Передмова

Цей посібник являє собою конспект лекцій з теорії алгебричних чисел, що їх автор читав у Київському Університеті. Фактично він є лише *вступом* до цієї теорії, в якому розглянуто тільки деякі основні факти про цілі алгебричні числа. Автор сподівається, що йому все ж вдалося дати поняття про найважливіші питання і методи, якими він вважає:

Теорію подільності – її викладено в розділі I на ґрунті теорії ідеалів дедекіндових кілець. Це найбільший (і найбільш повний) розділ курсу, що, напевне, викликано "алгебричним ухилом" автора.

Геометричні методи, які базуються на геометричному зображенні алгебричних чисел і лемі Мінковського – їх викладено в розділі II. Тут ми обмежились лише двома класичними результатами: теоремою про скінченність групи класів і теоремою Діріхле про групу одиниць (у вправах накреслено також доведення теореми Ерміта про скінченність кількості полів з даним дискримінантом).

Аналітичні методи, які базуються на вивченні дзета-функцій і рядів Діріхле – їх викладено в Розділі III. Це, мабуть, найменш повний розділ, хоч його й доведено до класичної теорми Діріхле про первинні числа в арифметичній прогресії. Але, на жаль, подальші результати в цьому напрямку вимагають набагато більшої піготовки (як аналітичної, так і суто арифметичної) і, незважаючи на палке бажання автора, обсяг курсу поставив перед ним досить жорстку межу.

Звичайно, фахівець одразу помітить, що багато важливих сюжетів у цих лекціях навіть не згадано (зображення чисел квадратичними формами, локальні методи і багато іншого). Знов-таки, тут нас обмежували реальні можливості досить невеликого за обсягом курсу. Втім автор сподівається, що цей невеличкий посібник зможе підготувати студентів до вивчення вже серйозних монографій на зразок книг [**КФ**], [**БШ**], [**АВ**] або [**Л2**]. Наскільки мені відомо, зараз не існує жодного підручника з теорії алгебричних чисел українською мовою; навіть і російською мовою такі більш-менш елементарні підручники, як [**ГВ**] та [**Г**], давно стали біліографічною рідкістю.

Невеликий обсяг ми намагалися компенсувати досить великою кількістю задач. За оцінкою автора, вони цілком доступні для "середнього читача" і ми конче рекомендуємо розв'язувати їх вже при першому читанні. Більшість задач являє собою або конкретизацію матеріалу відповідного розділу (ми намагались обирати найтиповіші і/або найцікавіші приклади, хоча читачеві вирішувати, наскільки ми того спромоглися), або подальший розвиток цього матеріалу. Зокрема, автор не втримався від включення задач, мета яких – показати далекосяжну паралель теорії алгебричних чисел з теорією алгебричних функцій (від однієї змінної). Виправданням тут є думка більшості фахівців про те, що одночасне знайомство з цими двома теоріями є вельми корисним для опанування їх обох.

Наш посібник орієнтований саме на початківців – студентів II–IV курсів. Тому ми розраховували, принаймні в основному тексті, лише на знання читачем загальноуніверситетського курсу алгебри. Такі підручники, як [**К**] або [**Ф**], разом з яким-небудь курсом лінійної алгебри (їх існує так багато, що наводити список тут є зайвим), повністю покривають потрібний матеріал. Звичайно, у деяких вправах ми користувались і певними фактами, які не входять до стандартного курсу: елементами теорії Ґалуа, теорією модулів над кільцями головних ідеалів тощо. Втім і цей матеріал не виходить за межі більш-менш загальноприйнятних "курсів абстрактної алгебри для початківців" і практично весь міститься, наприклад, у таких класичних підручниках, як [**ВВ**] або [**Л1**].

