли $\dfrac{\lg \|x\|_1}{\lg \|y\|_1} = \dfrac{\lg \|x\|_2}{\lg \|y\|_2}$ або, що рівносильно, коли $\dfrac{\lg \|x\|_2}{\lg \|x\|_1} = \dfrac{\lg \|y\|_2}{\lg \|y\|_1}$. Позначивши останнє відношення через α, отримуємо $\|x\|_2 = \|x\|_1^\alpha$ для всіх x, для яких $\|x\| \neq 1$.

Очевидно, що рівність $\|x\|_2 = \|x\|_1^\alpha$ буде виконуватись і для тих x, для яких $\|x\| = 1$. Крім того, числа $\lg \|x\|_1$ і $\lg \|x\|_2$ додатні, тому $\alpha > 0$. □

6.5 Неархімедові норми та метрики

У класичному математичному аналізі велику роль відіграє твердження, яке зазвичай називають *аксіомою Архімеда*:

для довільних дійсних чисел $a \neq 0$ і b знайдеться таке натуральне число n, що $|na| > |b|$.

Однак у сучасній математиці все більшого значення набувають нормовані поля, в яких ця аксіома не виконується[17].

Норма $\| \ \|$ в кільці K називається *неархімедовою*, якщо для довільних x і y виконується посилений варіант нерівності(N3):

[17] Зокрема, за останні п'ятдесят років розбудувався так званий *нестандартний* математичний аналіз з актуальними нескінченно малими та нескінченно великими величинами, який базується на неархімедовому розширенні поля дійсних чисел.

(N3′) $\|x+y\| \le \max(\|x\|, \|y\|)$[18].

Приклади неархімедових норм:

1. Тривіальне нормування, коли $\|x\| = 1$ для всіх $x \neq 0$.

2. Визначена у прикладі **5** на стор. 147 норма в кільці многочленів $P[x]$ (її неархімедовість випливає з того, що степінь суми двох многочленів не перевищує максимуму степенів доданків).

Твердження 6.9. *Нехай* $\| \ \|$ *— неархімедова норма на полі* P*. Тоді*

a) якщо $\|a\| \neq \|b\|$*, то* $\|a \pm b\| = \max(\|a\|, \|b\|)$;

b) множина $K = \{x \mid \|x\| \le 1\}$ *є кільцем, її підмножина* $I = \{x \mid \|x\| < 1\}$ *— максимальним ідеалом у* K*, а множина* $\{x \mid \|x\| = 1\}$ *— групою оборотних елементів кільця* K*.*

Доведення. a) Без обмеження загальності можна вважати, що $\|a\| < \|b\|$. Позаяк $\|b\| = \| - b\|$, то з умови (N3′) отримуємо:

$$\|a - b\| \le \max(\|a\|, \|b\|) = \|b\| \,.$$

Із другого боку,

$$\|b\| = \|a - (a - b)\| \le \max(\|a\|, \|a - b\|) \,,$$

і оскільки $\|a\| < \|b\|$, то $\|b\| \le \|a - b\|$. Отже,

$$\|a - b\| = \|b\| = \max(\|a\|, \|b\|) \,.$$

Рівність $\|a + b\| = \max(\|a\|, \|b\|)$ одержується з попередньої заміною b на $-b$.

b) Замкненість множини K відносно додавання, віднімання та множення випливає з умов (N2) і (N3′). Тому K є кільцем, причому з одиницею. Те, що підмножина I є ідеалом у K, також випливає з умови (N3′).

Позаяк ідеал I є власним (він не містить одиниці), то оборотних елементів із K він не містить. Із другого боку, для кожного елемента $a \in K \setminus I$ маємо $\|a\| = 1$. Але тоді з рівності

$$1 = \|1\| = \|a \cdot a^{-1}\| = \|a\| \cdot \|a^{-1}\|$$

[18] З означення неархімедової норми випливає, що від значень такої норми вимагається лише, щоб їх можна було порівнювати й множити. Тому поняття такої норми можна дуже узагальнити: замість $\mathbb{R}$ можна брати довільний лінійно впорядкований групоїд W із нулем, а під нормуванням кільця K розуміти відображення $x \mapsto \|x\|$ кільця K у множину $W_{\ge 0}$ невід'ємних елементів групоїда W, яке задовольняє умови (N1), (N2) і (N3′). Однак таке широке розуміння норми нам не знадобиться.

випливає, що $\|a^{-1}\| = 1$ і $a^{-1} \in K$. Тому будь-який елемент із $K \setminus I$ є оборотним. Отже, елемент $a \in K$ є оборотним тоді й лише тоді, коли $\|a\| = 1$.

Якщо ідеал J строго містить I, то він містить і елементи з $K \setminus I$, тобто оборотні. Але кожен ідеал, що містить оборотні елементи, збігається з усім кільцем. Тому ідеал I є максимальним. □

Метрика d на множині X називається *неархімедовою*, якщо виконується посилений варіант нерівності трикутника:

(М3′) $d(x,z) \le \max(d(x,y), d(y,z))$.

Легко перевіряється, що метрика на кільці, індукована неархімедовою нормою, також є неархімедовою (зробіть це!). Іншим важливим прикладом є метрика на множині X^ω усіх нескінченних послідовностей букв з алфавіту X, яка визначається так: беремо фіксоване число $\rho \in (0,1)$ і для довільних нескінченних послідовностей $u, v \in X^\omega$ кладемо $d(u,v) = \rho^k$, де k — довжина максимального спільного початку послідовностей u і v. Справді, якщо максимальним спільним початком послідовностей u і v є слово t довжини k, а послідовностей v і w — слово s довжини m, то $d(u,v) = \rho^k$ і $d(v,w) = \rho^m$. Припустимо, що $k \le m$ (випадок $k > m$ розбирається аналогічно). Тоді слово t є спільним початком послідовностей u і w (якщо $k = m$, то цей початок може не бути максимальним), а тому $d(u,w) \le \rho^k$. Разом із нерівністю $k \le m$ це дає:

$$d(u,w) \le \rho^k = \max(\rho^k, \rho^m) = \max(d(u,v), d(v,w))\,,$$

що й доводить неархімедовість метрики.

Властивості неархімедових просторів істотно відрізняються від властивостей звичних нам просторів з архімедовою метрикою.

Твердження 6.10. *Нехай X — метричний простір із неархімедовою метрикою d. Тоді*

a) усі трикутники в просторі X — рівносторонні або рівнобедрені, причому в останньому випадку основою є менша сторона;

b) центром кожної відкритої (замкненої) кулі є будь-яка її точка;

c) відкриті (замкнені) кулі даного радіуса r утворюють розбиття простору X.

Доведення. a) Нехай $d(x,y) \le d(y,z) \le d(z,x)$. Тоді з нерівності $d(z,x) \le \max(d(x,y), d(y,z))$ випливає, що $d(y,z) = d(z,x)$.

b) Нехай $B(a,r) = \{x \mid d(x,a) < r\}$ — відкрита куля радіуса r з центром у точці a, і $b \in B(a,r)$. Тоді для довільної точки $y \in B(b,r)$ із

нерівностей $d(y,b) < r$ і $d(b,a) < r$ випливає, що

$$d(y,a) \le \max(d(y,b), d(b,a)) < r.$$

Отже, $B(b,r) \subseteq B(a,r)$. Обернене включення доводиться аналогічно, тому $B(b,r) = B(a,r)$.

Для замкнених куль доведення аналогічне.

c) Із попереднього пункту випливає, що дві відкриті (замкнені) кулі даного радіуса або не перетинаються, або збігаються. □

6.6 Норми на $\mathbb{Q}$

Нехай p — фіксоване просте число. Для довільного ненульового цілого числа n через $\mathrm{ord}_p n$ позначимо показник степеня, із яким p входить у канонічний розклад числа n. Очевидно, що $\mathrm{ord}_p(nm) = \mathrm{ord}_p n + \mathrm{ord}_p m$.

Функцію ord_p можна поширити на множину ненульових раціональних чисел: для довільного раціонального числа $a = m/n$ покладемо $\mathrm{ord}_p(m/n) = \mathrm{ord}_p m - \mathrm{ord}_p n$. Легко перевіряється, що функція ord_p залежить від самого числа a, а не від його зображення у вигляді дробу: для дробу mk/nk маємо:

$$\mathrm{ord}_p \frac{mk}{nk} = \mathrm{ord}_p(mk) - \mathrm{ord}_p(nk) = (\mathrm{ord}_p m + \mathrm{ord}_p k) - (\mathrm{ord}_p n + \mathrm{ord}_p k) = \\ = \mathrm{ord}_p m - \mathrm{ord}_p n = \mathrm{ord}_p \frac{m}{n}.$$

Визначимо тепер на множині $\mathbb{Q}$ таку функцію:

$$|x|_p = \begin{cases} (1/p)^{\mathrm{ord}_p x}, & \text{якщо } x \neq 0; \\ 0, & \text{якщо } x = 0. \end{cases}$$

Теорема 6.9. *Функція $|x|_p$ є неархімедовою нормою на полі $\mathbb{Q}$.*

Доведення. Виконання умов (N1) і (N2) очевидне, тому перевіримо лише умову (N3′). Зрозуміло, що коли якесь із чисел x, y або $x+y$ дорівнює 0, то умова (N3′) виконується. Тому далі вважаємо, що жодне з чисел x, y і $x+y$ не є нулем. Нехай $x = a/b$, $y = c/d$. Оскільки для довільних цілих чисел m і n виконується нерівність $\mathrm{ord}_p(m+n) \ge \min(\mathrm{ord}_p m, \mathrm{ord}_p n)$, то

$$\mathrm{ord}_p(x+y) = \mathrm{ord}_p(ad+bc) - \mathrm{ord}_p(bc) \ge \\ \ge \min(\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)) - \mathrm{ord}_p b - \mathrm{ord}_p d = \\ = \min(\mathrm{ord}_p a + \mathrm{ord}_p d, \mathrm{ord}_p b + \mathrm{ord}_p c) - \mathrm{ord}_p b - \mathrm{ord}_p d = \\ = \min(\mathrm{ord}_p a - \mathrm{ord}_p b, \mathrm{ord}_p c - \mathrm{ord}_p d) = \min(\mathrm{ord}_p x, \mathrm{ord}_p y).$$

Тому

$$p^{\mathrm{ord}_p(x+y)} \geq p^{\min(\mathrm{ord}_p m, \mathrm{ord}_p n)} = \min(p^{\mathrm{ord}_p x}, p^{\mathrm{ord}_p y}).$$

Звідси

$$|x+y|_p = (1/p)^{\mathrm{ord}_p(x+y)} \leq \max(1/p^{\mathrm{ord}_p x}, 1/p^{\mathrm{ord}_p y}) = \max(|x|_p, |y|_p)\,. \ \square$$

Функція $|x|_p$ називається *p-адичною нормою* на полі $\mathbb{Q}$.

Твердження 6.11. *Якщо p і q — різні прості числа, то норми $|\ |_p$ і $|\ |_q$ на полі $\mathbb{Q}$ не еквівалентні.*

Доведення. Це випливає з наслідку 6.1 і того, що $\|p\|_p = \dfrac{1}{p} < 1$, $\|p\|_q = 1$. $\square$

Твердження 6.12. *Для кожного числа $\rho \in (0,1)$ функція $\|x\| = \rho^{\mathrm{ord}_p x}$ є нормою на полі $\mathbb{Q}$, еквівалентною нормі $|\ |_p$.*

Доведення. Виконання умов (N1) і (N2) очевидне, а виконання для функції $\|\ \|$ умови (N3′) випливає з доведеної вище нерівності

$$\mathrm{ord}_p(x+y) \geq \min(\mathrm{ord}_p x, \mathrm{ord}_p y).$$

Тому функція $\|\ \|$ є неархімедовою нормою на $\mathbb{Q}$.