Зміст

Передмова 1

Розділ I. Подільність 4
I.1. Приклад 1. Ґауссові числа 4
I.2. Приклад 2. Неоднозначність розкладу 6
I.3. Цілі алгебричні числа 7
I.4. Дедекіндові кільця. Теорія ідеалів 14
I.5. Дробові ідеали. Класи ідеалів 17
I.6. Кільця лишків. Норма ідеалу 20
I.7. Розклад первинних чисел. Дискримінант 27

Розділ II. Геометричні методи 34
II.1. Геометричне зображення алгебричних чисел 34
II.2. Лема Мінковського 38
II.3. Скінченність групи класів ідеалів 39
II.4. Група одиниць 43

Розділ III. Аналітичні методи 48
III.1. Ряди Діріхле 48
III.2. Рівномірний розподіл ідеалів за класами 50
III.3. Дзета-функції Дедекінда 53
III.4. Існування первинних ідеалів першого ступеня 55
III.5. Поля поділу кола 56
III.6. Первинні числа в арифметичних прогресіях 58

Покажчик 64

Бібліоґрафія 66

Розділ I

Подільність

I.1. Приклад 1. Ґауссові числа

Основною теоремою елементарної арифметики є, безперечно, теорема про однозначність розкладу цілого числа у добуток первинних (або простих). При всій її "очевидності" вона є дуже глибоким і аж ніяк не тривіальним фактом, який докорінно відрізняє кільце цілих чисел від більшості інших кілець, навіть дуже близьких до нього. Аналізуючи звичайні доведення, можна спробувати переносити їх на інші кільця. Класичний приклад – кільце многочленів від однієї змінної над полем – добре відомий із стандартного курсу алгебри. Зараз ми розберемо ще один приклад, більш "теоретико-числового" характеру.

Означення I.1.1. *Кільцем ґауссових чисел* зветься підкільце поля комплексних чисел $\Gamma = \mathbb{Z}[i] = \{\, a + bi \,|\, a, b \in \mathbb{Z} \,\}$.

У кільці ґауссових чисел, так само як і в кільцях цілих чисел і многочленів, можна означити *ділення з остачею*. Саме, покладемо $\mathrm{N}(\alpha) = |\alpha|^2 = a^2 + b^2$ для $\alpha = a + bi$. Тоді має місце такий факт.

Твердження I.1.2. *Для довільних ненульових елементів $\alpha, \beta \in \Gamma$ існують такі $\gamma, r \in \Gamma$, що $\alpha = \beta\gamma + r$, причому $\mathrm{N}(r) < \mathrm{N}(\beta)$.*
Звичайно число r зветься *залишком від ділення α на β*.

Доведення. Розглянемо число α/β. Воно знов має вигляд $a+bi$, де $a, b \in \mathbb{Q}$. Існують такі цілі числа a_0 і b_0, що $|a-a_0| \le 1/2$ і $|b-b_0| \le 1/2$. Покладемо $\gamma = a_0 + b_0 i$. Тоді $|\alpha/\beta - \gamma| < 1$, звідки $|\alpha - \beta\gamma| < |\gamma|$, тобто можна покласти $r = \alpha - \beta\gamma$. □

Як відомо (див., напр., [**K**, гл.5, §3, п.3]), з існування ділення з остачею випливає *однозначність розкладу*, тобто наступна теорема.

Теорема I.1.3. *Кожен ненульовий необертовний елемент $\alpha \in \Gamma$ розкладається у добуток* незвідних *елементів: $\alpha = \pi_1\pi_2\ldots\pi_n$, причому якщо ще $\alpha = \theta_1\theta_2\ldots\theta_m$, де всі θ_j також незвідні, то $m = n$ і, з точністю до нумерації співмножників, $\theta_j = \varepsilon_j\pi_j$, де кожен елемент ε є* обертовним *у кільці Γ.*

Тут, як звичайно, елемент π зветься *незвідним*, якщо він необертовний, але з рівності $\pi = \beta\gamma$ випливає, що один з елементів β, γ є обертовним.

Легко бачити, що елемент $\alpha \in \Gamma$ є обертовним тоді й лише тоді, коли $\mathrm{N}(\alpha) = 1$, тобто $\alpha = \pm 1$ або $\alpha = \pm i$. Знайдемо всі незвідні елементи кільця Γ. Зауважимо, перш за все, що завжди α ділить $\mathrm{N}(\alpha)$, яке є натуральним числом. Зокрема, якщо число π є незвідним у Γ, то, розклавши $\mathrm{N}(\pi)$ на первинні (натуральні) множники, ми бачимо, що π мусить ділити якесь первинне число p. Але з рівності $p = \pi\beta$ випливає, що $\mathrm{N}(p) = p^2 = \mathrm{N}(\pi)\mathrm{N}(\beta)$. Оскільки $\mathrm{N}(\pi) \neq 1$, звідси маємо:

> або $\mathrm{N}(\pi) = p^2$ – тоді $\mathrm{N}(\beta) = 1$, елемент β обертовний і тому p сам є незвідним;
> або $\mathrm{N}(\pi) = p$ – тоді $\pi\overline{\pi} = p$, тобто $p = a^2 + b^2$ для натуральних a і b.