Число ρ можна записати у вигляді $\rho = (1/p)^\alpha$, де $\alpha > 0$. Тоді $\|x\| = |x|_p^\alpha$ і еквівалентність норм випливає з твердження 6.8. $\square$

Теорема 6.10 (Островський[19])**.** *Із точністю до еквівалентності на полі $\mathbb{Q}$ є лише такі норми:*

a) тривіальна норма $\|x\| = 1$ (для $x \neq 0$);

b) архімедова норма $|x|$ (абсолютна величина);

c) неархімедова норма $|x|_p$ (p — просте число).

Доведення. Припустимо, що норма $\|\ \|$ — нетривіальна. Тоді можливі лише 2 випадки:

I. Існує таке натуральне число n, для якого $\|n\| > 1$. Нехай N — найменше з таких чисел. Оскільки $\|N\| > 1$, то існує таке додатне дійсне число α, що $\|N\| = N^\alpha$.

Кожне натуральне число n можна записати в системі числення з основою N:

$$n = a_0 + a_1 N + a_2 N^2 + \cdots + a_k N^k, \tag{6.12}$$

[19] Островський А.М. — вихованець відомої Київської алгебричної школи, створеної на початку XX ст. Д.О. Граве.

де $0 \le a_i < N$ і $a_k \ne 0$. Зауважимо, що з вибору N випливає, що $\|a_i\| \le 1$. Тоді

$$\|n\| \le \|a_0\| + \|a_1 N\| + \|a_2 N^2\| + \cdots + \|a_k N^k\| =$$
$$= \|a_0\| + \|a_1\| \cdot N^\alpha + \|a_2\| \cdot N^{2\alpha} + \cdots + \|a_k\| \cdot N^{k\alpha} \le$$
$$\le 1 + N^\alpha + N^{2\alpha} + \cdots + N^{k\alpha}.$$

Звідси, враховуючи, що $n \ge N^k$, отримуємо:

$$\|n\| \le N^{k\alpha}(1 + N^{-\alpha} + N^{-2\alpha} + \cdots + N^{-k\alpha}) <$$
$$< n^\alpha \Big(\sum\nolimits_{i=0}^{\infty} (1/N^\alpha)^i\Big) = c \cdot n^\alpha,$$

де $c = \sum_{i=0}^{\infty}(1/N^\alpha)^i$. Отже, для всіх натуральних n виконується нерівність $\|n\| < c \cdot n^\alpha$. Візьмемо довільне натуральне число m і підставимо в цю нерівність замість n число n^m. Отримуємо $\|n^m\| < c \cdot n^{m\alpha}$, звідки $\|n\| < \sqrt[m]{c} \cdot n^\alpha$. Позаяк це правильно для всіх m і $\lim\limits_{m\to\infty} \sqrt[m]{c} = 1$, то

$$\|n\| \le n^\alpha. \tag{6.13}$$

Доведемо тепер зворотну нерівність. Знову запишемо n у вигляді (6.12). Тоді $N^{k+1} > n$. Звідси

$$\|N^{k+1}\| = \|n + (N^{k+1} - n)\| \le \|n\| + \|N^{k+1} - n\|,$$

звідки

$$\|n\| \ge \|N^{k+1}\| - \|N^{k+1} - n\| \ge N^{(k+1)\alpha} - (N^{k+1} - n)^\alpha$$

(на останньому кроці ми скористалися рівністю $\|N\| = N^\alpha$ і нерівністю (6.13)). Ураховуючи, що $N^{k+1} > n \ge N^k$, звідси отримуємо:

$$\|n\| \ge N^{(k+1)\alpha} - N^{(k+1)\alpha}\Big(1 - \frac{n}{N^{k+1}}\Big)^\alpha \ge N^{(k+1)\alpha} - N^{(k+1)\alpha}\Big(1 - \frac{1}{N}\Big)^\alpha =$$
$$= N^{(k+1)\alpha}\Big(1 - \Big(1 - \frac{1}{N}\Big)^\alpha\Big) > n^\alpha \cdot d,$$

де $d = 1 - \big(1 - \frac{1}{N}\big)^\alpha$. Повторюючи попередні міркування з підстановкою замість n числа n^m, отримуємо, що $\|n\| \ge n^\alpha$.

Отже, $\|n\| = n^\alpha$ для всіх натуральних n. Тоді для довільного раціонального $\frac{n}{m}$ маємо такий ланцюжок імплікацій:

$$\frac{n}{m} \cdot m = n \;\Rightarrow\; \Big\|\frac{n}{m}\Big\| \cdot \|m\| = \|n\| \;\Rightarrow\; \Big\|\frac{n}{m}\Big\| = \frac{\|n\|}{\|m\|} = \frac{|n|^\alpha}{|m|^\alpha} = \Big|\frac{n}{m}\Big|^\alpha.$$

Таким чином, для всіх $x \in \mathbb{Q}$ виконується рівність $\|x\| = |x|^\alpha$. Тому, за твердженням 6.8, норми $\| \ \|$ і $|\ |$ еквівалентні.

II. Для всіх натуральних n виконується нерівність $\|n\| \leq 1$. Із нетривіальності норми й рівності $\left\|\frac{n}{m}\right\| = \frac{\|n\|}{\|m\|}$ випливає, що існують натуральні n, для яких $\|n\| < 1$. Нехай p — найменше з таких чисел.

Число p має бути простим. Справді, у противному разі з рівності $p = m \cdot k$ (де $m, k < p$) випливало б, що $\|p\| = \|m\| \cdot \|k\| = 1 \cdot 1 = 1$.

Покажемо тепер, що для всіх простих $q \neq p$ виконується рівність $\|q\| = 1$. Справді, припустимо, що $\|q\| < 1$. Виберемо таке велике число k, щоб виконувалися нерівності $\|p\|^k < 1/2$, $\|q\|^k < 1/2$. Позаяк числа p^k і q^k взаємно прості, то існують такі u і v, що $up^k + vq^k = 1$. Тоді

$$1 = \|1\| = \|up^k + vq^k\| \leq \|up^k\| + \|vq^k\| =$$
$$= \|u\| \cdot \|p^k\| + \|v\| \cdot \|q^k\| \leq \|p^k\| + \|q^k\| < \frac{1}{2} + \frac{1}{2} = 1.$$

Отримана суперечність доводить, що $\|q\| = 1$.

Із мультиплікативності норми випливає, що для довільного натурального числа $n = p^k \cdot m$, де m не ділиться на p, виконується рівність $\|n\| = \|p\|^k$. Ураховуючи ще рівність $\left\|\frac{n}{m}\right\| = \frac{\|n\|}{\|m\|}$, отримуємо, що для довільного раціонального числа x

$$\|x\| = \|p\|^{\mathrm{ord}_p x}. \tag{6.14}$$

Оскільки існує таке додатне дійсне число α, що $\|p\| = (1/p)^\alpha$, то $\|x\| = |x|_p^\alpha$ і за твердженням 6.8 норми $\| \ \|$ і $|\ |_p$ еквівалентні. □

Зауважимо, що для поля $\mathbb{Q}$ вибір у кожному класі еквівалентних норм певного канонічного представника (модуля числа в класі архімедових норм і норм $|\ |_p$ в інших класах) має, крім історичної традиції, й інші підстави. Зокрема, при такому виборі представників еквівалентних норм для кожного ненульового числа $x \in \mathbb{Q}$ добуток $\prod \|x\|$ усіх його норм буде дорівнювати 1.

6.7 Поле p-адичних чисел $\mathbb{Q}_p$

Ми вже знаємо, що коли застосувати до поля $\mathbb{Q}$ з нормою $|\ |$ конструкцію Кантора, то одержимо поле $\mathbb{R}$ дійсних чисел. А що буде, коли застосувати цю конструкцію до поля $\mathbb{Q}$ з нормою $|\ |_p$? Виявляється, що в цьому випадку з'являється вже відоме нам поле $\mathbb{Q}_p$ p-адичних чисел. Обґрунтуванню цього факту і присвячено цей розділ.

Отже, нехай норма на полі $\mathbb{Q}$ є p-адичною. Його поповнення за допомогою конструкції Кантора позначимо $\overline{(\mathbb{Q}, |\ |_p)}$. Розглянемо довільний елемент

$$\alpha_{-k}p^{-k}+\alpha_{-(k-1)}p^{-(k-1)}+\cdots+\alpha_{-1}p^{-1}+\alpha_0+\alpha_1 p+\cdots+\alpha_n p^n+\cdots\,, \quad (6.15)$$

поля $\mathbb{Q}_p$ p-адичних чисел. Усі члени цієї суми є раціональними числами, тому її можна розглядати як ряд над полем $\mathbb{Q}$. Легко бачити, що послідовність

$$\alpha_{-k}p^{-k},\ \ \alpha_{-k}p^{-k}+\alpha_{-(k-1)}p^{-(k-1)},\ \ldots,\ \alpha_{-k}p^{-k}+\cdots+\alpha_n p^n,\ \ldots \quad (6.16)$$

часткових сум цього ряду є фундаментальною відносно норми $|\ |_p$. Тому в полі $\overline{(\mathbb{Q}, |\ |_p)}$ цей ряд збігається до деякого елемента a. Якщо тепер кожному ряду (6.15) поставити у відповідність його суму, то отримаємо відображення χ поля $\mathbb{Q}_p$ в поле $\overline{(\mathbb{Q}, |\ |_p)}$. Із вправи 6.5 випливає навіть, що це відображення буде гомоморфізмом полів.

Якщо $\alpha_{-k} \neq 0$, то норма кожного члена послідовності (6.16) дорівнює p^k. Тоді за твердженням 6.7.c норма границі цієї послідовності (тобто суми ряду (6.15) (6.15)) також дорівнює p^k. Отже, при гомоморфізмі $\chi : \mathbb{Q}_p \to \overline{(\mathbb{Q}, |\ |_p)}$ ненульові елементи переходять у ненульові. Тому цей гомоморфізм є ін'єктивним.

Для завершення доведення ізоморфізму полів $\overline{(\mathbb{Q}, |\ |_p)}$ і $\mathbb{Q}_p$ лишилося показати, що гомоморфізм χ є сюр'єктивним, тобто що кожен елемент поля $\overline{(\mathbb{Q}, |\ |_p)}$ є сумою деякого ряду (6.15).

Дві фундаментальні відносно норми $|\ |_p$ послідовності елементів поля $\mathbb{Q}$ назвемо *еквівалентними*, якщо їх різниця збігається до нуля. Тоді поле $\overline{(\mathbb{Q}, |\ |_p)}$ — це множина класів еквівалентних фундаментальних послідовностей. Спочатку покажемо, що в кожному класі еквівалентності можна вибрати канонічного представника[20].

Твердження 6.13. *Нехай $(a^n)_{n\in\mathbb{N}}$ — фундаментальна відносно p-адичної норми послідовність раціональних чисел, яка не збігається до нуля. Тоді існує таке натуральне число k, що*

$$|a_k|_p = |a_{k+1}|_p = |a_{k+2}|_p = \cdots\,.$$

Доведення. Оскільки послідовність $(a^n)_{n\in\mathbb{N}}$ не збігається до нуля, то існує таке $\varepsilon > 0$, що для кожного натурального числа n знайдеться такий номер $m > n$, що $|a_m|_p > \varepsilon$. З іншого боку, із фундаментальності

[20] У якому сенсі канонічного, це ми уточнимо трохи пізніше.

цієї послідовності випливає існування такого N, що для всіх $u, v > N$ виконується нерівність $|a_u - a_v|_p < \varepsilon$. Виберемо тепер таке $k > N$, що $|a_k|_p > \varepsilon$. Тоді для всіх $m > k$ буде $|a_m - a_k|_p < \varepsilon$. Зокрема, $|a_m - a_k|_p \neq |a_k|_p$. Тому за твердженням 6.9.а для всіх $m > k$ маємо:

$$|a_m|_p = |a_k + (a_m - a_k)|_p = \max(|a_k|_p, |a_m - a_k|_p) = |a_k|_p\,. \qquad \square$$

Змінивши, у разі потреби, кілька перших членів (що не впливає на збіжність послідовності та її границю), можемо далі вважати, що

$$|a_1|_p = |a_2|_p = |a_3|_p = |a_4|_p = \cdots = (1/p)^m\,.$$

Тоді для послідовності $b_n = p^{-m}a_n$ матимемо:

$$|b_n|_p = |p^{-m}a_n|_p = |p^{-m}|_p \cdot |a_n|_p = p^m \cdot (1/p)^m = 1\,.$$

Запишемо b_n у вигляді $b_n = u_n/v_n$, де дріб u_n/v_n — нескоротний. Із рівності $|b_n|_p = 1$ випливає, що кожне з чисел u_n і v_n взаємно просте з p. Зокрема, існує таке ціле число w_n, що $w_n v_n \equiv 1 \pmod{p^n}$. Покладемо $d_n = u_n w_n \bmod p^n$. Тоді будемо мати:

$$d_n - b_n = (u_n w_n + tp^n) - \frac{u_n}{v_n} = \frac{u_n(w_n v_n - 1) + v_n t p^n}{v_n}\,.$$

Оскільки $w_n v_n - 1$ ділиться на p^n, а v_n взаємно просте з p, то $\operatorname{ord}_p(d_n - b_n) \geq n$, а тому $|d_n - b_n|_p \leq 1/p^n$. Отже, послідовність $(d_n - b_n)_{n\in\mathbb{N}}$ збігається до нуля, а тому послідовності $(b_n)_{n\in\mathbb{N}}$ і $(d_n)_{n\in\mathbb{N}}$ — еквівалентні. Крім того, із нерівності $|b_n|_p \neq |d_n - b_n|_p$ випливає, що

$$|d_n|_p = |b_n + (d_n - b_n)|_p = |b_n|_p = 1.$$

Отримані результати можна підсумувати у вигляді такого твердження:

Твердження 6.14. *Якщо фундаментальна відносно p-адичної норми послідовність $(a^n)_{n\in\mathbb{N}}$ раціональних чисел не є збіжною до нуля, то вона еквівалентна деякій фундаментальній послідовності $(p^m d_n)_{n\in\mathbb{N}}$, де число m фіксоване, а d_n для кожного n є цілим числом із проміжку $[0, p^n)$ і задовольняє умову $|d_n|_p = 1$.*

Розберемося докладніше, якими мають бути члени послідовності $(d_n)_{n\in\mathbb{N}}$. Із її фундаментальності випливає, що для кожного натурального числа k існує такий номер N, що для всіх $l, m > N$ виконується нерівність $|d_l - d_m|_p < 1/p^k$. Тобто число $d_l - d_m$ має ділитися принаймні

на p^{k+1}. Це означає, що коли записати кожне d_n у системі числення з основою p:

$$d_n = \alpha_0^{(n)} + \alpha_1^{(n)} p + \alpha_2^{(n)} p^2 + \cdots + \alpha_{k(n)}^{(n)} p^{k(n)},$$

то для всіх $n > N$ коефіцієнти $\alpha_0^{(n)}$, $\alpha_1^{(n)}$, $\ldots$, $\alpha_k^{(n)}$ не залежать від n. Тобто для довільного i послідовність $(\alpha_i^{(n)})_{n\in\mathbb{N}}$, починаючи з певного місця, стабілізується. Значення, на якому вона стабілізується, позначимо α_i.

Розглянемо тепер послідовність

$$\widetilde{d_0} = \alpha_0, \quad \widetilde{d_1} = \alpha_0 + \alpha_1 p, \quad \ldots, \quad \widetilde{d_n} = \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n, \quad \ldots . \tag{6.17}$$

Вона еквівалентна послідовності $(d_n)_{n\in\mathbb{N}}$. Справді, позначимо через $n(i)$ номер, починаючи з якого члени послідовності $(\alpha_i^{(n)})_{n\in\mathbb{N}}$ дорівнюють α_i. Нехай $N_k = \max(n(0), n(1), \ldots, n(k))$. Тоді для всіх $n > N_k$

$$d_n = \alpha_0 + \alpha_1 p + \cdots + \alpha_k p^k + \cdots + \alpha_{k(n)}^{(n)} p^{k(n)},$$

звідки $|d_n - \widetilde{d_n}|_p < 1/p^k$. Позаяк k довільне, то це означає, що послідовність $d_n - \widetilde{d_n}$ збігається до нуля.

Із доведеного випливає, що послідовність $(p^m \widetilde{d_n})_{n\in\mathbb{N}}$ буде еквівалентною послідовності $(p^m d_n)_{n\in\mathbb{N}}$, а тим самим і послідовності $(a_n)_{n\in\mathbb{N}}$. Послідовність $(p^m \widetilde{d_n})_{n\in\mathbb{N}}$ і будемо вважати канонічним представником того класу еквівалентних фундаментальних послідовностей, який містить $(a_n)_{n\in\mathbb{N}}$.

З іншого боку, послідовність $(p^m \widetilde{d_n})_{n\in\mathbb{N}}$ є послідовністю часткових сум ряду

$$\alpha_0 p^m + \alpha_1 p^{m+1} + \alpha_2 p^{m+2} + \cdots + \alpha_k p^{m+k} + \cdots, \tag{6.18}$$

тому вона збігається до суми цього ряду. Це завершує доведення того, що кожен елемент поля $\overline{(\mathbb{Q}, |\ |_p)}$ є сумою деякого ряду вигляду (6.15).

Таким чином, ми довели таку теорему:

Теорема 6.11. *Кожен ненульовий елемент a із поповнення $\overline{(\mathbb{Q}, |\ |_p)}$ поля $\mathbb{Q}$ з p-адичною нормою однозначно записується у вигляді*

$$a = \sum_{k=m}^{\infty} \alpha_k p^k, \quad \text{де } m \in \mathbb{Z}, \quad \alpha_m \neq 0 \quad i \quad 0 \leq \alpha_k < p \quad \text{для всіх } k. \tag{6.19}$$

При такому записі елементів поповнення $\overline{(\mathbb{Q}, |\ |_p)}$ воно ототожнюється з полем $\mathbb{Q}_p$ p-адичних чисел.

Зауваження. **1**. Якщо елемент $a \in \mathbb{Q}_p$ має такий вигляд, як у (6.19), то $|a|_p = (1/p)^m$.

2. Кільце $\mathbb{Z}_{(p)}$ цілих p-адичних чисел збігається з множиною $\{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$. Якщо елемент $a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$ кільця $\mathbb{Z}_{(p)}$ ототожнити з послідовністю $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ його коефіцієнтів, то $\mathbb{Z}_{(p)}$ можна ототожнити з множиною X^ω усіх нескінченних послідовностей букв з алфавіту $X = \{0, 1, \ldots, p-1\}$. Тоді p-адична метрика на $\mathbb{Z}_{(p)}$ збігається з метрикою на X^ω, визначеною на стор. 153.

6.8 Топологія поля $\mathbb{Q}_p$

Топологічне поле називається *локально компактним*, якщо існує окіл нуля, замикання якого є компактним.

Теорема 6.12. *Локально компактне нормоване поле P є повним.*

Доведення. Нехай $(a_n)_{n\in\mathbb{N}}$ — послідовність Коші елементів поля P і U — такий окіл нуля, замикання $\overline{U}$ якого є компактним. Із відкритості U випливає існування такого $\varepsilon > 0$, що множина $\{a \in P \mid \|a\| < \varepsilon\}$ міститься в U. Тоді з означення послідовності Коші випливає існування такого N, що $a_m - a_N \in U$ для всіх $m > N$. Послідовність $(a_n - a_N)_{n\in\mathbb{N}}$ також є послідовністю Коші. У компактній множині кожна нескінченна підмножина має граничну точку. Тому з компактності $\overline{U}$ випливає існування підпослідовності $a_{m_1} - a_N$, $m_{p_2} - a_N$, …, яка збігається до деякого $b \in \overline{U}$. Тоді за твердженням 6.7.b послідовність $(a_n - a_N)_{n\in\mathbb{N}}$ також збігається до b. А звідси вже випливає, що $\lim\limits_{n\to\infty} a_n = b + a_N$. □

Для кожного фіксованого цілого числа m позначимо через U_m множину p-адичних чисел вигляду $a = \sum_{k=m}^{\infty} \alpha_k p^k$. Оскільки для кожного такого числа a

$$|a|_p \leq (1/p)^m < (1/p)^{m-1},$$

то U_m є околом нуля.

Вправа 6.6. *Доведіть, що $U_m + U_m = U_m$.*

Твердження 6.15. *Для кожного m множина U_m і її доповнення $\overline{U_m} = \mathbb{Q}_p \setminus U_m$ є замкненими (отже, і відкритими) підмножинами поля $\mathbb{Q}_p$.*

Доведення. Із доведення твердження 6.13 видно, що воно є правильним для довільних послідовностей Коші елементів поля $\mathbb{Q}_p$. Звідси і з

твердження 6.7.c випливає, що норма границі кожної збіжної послідовності елементів із U_m не перевищує $(1/p)^m$. А тому така послідовність збігається до елемента з U_m, що й доводить замкненість U_m.

Припустимо тепер, що послідовність Коші $(a_n)_{n\in\mathbb{N}}$ елементів із $\overline{U_m}$ збігається до деякого елемента $a \in U_m$. Тоді з тверджень 6.7.c і 6.13 випливає, що майже для всіх членів послідовності $(a_n)_{n\in\mathbb{N}}$ виконується рівність $|a_n|_p = |a|_p$. Але тоді з нерівності $|a|_p \leq (1/p)^m$ випливає, що майже всі члени послідовності $(a_n)_{n\in\mathbb{N}}$ належать множині U_m, що суперечить умові. Тому послідовність елементів з $\overline{U_m}$ може збігатися лише до елемента з $\overline{U_m}$. Отже, множина $\overline{U_m}$ також є замкненою.

Відкритість множин U_m і $\overline{U_m}$ тепер випливає з того, що кожна з них є доповненням другої. □

Зокрема, із твердження 6.15 одразу випливає, що поле $\mathbb{Q}_p$ є незв'язним.

Твердження 6.16. *Для кожного m множина U_m є компактною.*

Доведення. Компактність рівносильна тому, що кожна нескінченна підмножина має граничну точку. Нехай M — нескінченна підмножина з U_m. Кожен елемент $a \in M$ запишемо у вигляді $a = \sum_{k=m}^{\infty} \alpha_k p^k$. Оскільки для елементів із M коефіцієнт α_m може набувати щонайбільше p різних значень, то існує значення, яке набувається нескінченно багато разів. Нехай це α'_m. Множину тих елементів із M, для яких $\alpha_m = \alpha'_m$, позначимо M_m.

А далі міркуємо аналогічно. Коефіцієнт α_{m+1} елементів з M_m може набувати щонайбільше p різних значень. Тому існує значення, яке набувається нескінченно багато разів. Нехай це α'_{m+1}. Множину тих елементів із M_m, для яких $\alpha_{m+1} = \alpha'_{m+1}$, позначимо M_{m+1}. І т. д.