Оскільки відображення $\alpha \mapsto \overline{\alpha}$ є *ізоморфізмом*, тобто зберігає всі арифметичні операції, то елементи π та $\overline{\pi}$ є незвідними одночасно. Крім того, легко перевірити, що відношення $\overline{\pi}/\pi$ лежить в Γ тоді й лише тоді, коли $p = 2$, тобто $\pi = 1 \pm i$.

Залишилось визначити, які первинні натуральні числа є незвідними і в кільці ґауссових чисел. Для цього згадаємо, що з однозначності розкладу випливає наступний критерій незвідності (див. [**К**, гл.5, §3, Теорема 1]).

Твердження I.1.4. *Елемент π кільця з однозначним розкладом є незвідним тоді й лише тоді, коли з того, що він ділить добуток, випливає, що він ділить один із співмножників.*

Для кільця ґауссових чисел звідси випливає такий більш конкретний результат.

Наслідок I.1.5. *Первинне натуральне число p залишається незвідним у кільці ґауссових чисел тоді й лише тоді, коли порівняння $x^2 \equiv -1 \pmod{p}$ не має розв'язків* (тобто -1 не є квадратичним лишком за модулем p*).*

Доведення. Якщо це порівняння має розв'язок a, то $(a+i)(a-i) = a^2+1$ ділиться на p, причому обидва співмножники $a \pm i$ не діляться на p. Отже, число p не є незвідним. Навпаки, якщо p не є незвідним, то, як ми бачили вище, $p = a^2 + b^2$ для деяких цілих a і b. При цьому ясно, що $b \not\equiv 0 \pmod{p}$, а тому знайдеться ціле c, таке що $bc \equiv 1 \pmod{p}$. Звідси, очевидно, $(ac)^2 \equiv -1 \pmod{p}$. □

Зважаючи на критерій розв'язності порівняння $x^2 \equiv n \pmod{p}$ (див. [**ИВ**] або [**К**, гл.9, §2, вправа 7]), одержуємо остаточний результат.

Наслідок I.1.6. *Первинне натуральне число p є незвідним ґауссовим числом тоді й лише тоді, коли $p \equiv -1 \pmod{4}$.*

Остаточно одержуємо повний перелік незвідних ґауссових чисел (з точністю до обертовних множників). Ними є:

- первинні натуральні числа p, такі що $p \equiv -1 \pmod{4}$;

- числа $a \pm bi$, де a і b – такі натуральні числа, що $a^2 + b^2 = p$, де p натуральне первинне число, таке що $p \equiv 1 \pmod 4$;
- число $1 + i$.

Вправи I.1. (1) Доведіть наступне твердження (теорему Лаґранжа про два квадрати):

Рівняння $x^2 + y^2 = n$ (з цілими x, y і натуральним n) має розв'язок тоді й лише тоді, коли у розкладі числа n на первинні (натуральні) множники: $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, де всі p_j попарно різні, для кожного з дільників $p_j \equiv -1 \pmod 4$ показник k_j є парним.

(2) Знайдіть кількість "істотно різних" розв'язків рівняння $x^2+y^2 = n$ (тобто таких, які відрізняються не лише порядком і знаками x, y).

(3) Доведіть, що у кожному з перелічених нижче кілець існує алгоритм ділення з остачею:
   (a) $\mathbb{Z}[\sqrt{-2}] = \{ a + bi\sqrt{2} \mid a, b \in \mathbb{Z} \}$;
   (b) $\mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in Z \}$;
   (c) $\mathbb{Z}[\sqrt{3}] = \{ a + b\sqrt{3} \mid a, b \in Z \}$.