Легко бачити, що елемент $a' = \sum_{k=m}^{\infty} \alpha'_k p^k$ є граничною точкою множини M. □

Наслідок 6.2. *Кільце $\mathbb{Z}_{(p)}$ цілих p-адичних чисел є компактним.*

Доведення. Це випливає з рівності $\mathbb{Z}_{(p)} = U_1$ і твердження 6.16. □

Наслідок 6.3. *Поле $\mathbb{Q}_p$ p-адичних чисел є локально компактним.*

Доведення. Це випливає з твердження 6.16 і того, що кожна з множин U_m є околом нуля. □

Твердження 6.17. *Поле $\mathbb{Q}_p$ є скрізь розривним* (тобто не містить неодноелементних зв'язних підмножин).

Доведення. Нехай підмножина $M \subseteq \mathbb{Q}_p$ містить більше одного елемента. Виберемо в M певний елемент a і розглянемо множину

$$M' = M - a = \{x - a \mid x \in M\}.$$

Візьмемо в M' довільний ненульовий елемент b і виберемо ціле число m так, щоб виконувалася нерівність $(1/p)^m < |b|_p$. Тоді за твердженням 6.15 обидві компоненти розбиття

$$M' = (M' \cap U_m) \cup (M' \cap \overline{U_m})$$

є відкритими множинами, причому непорожніми: $M' \cap U_m$ містить 0, а $M' \cap \overline{U_m}$ містить b.

Отже, множина M' є незв'язною. Але тоді незв'язною буде і множина M, бо за теоремою 6.7 відображення $M' \to M$, $y \mapsto y + a$, є гомеоморфізмом. □

6.9 Задачі

1. Доведіть, що кожен ненульовий ендоморфізм групи $\mathbb{C}_{p^\infty}$ є сюр'єктивним.
2. Нехай A — область цілісності, а S — група всіх оборотних елементів з A. Доведіть, що кільце часток AS^{-1} збігається з A.
3. Доведіть, що кільце часток $\mathbb{Z}_6 S^{-1}$, де $S = \{1, 2, 4\}$, ізоморфне полю $\mathbb{Z}_3$.
4. a) Доведіть, що для довільних монотонної функції $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ і неархімедової метрики d на множині X функція $d'(x, y) = f(d(x, y))$ також буде неархімедовою метрикою на X.

   b) Покажіть, що для архімедових метрик попереднє твердження не є правильним.
5. Доведіть, що для довільної метрики d на множині X функція $d_1(x, y) = \frac{d(x,y)}{1+d(x,y)}$ також буде метрикою.
6. Доведіть, що на скінченному полі існує лише одна норма — тривіальна.
7. Доведіть, що на полі ненульової характеристики не можна визначити архімедову норму.
8. У полі $\mathbb{Q}$ з нормою $|\ |_p$ знайдіть найменший радіус кулі, яка містить усі цілі числа.
9. Доведіть, що множина $P((x))$ рядів Лорана з коефіцієнтами з поля P (тобто формальних рядів вигляду $\sum_{n \in \mathbb{Z}} a_n x^n$, які містять лише скінченну кількість ненульових доданків із від'ємними показниками) утворює поле відносно звичайних додавання та множення рядів і що це поле ізоморфне полю часток кільця $P[[x]]$ формальних степеневих рядів із коефіцієнтами з поля P.

10. Нехай $a \in (0,1)$, P — поле, а K — одне з кілець $P[x]$, $P[[x]]$ або $P((x))$ (див. задачу 9). Для довільного ненульового многочлена (ряду) $f(x) \in K$ через $\omega(f)$ позначимо показник найменшого степеня змінної x, який зустрічається в запису $f(x)$ із ненульовим коефіцієнтом. Доведіть, що $\|f(x)\| = a^{\omega(f)}$ є неархімедовою нормою на K.

11. Доведіть, що норма $\|\ \|$ на полі P характеристики 0 буде неархімедовою тоді і тільки тоді, коли для кожного цілого числа n виконується нерівність $\|n\| \leq 1$.

12. Доведіть, що на полі P дві еквівалентні норми $\|\ \|_1$ і $\|\ \|_2$ або обидві архімедові, або обидві неархімедові.

13.* Доведіть, що норми $\|\ \|_1$ і $\|\ \|_2$ на полі P будуть еквівалентними тоді й лише тоді, коли $\{x \in F \mid \|x\|_1 < 1\} = \{x \in F \mid \|x\|_2 < 1\}$.

14. a) Нехай $\alpha > 0$ — фіксоване дійсне число. Для довільного $x \in \mathbb{Q}$ покладемо $\|x\| = |x|^\alpha$, де $|\ |$ — звичайна абсолютна величина. Доведіть, що $\|\ \|$ буде нормою на $\mathbb{Q}$ тоді й лише тоді, коли $\alpha \leq 1$.

    b) Аналогічне завдання для поля $\mathbb{R}$.

15. Доведіть, що коли $\alpha < 0$, то функція $\|x\| = |x|^\alpha$ не є нормою на $\mathbb{Q}$.

16. Доведіть, що для кожної архімедової норми $\|\ \|$ на полі $\mathbb{Q}$ можна вказати таке дійсне число $a \in (0,1]$, що $\|x\| = |x|^a$ для всіх $x \in \mathbb{Q}$.

17. Нехай $x \in \mathbb{Q}$. Доведіть, що коли для всіх простих p виконується нерівність $|x|_p \leq 1$, то $x \in \mathbb{Z}$.

18. Обчисліть: a) $\operatorname{ord}_2 124$; b) $\operatorname{ord}_3 333$; c) $\operatorname{ord}_5 0{,}0125$; d) $\operatorname{ord}_2 0{,}0125$; e) $\operatorname{ord}_3 123456$; f) $\operatorname{ord}_3(-13{,}23)$; g) $\operatorname{ord}_5(-13{,}23)$; h) $\operatorname{ord}_7(-13{,}23)$; i) $\operatorname{ord}_{11}(-13{,}23)$; j) $\operatorname{ord}_3 10!$; k) $\operatorname{ord}_2 9!$; l) $\operatorname{ord}_3\left((9!)^2/3^9\right)$; m) $\operatorname{ord}_2\left(2^{2^n}/2^n\right)$; n) $\operatorname{ord}_2\left(2^{2^n}/(2^n)!\right)$; o) $\operatorname{ord}_p(p^k!)$.

19. Нехай $0 < a < p$. Доведіть, що $\operatorname{ord}_p(ap^k!) = a(1 + p + p^2 + \cdots + p^{k-1})$.

20.* Нехай $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ — запис натурального числа n у системі числення з основою p. Доведіть, що $\operatorname{ord}_p(n!) = \dfrac{n - s_n}{p-1}$, де $s_n = a_0 + \cdots + a_k$ — сума цифр числа n.

21. Обчисліть перші п'ять коефіцієнтів p-адичного розкладу числа:

    a) $0.12022\ldots \cdot 2.0112\ldots$ $(p = 3)$; b) $(0.13212\ldots)^{-1}$ $(p = 5)$;

    c) $0.012 - 25.431\ldots$ $(p = 7)$.

22. Запишіть число a як елемент $a = \alpha_{-k}\ldots\alpha_{-1}.\alpha_0\alpha_1\alpha_2\ldots$ поля p-адичних чисел:

    a) $a = \frac{2}{3}$, $p = 2$; b) $a = \frac{1}{5}$, $p = 3$; c) $a = \frac{1}{100}$, $p = 5$; d) $a = \frac{1}{100}$, $p = 3$; e) $a = -\frac{1}{5}$, $p = 3$; f) $a = -\frac{2}{3}$, $p = 5$; g) $a = -\frac{3}{5}$, $p = 7$; h) $a = \frac{1}{4!}$, $p = 2$; i) $a = \frac{1}{5!}$, $p = 5$; j) $a = \frac{1}{6!}$, $p = 3$.

23. Доведіть, що p-адичне число $\alpha_k p^k + \alpha_{k+1} p^{k+1} + \alpha_{k+2} p^{k+2} + \cdots$ буде раціональним тоді й лише тоді, коли послідовність його коефіцієнтів α_k, α_{k+1}, α_{k+2}, $\ldots$ буде, починаючи з певного місця, періодичною.

24. Доведіть, що p-адичний розклад числа $a \in \mathbb{Q}_p$ буде скінченним тоді й лише тоді, коли a є додатним раціональним числом із знаменником, який є степенем p.

25. Доведіть, що поле $\mathbb{R}$ не ізоморфне жодному полю $\mathbb{Q}_p$.

26. Доведіть, що коли $p \neq q$, то поля $\mathbb{Q}_p$ і $\mathbb{Q}_q$ не ізоморфні.

27. Доведіть, що єдиним автоморфізмом поля $\mathbb{Q}_p$ є тотожний автоморфізм.

28. Доведіть, що кожна послідовність цілих чисел містить підпослідовність Коші відносно норми $|\ |_p$.

29.* Доведіть, що кожна послідовність цілих p-адичних чисел містить збіжну відносно норми $|\ |_p$ підпослідовність.

30. З'ясуйте, чи буде послідовність $(p^n)_{n\geq 0}$ збіжною в полі $\mathbb{Q}_p$, і в разі позитивної відповіді знайдіть границю.

31. Доведіть, що ряд $a_1 + a_2 + a_3 + \cdots$ елементів поля $\mathbb{Q}_p$ збігається тоді й лише тоді, коли послідовність $(a_n)_{n\geq 1}$ його членів збігається до 0.

32. Нехай $x \in \mathbb{Q}$. Знайдіть необхідну й достатню умову для того, щоб виконувалася рівність $\lim\limits_{n\to\infty} \left|\frac{x^n}{n!}\right|_p = 0$.

33. Знайдіть у полі $\mathbb{Q}_p$ суму ряду:
    a) $1 + p + p^2 + p^3 + p^4 + p^5 + \cdots$;
    b) $1 - p + p^2 - p^3 + p^4 - p^5 + \cdots$;
    c) $1 + (p-1)p + p^2 + (p-1)p^3 + p^4 + (p-1)p^5 + \cdots$.

34. Доведіть, що в полі $\mathbb{Q}$ з нормою $|\ |_p$ дана послідовність не є збіжною:
    a) $a_n = n$; b)* $a_n = 1 + p^{1!} + p^{2!} + \cdots + p^{n!}$.

35.* Нехай m — натуральне число, взаємно просте з p. Доведіть, що в полі p-адичних чисел послідовність $(m^{p^n})_{n\geq 1}$ є збіжною.

36. Доведіть, що в кільці цілих 7-адичних чисел $\sqrt{2}$ і $\sqrt{11}$ існують, а $\sqrt{3}$ і $\sqrt{5}$ — не існують.

37. Доведіть, що в кільці цілих 11-адичних чисел $\sqrt{3}$ і $\sqrt{5}$ існують, а $\sqrt{2}$ і $\sqrt{7}$ — не існують.

38. Для яких простих чисел p з інтервалу $(1, 25)$ у полі $\mathbb{Q}_p$ можна добути квадратний корінь з -1?

39. Обчисліть перші п'ять знаків числа $\sqrt{-1}$ у полі a) $\mathbb{Q}_5$, b) $\mathbb{Q}_{13}$.

40. Нехай $p > 2$, а m — квадратичний лишок за модулем p. Доведіть, що в полі p-адичних чисел існують два різні квадратні корені з числа m.

41. Обчисліть у полі $\mathbb{Q}_2$ перші 6 знаків числа $\sqrt{-7}$.

42. З'ясуйте, чи існує в полі $\mathbb{Q}_{13}$ квадратний корінь із числа a) 5, b) 10, c) -10, d) 0.43271, e) 0.51209, f) 41.21, g) 4.121, h) 7^5, i) $3 - 5 \cdot 13^2$.

43. Нехай p — непарне просте число. Доведіть, що можна вибрати такі чотири натуральні числа a_1, a_2, a_3 і a_4, що для кожного ненульовового $c \in \mathbb{Q}_p$ рівно одне з чисел a_1c, a_2c, a_3c і a_4c має в полі $\mathbb{Q}_p$ квадратний корінь.

44. Нехай p — непарне просте число. Доведіть, що в полі p-адичних чисел існує лише один корінь степеня p з одиниці.

45.* Доведіть, що для кожного простого числа p многочлен $x^p - x$ має в полі $\mathbb{Q}_p$ рівно p різних коренів.

46. Доведіть, що кільце $\mathbb{Z}$ є скрізь щільною підмножиною кільця $\mathbb{Z}_{(p)}$.

47. Доведіть, що поле $\mathbb{Q}$ є скрізь щільною підмножиною поля $\mathbb{Q}_p$.

Відповіді та вказівки

Глава 1. **3.** Тільки A і $\varnothing$. *Вказівка.* A не містить нетривіальних інваріантних підмножин. **5.** a),b) 0, V; c) всі підпростори. **6.** *Вказівка.* Нехай $\langle A;(\omega_i)_{i\in I}\rangle$ — алгебра. Візьмемо довільний $a\in A$ і визначимо: $B_0=\{a\}$, $B_{n+1}=B_n\cup\bigcup_{i\in I}\omega_i(B_n)$. Тоді $B=\bigcup_n B_n$ — не більше ніж зліченна підалгебра. **8.** *Вказівка.* Нехай d — НСД елементів підалгебри $A\subseteq\langle\mathbb{N};+\rangle$ і $a_1,\dots,a_k$ — набір елементів з A, НСД яких дорівнює d. Покажіть, що $\langle a_1,\dots,a_k\rangle$ містить майже всі елементи, кратні d, а тому A має скінченну систему твірних. **11.** *Вказівка.* Якщо $\langle X\smallsetminus\{b\}\rangle\neq\mathcal{A}$, то $\langle X\smallsetminus\{b\}\rangle$ міститься в деякій максимальній підалгебрі C. Оскільки $b\in C$, то $\langle X\rangle\subseteq C\neq\mathcal{A}$. **17.** *Вказівка.* Використайте задачу 1.16 і те, що деморганівський добуток двох відношень еквівалентності буде відношенням еквівалентності тоді й лише тоді, коли вони комутують. **19.** *Вказівка.* b) Розгляньте гомоморфізм $\varphi: A\to A/\theta_1\times A/\theta_2$, $a\mapsto(\overline{a}_{\theta_1},\overline{a}_{\theta_2})$. Із $\theta_1\cap\theta_2=\mathbf{o}_A$ випливає ін'єктивність φ. Нехай тепер $(\overline{a'}_{\theta_1},\overline{a''}_{\theta_2})\in A/\theta_1\times A/\theta_2$. Тоді існує такий a, що $(a',a)\in\theta_1$, $(a,a'')\in\theta_2$, звідки $(\overline{a'}_{\theta_1},\overline{a''}_{\theta_2})=(\overline{a}_{\theta_1},\overline{a}_{\theta_2})$. **22.** Ні. *Вказівка.* На множині $\mathbb{Z}_n$ визначимо унарну операцію $x^*=(x+1)\bmod n$. Тоді всі алгебри $\langle\mathbb{Z}_n;{}^*\rangle$ — скінченні, а $A=\prod_n(\mathbb{Z}_n;{}^*)$ не містить скінченних підалгебр. **23.** *Вказівка.* У нетривіальному підпрямому розкладі всі множники будуть абелевими. **24.** Тільки C_{p^n} і C_{p^∞}. *Вказівка.* Усі елементи повинні мати скінченний порядок, причому серед простих дільників порядків елементів не може бути різних.

Глава 2. **1.**

	0	a
0	0	0
a	0	0

,

	1	a
1	1	a
a	a	1

,

	0	1
0	0	0
1	0	1

,

	a	b
a	a	a
b	b	b

,

	a	b
a	a	b
b	a	b

.

Дві останні напівгрупи антизоморфні. **2**. b) Тоді й лише тоді, коли елемент a — оборотний. **3**. *Вказівка.* Розгляньте нескінченний в обидва боки ланцюг. **4.** a) $\binom{n}{i}^2 i!$; b) $\mathrm{S}(n,i)\frac{n!}{(n-i)!}$; c) $\mathrm{S}(n+1,i+1)\frac{n!}{(n-i)!}$, (де $\mathrm{S}(n,i)$ — число Стірлінга другого роду). **6.** *Вказівка.* Покажіть, що для для даного a розв'язки рівнянь $ax=a$ і $ya=a$ є відповідно правою та лівою одиницями. **7.** Ні. *Вказівка.* a) Нехай $S=\{a,b,c\}$, $aa=cc=a$, $bb=b$, усі інші добутки дорівнюють c. Тоді $\{a,b\}$ є системою твірних, для якої асоціативність множення виконується. Але $ab\cdot c=cc=a$, $a\cdot bc=ac=c$. b) Нехай $S=\{a,a^2,a^3\}$, $a\cdot a^3=a^3\cdot a=a$, $a^2\cdot a^2=a^2$. Тоді $a\cdot(a\cdot a^2)=a\cdot a^3=a$, але $(a\cdot a)\cdot a^2=a^2\cdot a^2=a^2$. **8**. 2^n-1. **9**. *Вказівка.* $T_n^{(1)}$ і $T_n^{(0)}$ ізоморфні зв'язці, що будується за ланцюгом довжини n. **10**. G — періодична група. **14**. a) $\sum_{k=1}^n\binom{n}{k}k^{n-k}$; b) $\sum_{k=0}^n\binom{n}{k}(k+1)^{n-k}$. *Вказівка.* Спочатку виберіть образ ідемпотента, а потім підрахуйте кількість ідемпотентів із цим образом. **15.** a) 9, b) 12, c) 18, d) 16. **16.** *Вказівка.* Якщо $a^m\in I$, то $a^l\in I$ для всіх $l\geq m$. Зокрема, I завжди містить групову частину S. **17.** $n\cdot\tau(k)$, де $\tau(k)$ — кількість дільників числа k. *Вказівка.* Поставивши у відповідність конгруенції ρ на $\langle a\rangle$ індуковану конгруенцію $\overline{\rho}$ на G_a, одержимо сюр'єкцію множини конгруенцій на $\langle a\rangle$ на множину конгруенцій на G_a.

Тому кожна конгруенція ρ на $\langle a\rangle$ задається парою чисел (t,m), де $1\le t\le n$, $m|k,$. При цьому $a^p\rho a^q \Leftrightarrow p\equiv q \pmod m$ для $p,q\ge t$, а класи $\overline{1},\overline{2}\dots,\overline{t-1}$ — одноелементні. **18.** Усі моногенні напівгрупи. **19.** *Вказівка.* Розглянемо лише ті елементи $\pi\in\mathcal{T}(\mathbb{N})$, компоненти зв'язності графів дії яких мають такий вигляд: цикл довжини k, до якого причеплено кілька "хвостів" довжини n. Всі такі елементи мають тип (n,k). Зіставимо елементу π послідовність $a_1,a_2,\dots$, де a_m — кількість компонент із m "хвостами". Моногенні піднапівгрупи, породжені елементами, яким відповідають різні послідовності, — не подібні. **20.** *Вказівка.* Нехай $a_1,\dots a_{\tau(k)}$ — усі дільники числа k. Тоді кожний елемент $\pi\in\mathcal{IS}(\mathbb{N})$ типу (n,k) із точністю до подібності характеризується набором $(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_{\tau(k)})$, де α_i — кількість ланцюгів довжини i, а β_j — кількість циклів довжини a_j у ланцюговому розкладі π. **22.** Кожна конгруенція задається парою (k,d) натуральних чисел і має вигляд $\{1\}$, $\{2\}$, $\dots$, $\{k-1\}$, $\{k+nd\mid n\ge 0\}$, $\{k+1+nd\mid n\ge 0\}$, $\dots$, $\{k+(d-1)+nd\mid n\ge 0\}$. Конгруенціями Ріса будуть лише ті, для яких $d=1$. *Вказівка.* Якщо k — найменше число, для якого клас $\overline{k}$ містить >1 елемента, то $k+d$ — найменше число з $\overline{k}\setminus\{k\}$. **27.** а) $\sum_{i=0}^k\binom{n}{i}\binom{k}{i}i!$; b) k^n, c) $(k+1)^n$. **30.** а) $\sum_{i=0}^k\binom{n}{i}\binom{k}{i}i!$; b) n^k, c) $(n+1)^k$. **31.** а) $\sum_{i=0}^k\binom{n}{i}^2 i!$; b) $\sum_{i=1}^k \mathrm{S}(n,i)\frac{n!}{(n-i)!}$; c) $\sum_{i=0}^k \mathrm{S}(n+1,i+1)\frac{n!}{(n-i)!}$, (де $\mathrm{S}(n,i)$ — число Стірлінга другого роду). **32.** *Вказівка.* а) $axb\cdot ayb=axyb\Rightarrow xbay=xy$, звідки $abay=ay$, $abayb=ayb$ і $bay=y$. Аналогічно доводиться і рівність $xba=x$. **33.** а) B_n; b) B_{n+1} (B_n — n-те число Белла). **35.** а) $\binom{n}{k}$; b) $\mathrm{S}(n,k)$; c) $\mathrm{S}(n+1,k+1)$ (де $\mathrm{S}(n,i)$ — число Стірлінга другого роду). **37.** а) $\binom{n}{k}k!$; b) $\mathrm{S}(n,k)k!$; c) $\mathrm{S}(n+1,k+1)k!$ (де $\mathrm{S}(n,i)$ — число Стірлінга другого роду). **38.** а) $\binom{n}{k}$; b) $\binom{n}{k}k^{n-k}$; c) $\binom{n}{k}(k+1)^{n-k}$. **40.** Усі відношення Ґріна збігаються з відношенням рівності. **44.** *Вказівка. Необхідність.* Нехай $aba=a$, $bab=b$ і $ab=ba$. Крім того, $aaa=a$. Тому $a=ababa=baaab=bab=b$. *Достатність.* Оскільки $a\cdot a^2=a^2\cdot a$, то $a=a^2$. Тепер із $aba\cdot a=aba=a^2\cdot ba=a\cdot aba$ випливає $a=aba$. **45.** *Вказівка.* Із $\varphi^2=id$ випливає, що φ насправді є антиізморфізмом. В інверсній напівгрупі таким антиізоморфізмом є $a\mapsto a^{-1}$. Навпаки, нехай такий φ і b,c — елементи, інверсні до a. Тоді $\varphi(b)=\varphi(ba\cdot b)=\varphi(b)\cdot ba=\varphi(b)\cdot ba\cdot ca=\varphi(ca\cdot ba\cdot b)=$ $=\varphi(cab)=\varphi(c\cdot ac\cdot ab)=ab\cdot ac\cdot\varphi(c)=ac\cdot\varphi(c)=\varphi(cac)=\varphi(c)$, звідки $b=c$. **46.** *Вказівка.* Якщо a і b — інверсні, то елемент $e=ab$ є ідемпотентом і $a,b\in eSe$. **47**. *Вказівка.* Нехай $ab\ne a$. Тоді для довільного c буде $a\cdot bc=ab\cdot c$, звідки $bc=c$. Отже, кожен елемент b, який не є правою одиницею, є лівою одиницею. Але різні ліві та праві одиниці одночасно існувати не можуть.

Глава 3. **4.** Ні. **5.** Ні. *Вказівка.* Для родини функцій $f_n=n\cdot|x-1/2|$, $n\in\mathbb{N}$, точної верхньої грані не існує. **6.** *Вказівка.* Якщо $(A_i)_{i\in I}$ — ланцюг множин із L, то $A=\bigcup_{i\in I}A_i$ також належить L. Далі застосуйте лему Цорна. **7**. *Вказівка. І спосіб.* Задайте яку-небудь бієкцію між $\mathbb{N}$ і $\mathbb{Z}^2$, а потім візьміть на площині центральносиметричну смугу ширини $l>1$ і повертайте її навколо центра координат. Для кожного фіксованого положення смуги візьміть усі точки з цілими координатами, що попадають у смугу. (Заува-

жимо, що будь-які два елементи з побудованого антиланцюга навіть мають скінченний перетин). *II спосіб.* Задайте яку-небудь бієкцію між $\mathbb{N}$ і $\mathbb{Q}$, а потім зафіксуйте константу $c > 0$ і кожному дійсному числу a зіставте множину $M_a = (a, a+c) \cap \mathbb{Q}$. **8.** *Вказівка.* Досить розглянути випадок $k = 2$. Нехай для елементів $a_1, a_2 \in M_1$ і $b_1, b_2 \in M_2$ у відповідних множинах верхніх граней нема. Розгляньте ту з множин M_1 і M_2, яка містить верхню грань множини $\{a_1, a_2, b_1, b_2\}$. **10**. *Вказівка.* Розгляньте відображення $I \to J$, $x \mapsto x \vee b$, і $J \to I$, $y \mapsto y \wedge a$. **11.** *Вказівка.* Використайте задачу 3.10 і теорему про ущільнення. **14.** *Вказівка.* a) Використовуючи нерівності $ac \leq a$, $bc \leq b$, $ac \leq c$, $bc \leq c$ і вправу 3.3, доведіть нерівності $ac + bc \leq a + b$ і $ac + bc \leq c$. **15.** *Вказівка.* a) Скористайтеся нерівністю $b + c \geq bc$. c) Позаяк $a, b \leq a + b$, то $a(b + c) = a(b + c)(a + b) = a\big(b + c(a + b)\big) = a(b + bc) = ab$. **17.** *Вказівка.* a) $\Rightarrow$ b). Оскільки $ab \leq a$, то $a(ab+c) = ab+ac$. b) $\Rightarrow$ c). Позаяк $a = a(a+b)$, то $(a+b)(a+c) = (a+b)\big((a+b)a+c\big) = (a+b)a+(a+b)c = a+(a+b)c$. c) $\Rightarrow$ a). Оскільки з $a \leq b$ випливає $a+b = b$, то $b(a+c) = (a+b)(a+c) = a+(a+b)c = {} = a+bc$. a) $\Rightarrow$ d): покажіть, що обидві частини рівності дорівнюють $a+bc+d$. d) $\Rightarrow$ a). Покладіть $b = d$. a) $\Rightarrow$ e). $a = a+ab = a+bc = (a+b)c = (b+c)c = c$. e) $\Rightarrow$ a). Якщо $a \leq c$, то $a + bc \leq (a + b)c \leq c$. Крім того, $(a + b)c \cdot b = cb$. Тому $cb \geq (a + bc) \cdot b \geq bc \cdot b = cb$, звідки $(a + bc) \cdot b = cb$. Отже, $(a + b)c \cdot b = {} = (a + bc) \cdot b$. Аналогічно доводиться, що $(a + b)c + b = (a + bc) + b$. a) $\Rightarrow$ f). Випливає з наслідку 3.2 і того, що підрешітка модулярної решітки є модулярною. f) $\Rightarrow$ a). Випливає з критерію модулярності (теорема 3.6). **19.** *Вказівка.* Оскільки $a_1 \leq b_2 b_3 \cdots b_n$, то $\big(a_1 + (a_2 + \cdots + a_n)\big)\, b_1 b_2 \cdots b_n = {} = \big(a_1+(a_2+\cdots+a_n)b_2 \cdots b_n\big)b_1$. Тепер, ураховуючи нерівність $a_2+\cdots+a_n \leq b_1$, маємо: $\big(a_1+b_2 \cdots b_n(a_2+\cdots+a_n)\big)b_1 = a_1b_1+(a_2+\cdots+a_n)b_2 \cdots b_n$. Далі застосуйте індукцію. **20.** *Вказівка.* a) $\Rightarrow$ b). $(a+c)(b+c) = ab+ac+cb+cc = ab+c$. b) $\Rightarrow$ c). $ab+bc+ca = ab+(bc+ca) = (a+bc+ca)(b+bc+ca) = (a+bc)(b+ca) = {} = (a + b)(a + c)(b + c)(b + a)$. c) $\Rightarrow$ a). Якщо $a \leq c$, то $ab + bc + ca = a + bc$, $(a + b)(b + c)(c + a) = (a + b)c$, що дає модулярність. Оскільки $c \geq bc + ca$, то $c(ab + bc + ca) = c \cdot ab + bc + ca = bc + ca$. З іншого боку, $c(a + b)(b + c)(c + a) = {} = c(a+b)$. Тому $c(a+b) = ca+cb$. a) $\Rightarrow$ d). Це лема 3.2. d) $\Rightarrow$ c). Згідно із задачею 3.7.e решітка L є модулярною. Нехай $u = ab+bc+ca$, $v = (a+b)(b+c)(c+a)$, $p = ac + b(a + c)$, $q = bc + a(b + c)$, $r = ab + c(a + b)$. Використовуючи модулярний закон (задача 3.7.b), покажіть, що $p + r = v$, $q + r = v$, $pr = u$, $qr = u$. Тому $p = q$. Далі покажіть, що $p = p + q = v$, $p = pq = u$. b) $\Rightarrow$ e). Оскільки $a + c \geq c$, то $a + bc = (a + b)(a + c) \geq (a + b)c$. e) $\Rightarrow$ a). Після множення обох частин нерівності $(a + b)c \leq a + bc$ на c отримуємо $(a + b)c \leq (a + bc) \leq ac + bc$. Із другого боку, із нерівностей $a + b \geq ac + bc$ і $c \geq ac + bc$ випливає, що $(a + b)c \geq ac + bc$. **21.** *Вказівка.* a) $\Rightarrow$ e). Якщо $ab \leq c$ і $a \leq b + c$, то $ac = a(c + bc) = ac + abc = ac + ab = a(b + c) = a$. **24.** *Вказівка.* Використайте нормальну форму — диз'юнктивну або кон'юнктивну. **27.** *Вказівка.* Решітка ідеалів є підрешіткою решітки підгруп адитивної групи кільця. **29.** *Вказівка.* Якщо абелева група є циклічною, то решітка підгруп є прямим добутком решіток підгруп примарних циклічних компонент. **30.** *Вказівка.*

Використайте критерій дистрибутивності модулярної решітки. **32.** *Вказівка.* а) $(a+b)+a'b' = a+ab'+a'b'+b = a+(a+a')b'+b = a+b'+b = a+1 = 1$; b) $(a+b)\cdot a'b' = aa'b' + ba'b' = 0\cdot b' + 0\cdot a' = 0$. **33.** Ні. **38.** *Вказівка.* Досить показати існування або нескінченного спадного, або нескінченного зростаючого ланцюга. Якщо кожен спадний ланцюг обривається, то для кожного $a \neq 0$ існує атом $b \leq a$. Якщо атомів скінченна кількість, то решітка скінченна. Якщо ж атомів нескінченно багато, то одержуємо нескінченний зростаючий ланцюг $0 < a_1 < a_1 + a_2 < a_1 + a_2 + a_3 < \cdots$. **39.** Наприклад, підалгебра алгебри $\mathcal{B}(\mathbb{N})$, що складається з усіх скінченних і коскінченних підмножин. **41.** 2^{2^n}. *Вказівка.* Кожен елемент із $\langle a_1, \ldots, a_n\rangle$ можна записати у вигляді ДДНФ від $a_1, \ldots, a_n$. **42.** B_n — n-те число Белла. *Вказівка.* Кожному розбиттю $M = A_1 \cup \cdots \cup A_k$ відповідає підалгебра, породжена елементами A_1, …, A_k. Інших підалгебр нема. **43.** *Вказівка.* Комутативність випливає з $ab - ba = (ab-ba)^3 = 0$, тотожність — із $x + x = (x+x)^2$. **53**. *Вказівка.* Якщо $\mathcal{P}(M) \simeq \mathfrak{B}(N)$, то множина N — нескінченна. Тоді в $\mathfrak{B}(N)$ існує такий елемент a, що довжини як зростаючих, так і спадних ланцюгів із початком в a не обмежені. А в $\mathcal{P}(M)$ таких елементів нема.

Глава 4. **4.** *Вказівка.* Якщо $a = a_0 + a_1x + a_2x^2 + \cdots$ і $a_0 \neq 0$, то коефіцієнти ряду $1/a = b_0 + b_1x + b_2x^2 + \cdots$ обчислюються рекурентно: $b_0 = 1/a_0$ і $b_k = -\frac{1}{a_0}\sum_{i=1}^{k} a_i b_{k-i}$ при $k > 0$. **5.** $\mathcal{A}_1 \simeq \mathcal{A}_6$, $\mathcal{A}_4 \simeq \mathcal{A}_5$. *Вказівка.* $\dim \mathcal{A}_1 = \dim \mathcal{A}_4 = \dim \mathcal{A}_5 = \dim \mathcal{A}_6 = 2$, $\dim \mathcal{A}_2 = \dim \mathcal{A}_3 = \dim \mathcal{A}_7 = \dim \mathcal{A}_8 = \infty$. Крім того, в $\mathcal{A}_4$ є нільелементи, а в $\mathcal{A}_1$ — нема. Серед алгебр $\mathcal{A}_2$ $\mathcal{A}_3$, $\mathcal{A}_7$, $\mathcal{A}_8$ 1-породженою є тільки $\mathcal{A}_2$, а нільелементи містить лише $\mathcal{A}_8$. Крім того, в $\mathcal{A}_7$ є дільники нуля, а в $\mathcal{A}_3$ — нема. **7.** *Вказівка.* Кожне з відображень $x \mapsto ax$ і $x \mapsto xa$ має нульове ядро тоді й лише тоді, коли воно є бієктивним. **8.** *Вказівка.* Розгляньте мінімальний многочлен елемента a. **9.** *Вказівка.* Якщо нетривіальних односторонніх ідеалів нема, то для даного ненульового елемента a існують такі e_l і e_r, що $e_la = ae_r = a$. Далі покажіть, що $e_lx = xe_r = x$ для довільного елемента x. **14.** Ні. *Вказівка.* $\dim \mathbf{H} = 4$, $\dim \mathbb{C}[Q_8] = 8$. **15.** Ні. **18.** *Вказівка.* Квадрат кватерніона z буде дійсним тоді й лише тоді, коли z дійсний або чисто уявний. **20**. *Вказівка.* Якщо $x^2 \in \mathbb{R}$, то x є скалярним або векторним. $x^3 - 1 = (x-1)(x^2+x+1)$, а другий множник має нескінченно багато коренів. **22.** *Вказівка.* n-вимірну алгебру над $\mathbb{C}$ можна розглядати як $2n$-вимірну алгебру над $\mathbb{R}$. Далі застосуйте теорему Фробеніуса. **25.** *Вказівка.* Для доведення першої частини використайте задачу 4.23. **26.** *Вказівка.* Розгляньте матриці $E = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $I = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $K = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. **29.** *Вказівка.* Використайте задачу 4.28. **31.** *Вказівка.* Виберіть базу $1, b$ і нехай $b^2 = \alpha + \beta b$. Далі — безпосередня перевірка. **32.** *Вказівка.* Покажіть, що можна вибрати базу $1, j$ так, щоб виконувалася одна з трьох можливостей: або $j^2 = -1$, або $j^2 = 1$, або $j^2 = 0$. **33.** $\mathbb{C}\oplus\mathbb{C}$, $\mathbb{C}[x]/(x^2)$. *Вказівка.* Покажіть, що можна вибрати базу $1, j$ так, щоб виконувалася одна з двох можливостей: або $j^2 = 1$, або $j^2 = 0$. **34.** *Вказівка.* Якщо p і q — різні прості числа, то квадратичні розширення $\mathbb{Q}(\sqrt{p})$ і $\mathbb{Q}(\sqrt{q})$ неізоморфні. **35.** *Вказівка.* $b\cdot bb = ba = -b$, $bb\cdot b = ab = b$.

Для $A = \alpha a + \beta b$, $X = xa + yb$, $B = \gamma a + \delta b$ рівняння $AX = B$ і $XA = B$ зводяться відповідно до систем $\begin{cases} \alpha x + \beta y &= \gamma, \\ -\beta x + \alpha y &= \delta \end{cases}$ і $\begin{cases} \alpha x + \beta y &= \gamma, \\ \beta x - \alpha y &= \delta \end{cases}$ із визначником $\pm(\alpha^2+\beta^2)$. Якщо $\beta \neq 0$, то система $AX = A$, $XA = A$ — несумісна. **37.** *Вказівка.* Якщо a — елемент порядку n, то $(1+a+\cdots+a^{n-1})(1-a) = 0$. **40.** a) 3, b) 5, c) 4. *Вказівка.* Розмірність центру дорівнює кількості класів спряжених елементів. **42.** Лише для одиничної групи. **43.** a) 0, $\langle b\rangle$; b) 0, $\langle 1-b\rangle$, $\langle 1+b\rangle$. *Вказівка.* Кожен нетривіальний ідеал є одновимірним підпростором. **44.** 0, $M_2(\mathbb{Z}_2)$, матриці з нульовим першим стовпчиком, матриці з нульовим другим стовпчиком, матриці з однаковими стовпчиками. **45.** 2^n. *Вказівка.* Кожен ідеал однозначно визначається множиною номерів тих компонент, які для всіх елементів ідеалу дорівнюють 0. **46.** *Вказівка.* a) Розгляньте ненульовий одночлен найменшого степеня, який зустрічається в елементах ідеалу I, і використайте задачу 4.4. **47.** a) 8, b) 32. **49.** *Вказівка.* a) Нетривіальна тільки друга частина твердження. Нехай I — лівий ідеал і $U = \langle \varphi(v) \mid \varphi \in I, v \in P^n\rangle$. Включення $I \subseteq I^l_U$ очевидне. Нехай $v = \alpha_1 v_1 + \cdots + \alpha_k v_k$, де $v_i = \varphi_i(u_i)$ для деяких $u_i \in P^n$, $\varphi_i \in I$. Візьмемо довільний ненульовий вектор $f \in P^n$ і доповнимо його до бази: $f_1 = f$, f_2, $\ldots$, f_n. Позначимо через ψ_i перетворення, для якого $\psi_i(f) = u_i$, $\psi_i(f_j) = 0$ при $j \neq 1$, і нехай $\psi_{f,v} = \alpha_1\psi_1\varphi + \cdots + \alpha_k\psi_k\varphi$. Тоді $\psi_{f,v} \in I$, $\psi_{f,v}(f) = v$ і $\psi_{f,v}(f_j) = 0$ при $j \neq 1$. Нехай тепер $\varphi \in I^l_U$ і $\varphi(e_i) = w_i$, $(i = 1, \ldots, n)$. Тоді $\varphi = \psi_{e_1,w_1} + \cdots + \psi_{e_n,w_n}$, звідки $\varphi \in I$, що доводить зворотне включення. b) Для доведення другої частини твердження розгляньте на P^n невироджену білінійну симетричну форму (u, v) і доведіть, що для правого ідеалу I множина $I^* = \{\varphi^* \mid \varphi \in I\}$ (де φ^* є перетворенням, спряженим до φ) є лівим ідеалом. Далі використайте п. a). **51.** *Вказівка.* Використайте задачу 4.50. **52.** *Вказівка.* Це — матричне переформулювання задачі 4.49. **53.** $\mathbb{C} \oplus \ldots \oplus \mathbb{C}$. **54.** Підалгебра $\mathcal{A}$ буде напівпростою комутативною тоді й лише тоді, коли для неї існує власна база (спільна для всіх перетворень з $\mathcal{A}$). **55.** *Вказівка.* Для кожного інваріантного відносно алгебри A підпростору з $\mathbb{C}^n$ його ортогональне доповнення також буде інваріантним підпростором. Розкладіть $\mathbb{C}^n$ у пряму суму мінімальних інваріантних підпросторів. Обмеження $\mathcal{A}$ на кожен із таких підпросторів дає незвідне зображення й кожен ненульовий елемент з $\mathcal{A}$ хоча б на одному з цих підпросторів дії нетривіально. **56.** $T^{-1}DT$, де T — фіксована невироджена матриця, а D — підалгебра клітинно-діагональних матриць із фіксованими розмірами клітин. *Вказівка.* З теореми 4.14 випливає, що кожна напівпроста підалгебра з $M_n(\mathbb{C})$ подібна деякій підалгебрі вигляду $\operatorname{diag}(M_{k_1}(\mathbb{C}), \ldots, M_{k_m}(\mathbb{C}))$. **57.** *Вказівка.* Перетин інваріантних підпросторів знову є інваріантним. Тому з мінімальності V_1 випливає, що перетин $V_k \cap (V_1 + \cdots + V_{k-1})$ або нульовий, або збігається з V_k. Лишіть із набору V_1, $\ldots$, V_n лише ті підпростори, які не містяться в сумі попередніх. **58.** *Вказівка.* Якщо ідеал I має непорожній перетин із $M_{n_i}(\mathbb{C})$, то він містить $M_{n_i}(\mathbb{C})$.

Глава 5. **1**. Так. *Вказівка.* Використайте задачу 3.17. **2.** $x^n = 1$ і тотожно-

сті (5.5). **3.** *Вказівка.* Тотожність $f^k(x) = f^m(y)$ $(k < m)$ рівносильна тотожності $f^k(x) = f^k(y)$; система $f^k(x) = f^{k+p}(x)$, $f^m(x) = f^{m+q}(x)$ рівносильна тотожності $f^{\min(k,m)}(x) = f^{\min(k,m)+\text{НСД}(p,k)}(x)$; система $f^k(x) = f^k(y)$, $f^m(x) = f^{m+q}(x)$ рівносильна тотожності $f^{\min(k,m)}(x) = f^{\min(k,m)}(y)$. **4.** Граф дії унару є диз'юнктним набором циклів довжини k, кожен із яких містить рівно один елемент вільної системи твірних. **5.** a) Граф дії є диз'юнктним набором циклів довжини 1 і 3; b) $\langle X \dot\cup \{y\}; f\rangle$, де $f(x) = f(y) = y$ для всіх $x \in X$; c) усі унари. **7.** *Вказівка.* Кожну тотожність можна звести до вигляду $\gamma_1 x_1 + \cdots + \gamma_k x_k = 0$, яка рівносильна системі $\gamma_1 x_1 = 0$, …, $\gamma_k x_k = 0$. **8.** $\prod_{i\in I} \mathbb{Z}_n$. **9.** Бути прямою сумою циклічних груп однакового порядку. *Вказівка.* Використайте задачу 5.7 і 5.8. **10.** a) $nx = 0$; b) $\text{НСК}(n,m)\cdot x = 0$; c) $0\cdot x = 0$. **11.** *Вказівка.* Нехай $\mathfrak{M}$ — найменший клас алгебр, який містить $\mathcal{A}$ і замкнений відносно взяття підалгебр і прямих добутків. Із доведення теореми 5.3 випливає, що для скінченної множини X вільна алгебра $F(X)$ із класу $\mathfrak{M}$ буде скінченною. **12.** Нехай $\mathfrak{N}$ — клас усіх ізоморфних образів факторалгебр підалгебр прямих добутків алгебр із $\mathfrak{K}$. Включення $\mathfrak{K} \subseteq \mathfrak{N} \subseteq \mathfrak{M}$ випливає з теореми Біркгофа. Для доведення включення $\mathfrak{M} \subseteq \mathfrak{N}$ покажіть замкненість $\mathfrak{N}$ відносно підалгебр, гомоморфних образів і прямих добутків. **14.** *Вказівка.* a) Цей клас не замкнений відносно прямих добутків. b) Нехай $F(X)$ — вільна нільпотентна напівгрупа і n — її ступінь нільпотентності. Нехай A нільпотентна напівгрупа класу нільпотентності $m > n$ і $a_1, \ldots, a_n \in A$ — такі, що $a_1 \cdots a_n \neq 0$. Тоді жодне сюр'єктивне відображення $X \to \{a_1, \ldots, a_n\}$ не піднімається до гомоморфізму $F(X) \to A$. **15.** *Вказівка.* Див. вказівку до задачі 5.14. **16.** Множина всіх слів довжини $< n$ у даному алфавіті X (як факторнапівгрупа вільної напівгрупи X^+ за ідеалом слів довжини $\geq n$). **17.** Напівгрупові алгебри напівгруп із задачі 5.16. **19**. *Вказівка.* Покладіть $1 = x/x$, $x^{-1} = (x/x)/x$, $xy = x/\big((y/y)/y\big)$ і перепишіть у нових позначеннях тотожності (5.5). **20**. *Вказівка.* Покладіть $b/a = ba^{-1}$. **43.** *Вказівка.* a) $ab - ba = (ab - ba)^3 = 0$; b) $a + a = (a + a)^2 = (a + a) + (a + a)$.

Глава 6. **11.** *Вказівка. Достатність.* $\|x + y\|^k = \|(x + y)^k\| = \|x^k + {} + \binom{k}{1}x^{k-1}y + \cdots + y^k\| \leq \|x^k\| + \|\binom{k}{1}x^{k-1}y\| + \cdots \leq \|x^k\| + \|x^{k-1}y\| + \|x^{k-2}y^2\| + \cdots$, бо $\|n\| \leq 1$. Нехай тепер $\max(\|x\|, \|y\|) = a$ і $\|x + y\| = a + \alpha$, де $\alpha > 0$. Тоді $(a + \alpha)^k \leq a^k + a^k + \cdots = (k + 1)a^k$. З іншого боку, $(a + \alpha)^k \geq a^k + ka^{k-1}\alpha + {} + \frac{k(k-1)}{2}a^{k-2}\alpha^2$. Звідси $ka^{k-2}\big(a\alpha + \frac{k-1}{2}\alpha^2\big) \leq ka^k$. Зокрема, $\frac{k-1}{2}\alpha^2 \leq a^2$ для всіх k. Суперечність. Отже, $\alpha \leq 0$ і $\|x + y\| \leq \max(\|x\|, \|y\|)$. **14.** *Вказівка.* Оскільки для всіх x, y має бути $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$, то $2^\alpha |x|^\alpha \leq 2 \cdot |x|^\alpha$, звідки $\alpha \leq 1$. Навпаки, нехай $0 < \alpha \leq 1$. Тоді $z^\alpha \geq z$ для всіх $z \in [0, 1]$. Нерівність $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$ рівносильна нерівності $1 \leq \frac{|x|^\alpha}{|x+y|^\alpha} + \frac{|y|^\alpha}{|x+y|^\alpha}$. Але $\frac{|x|^\alpha}{|x+y|^\alpha} + \frac{|y|^\alpha}{|x+y|^\alpha} = \big|1 - \frac{y}{x+y}\big|^\alpha + \big|1 - \frac{x}{x+y}\big|^\alpha \geq 1 - \frac{y}{x+y} + 1 - \frac{y}{x+y} = 1$. **15.** *Вказівка.* Нехай $x > 1$. Оскільки $x + (1 - x) = 1$, то для норми має виконуватися нерівність $1 \leq x^\alpha + (x-1)^\alpha$, яка рівносильна нерівності $(x^{-\alpha} - 1)((x-1)^{-\alpha} - 1) \leq 1$, що хибна при $x - 1 > \log_{(-\alpha)} 2$. **16.** *Вказівка.* За теоремою Островського всі архімедові норми $\|\ \|$ на $\mathbb{Q}$ рівносильні. Далі використайте твердження

6.8 і задачу 6.14.a. **18.** a) 2; b) 2; c) -1; d) -4; e) 1; f) 3; g) -2; h) 2; i) 0; j) 4; k) 7; l) -1; m) $2^n - n$; n) 1; o) $1 + p + p^2 + \cdots + p^{k-1}$. **21.** a) $2.1211\ldots$; b) $0.12102\ldots$; c) $51.240\ldots$. **22.** a) $0.01(10)$; b) $0.2(0121)$; c) $43.(3)$; d) $0.1(01220211101021022220)$; e) $0.1(2101)$; f) $0.1(31)$; g) $0.5(2145)$; h) $110.(10)$; i) $4.(43)$; j) $22.(2212)$. **25.** У полі $\mathbb{Q}_p$ не існує $\sqrt{p}$. **26.** Знайдіть для кожного з полів кількість тих цілих чисел $k \in [0, pq)$, для яких у даному полі існує $\sqrt{k}$. **30.** Послідовність є збіжною, границя дорівнює 0. **31.** *Вказівка.* Для достатності досить показати, що часткові суми $S_n = a_1 + \cdots + a_n$ утворюють послідовність Коші. А це випливає з нерівності $|S_m - S_n|_p \le \max(|a_{n_1}|_p, \ldots, |a_m|_p)$. **32.** $\operatorname{ord}_p x \ge 1$ для $p > 2$ і $\operatorname{ord}_2 x \ge 2$ для $p = 2$. *Вказівка.* $\operatorname{ord}_p n! = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$. **33.** a) $\frac{1}{1-p}$; b) $\frac{1}{1+p}$; c) $\frac{p^2-p+1}{1-p^2}$. **34.** *Вказівка.* a) Нехай $n \xrightarrow[|\ |_p]{} \frac{m}{k}$, де $\frac{m}{k}$ — нескоротний дріб і $\operatorname{ord}_p k = N$. Візьмемо $\varepsilon < 1/p^N$. Припустимо, що $\left|n - \frac{m}{k}\right|_p < \varepsilon$ для всіх $n > n_0$. Запишемо $nk - m = p^{N_n} M_n$, де $N_n = \operatorname{ord}_p(nk - m)$. Тоді $N_n > N$ для всіх $n > n_0$. Звідси і з рівності $(n+1)k - m = (nk - m) + k$ випливає, що $\operatorname{ord}_p k > N$. Суперечність. b) Нехай $a_n \xrightarrow[|\ |_p]{} \frac{m}{k}$ і $\operatorname{ord}_p\left(a_n - \frac{m}{k}\right) = N_n$. Для достатньо великих n маємо: $N_n \le \operatorname{ord}_p(a_n k - m) \le \log_p |a_n k - m| < \log_p(|k| + 1)a_n < 2n!$. Тоді для $m > n$ маємо: $a_m - \frac{m}{k} = \left(a_n - \frac{m}{k}\right) + (a_m - a_n) = p^{N_n} \cdot \frac{u}{v} + p^{(n+1)!} \cdot A$, звідки $\operatorname{ord}_p\left(a_m - \frac{m}{k}\right) = N_n$ і норма $\left|a_m - \frac{m}{k}\right|_p = p^{-N_n}$ — фіксована і не прямує до 0. **38.** Для $p = 5, 13, 17$. *Вказівка.* -1 має бути квадратичним лишком за модулем p. **39.** a) $0.21213\ldots$, $0.33231\ldots$; b) $0.55105\ldots$, $0.8\,7\,11\,12\,7\ldots$. **41.** $0.101011\ldots$, $0.110100\ldots$. **42.** Так — b, c, d, f, i; ні — a, e, g, h. **43.** *Вказівка.* Можна взяти (a, b, pa, pb), де a — квадратичний лишок, а b — квадратичний нелишок за модулем p. **44.** *Вказівка.* Із теореми Ферма випливає, що коли $a^p = 1$ і $a \ne 1$, то a має вигляд $a = 1 + p^k(a_k + a_{k+1}p + a_{k+2}p^2 + \cdots)$, де $k > 0$ і $a_k \ne 0$. Обчисліть p-й степінь цього числа.

Позначення

$\langle A; \Omega \rangle$ — універсальна алгебра з носієм A і сигнатурою Ω — 6;

$\langle A; (\omega_i)_{i \in I} \rangle$ — універсальна алгебра з носієм A і родиною дій $(\omega_i)_{i \in I}$ — 6;

$A/\sim$ — факторалгебра алгебри A за конгруенцією $\sim$ — 13;

$a_{\triangle}$ — нижній конус елемента a — 60;

$a^{\triangledown}$ — верхній конус елемента a — 60;

$\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$ — пряма сума алгебр $\mathcal{A}_1, \ldots, \mathcal{A}_n$ — 89;

$\mathcal{B}(X)$ — напівгрупа всіх бінарних відношень на множині X — 27;

$\mathfrak{B}_n$ — напівгрупа Брауера на n-елементній множині — 28;

$\mathfrak{B}(M)$ — упорядкована за включенням множина всіх підмножин множини M — 61;

$\mathfrak{B}_{fin}(M)$ — решітка всіх скінченних підмножин множини M — 61;

$\mathrm{Con}(A)$ — множина всіх конгруенцій на універсальній алгебрі A — 11;

$\mathcal{D}(a)$ — клас еквівалентності $\mathcal{D}$-відношення Ґріна, який містить елемент a — 41;

$\mathrm{End}\, A$ — множина ендоморфізмів універсальної алгебри A — 30;

$E(S)$ — множина ідемпотентів напівгрупи S — 23;

$F(X)$ — вільна напівгрупа з множиною твірних X — 25;

$F(\Omega, X)$ — вільна алгебра сигнатури Ω із системою твірних X — 10;

$F_\Lambda(\Omega, X)$ — вільна алгебра многовиду (Ω, Λ) — 124;

$\mathcal{FP}(S)$ — факторстепінь напівгрупи перетворень S — 29;

$\mathbb{H}$ — тіло кватерніонів — 90;

$\mathcal{H}(a)$ — клас еквівалентності $\mathcal{H}$-відношення Ґріна, який містить елемент a — 41;

$\mathbf{i}_A$ — одинична конгруенція на алгебрі A — 11

$\inf A$ — точна нижня грань множини A — 59;

$\mathcal{IS}(X)$ — симетрична інверсна напівгрупа всіх часткових підстановок на множині X — 27;

$\mathcal{J}(a)$ — клас еквівалентності $\mathcal{J}$-відношення Ґріна, який містить елемент a — 41;

$\mathrm{Ker}\, \varphi$ — ядро гомоморфізму φ або зображення φ — 10, 99;

$\mathcal{L}(a)$ — клас еквівалентності $\mathcal{L}$-відношення Ґріна, який містить елемент a — 40;

$\langle M \rangle$ — підалгебра, породжена множиною M — 8;

$N(x)$ — норма кватерніона x — 91;

$n(\omega)$ — арність операції ω — 6;

$\mathbf{o}_A$ — нульова конгруенція на алгебрі A — 11;

$\mathrm{ord}_p n$ — показник степеня, із яким просте число p входить у канонічний розклад числа n — 154;

$P(A)$ — глобальна надалгебра алгебри A або напівгрупа-степінь напівгрупи A — 7, 28;

$P[S]$ — групова (відповідно напівгрупова) P-алгебра групи (відповідно напівгрупи) S — 87;

$\mathcal{PT}(X)$ — напівгрупа всіх часткових перетворень множини X — 26;

$P\langle x_1, \ldots, x_n\rangle$ — тензорна P-алгебра з твірними $x_1, \ldots, x_n$ — 88;

$\mathbb{Q}_p$ — поле p-адичних чисел — 138;

$\mathcal{R}(a)$ — клас еквівалентності $\mathcal{R}$-відношення Ґріна, який містить елемент a — 40;

S^1 — напівгрупа S із приєднаною одиницею (якщо в S не було одиниці), або сама S у противному разі — 25;

$\mathrm{Sub}(A)$ — множина всіх підалгебр універсальної алгебри A — 61;

$\sup A$ — точна верхня грань множини A — 59;

$\mathcal{T}(X)$ — симетрична напівгрупа всіх перетворень множини X — 26;

$W(\mathfrak{M})$ — похідний многовид многовиду $\mathfrak{M}$ — 129;

X^* — вільний моноїд із множиною твірних X — 25;

$\widehat{x}$ — уявна (векторна) частина кватерніона x — 90;

$\overline{x}$ — кватерніон, спряжений до кватерніона x — 90;

$\|x\|$ — норма елемента x — 146;

$Z(\mathcal{A})$ — центр алгебри $\mathcal{A}$ — 86;

$\mathbb{Z}_{(p)}$ — кільце цілих p-адичних чисел — 135;

$\mu \dotplus \nu$ — пряма сума зображень μ та ν — 101;

$\varphi \circ \psi$ — де-морганівський добуток бінарних відношень φ і ψ — 27;

(Ω, Λ) — многовид алгебр сигнатури Ω, який визначається тотожностями Λ — 117;

$\prod_{i\in I} A_i$ — прямий добуток родини алгебр $(A_i)_{i\in I}$ — 14;

$|\ |_p$ — p-адична норма на полі $\mathbb{Q}$ — 154.

Література

[1] *Бахтурин Ю.А.* Основные структуры современной алгебры. — М. : Наука, 1990.

[2] *ван дер Варден* Алгебра. — М. : Наука, 1976.

[3] *Дрозд Ю.А., Кириченко В.В.* Конечномерные алгебры. — К. : Вища школа, 1980.

[4] *Калужнин Л.А.* Введение в общую алгебру. — М. : Наука, 1973.

[5] *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп. — М. : Мир, 1972. — Т. 1.

[6] *Коблиц Т.* p-адические числа, p-адический анализ и дзета-функции. — М. : Мир, 1982.

[7] *Кон П.* Универсальная алгебра. — М. : Мир, 1968.

[8] *Кострикин А.И.* Введение в алгебру. Основные структуры. — М. : Физмалит, 2001.

[9] *Курош А.Г.* Общая алгебра. Лекции 1969–1970 учебного года. — М. : Наука, 1974.

[10] *Курош А.Г.* Лекции по общей алгебре. — М. : Наука, 1962.

[11] *Ленг С.* Алгебра. — М. : Мир, 1968.

[12] *Мальцев А.И.* Алгебраические системы. — М. : Наука, 1970.

[13] *Скорняков Л.А.* Элементы общей алгебры. — М. : Наука, 1983.