(4) Опишіть незвідні елементи у кільцях з попередньої вправи. Скористайтесь одержаними результатами для того, щоб дати критерії розв'язності (у цілих числах) рівнянь:
   (a) $x^2 + 2y^2 = n$;
   (b) $x^2 - 2y^2 = n$;
   (c) $x^2 - 3y^2 = n$.

(Для дослідження відповідних порівнянь скористайтесь квадратичним законом взаємності, див. [**ИВ**] чи [**К**, гл.9, §2], вправи 7 і 8).

I.2. Приклад 2. Неоднозначність розкладу

На відміну від кільця ґауссових чисел та від кілець, розглянутих у вправах до попереднього розділу, у багатьох, здавалося б, аналогічних випадках розклад на незвідні множники виявляється вже неоднозначним.

Наведемо один простий приклад. Розглянемо множину $A = \mathbb{Z}[\sqrt{-5}]$ усіх (комплексних) чисел вигляду $a + bi\sqrt{-5}$, де a і b – довільні цілі числа. Тривіально перевіряється, що A утворює кільце (відносно звичайних операцій множення і додавання). Так само, як для звичайних цілих чисел, будемо казати, що число $a \in A$ *ділить* $b \in A$ і писати $a \mid b$, якщо в кільці A має розв'язок рівняння $ax = b$. *Нормою* числа $a = a + bi\sqrt{-5}$ назвемо ціле число $\mathrm{N}(a) = |a|^2 = a^2 + 5b^2$. Тоді має місце таке просте твердження, доведення якого ми залишаємо читачеві.

Твердження I.2.1. (1) $\mathrm{N}(ab) = \mathrm{N}(a)\mathrm{N}(b)$; *зокрема, якщо* $a \mid b$, *то також і* $\mathrm{N}(a) \mid \mathrm{N}(b)$.

(2) $\mathrm{N}(a) = 1$ *тоді й лише тоді, коли* $a = \pm 1$*; зокрема,* ± 1 *– це єдині числа, на які діляться всі числа з* A.

(3) *В* A *немає чисел з нормою* 2 *або* 3.

Приклад I.2.2. (1) Число 2 є незвідним в A. Дійсно, якщо $2 = ab$, то $4 = \mathrm{N}(2) = \mathrm{N}(a)\mathrm{N}(b)$. Оскільки $\mathrm{N}(a) \neq 2$, то або $\mathrm{N}(a) = 1$, або $\mathrm{N}(b) = 1$. Якщо ж, наприклад, $\mathrm{N}(a) = 1$, то $a = \pm 1$, а $b = \pm 2$.

(2) Так само перевіряється, що числа 3 та $1 \pm i\sqrt{5}$ є незвідними.

Тепер очевидна тотожність:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

показує, що в кільці A *розклад чисел у добуток незвідних не є однозначним.*

Вправи I.2. (1) Покажіть, що у кільцях $\mathbb{Z}[\sqrt{d}]$ при $d = -3, -6, -7, -10$ розклад чисел на незвідні множники також не є однозначним.

(2) Позначимо $\omega = (1 + i\sqrt{3})/2$.

(a) Перевірте, що множина $\Lambda = \mathbb{Z}[\omega] = \{\, a + b\omega \mid a, b \in \mathbb{Z} \,\}$ є кільцем, яке містить підкільце $\mathbb{Z}[\sqrt{-3}]$.

(b) Доведіть, що у кільці Λ існує ділення з остачею відносно функції $\mathrm{N}(z) = |z|^2$.

(c) Які первинні натуральні числа залишаються незвідними в кільці Λ?

(d) Застосуйте одержані результати для дослідження рівняння $x^2 + 3y^2 = n$.

(3) Доведіть результати, аналогічні попередній вправі, замінивши $\sqrt{-3}$ на $\sqrt{-7}$ або $\sqrt{-11}$. Чи можна зробити те саме для $\sqrt{-5}$?

I.3. Цілі алгебричні числа

Розглянемо деяке розширення K поля $\mathbb{Q}$ раціональних чисел. Нагадаємо, що елемент $\alpha \in \mathsf{K}$ зветься *цілим алгебричним*, якщо він задовольняє рівняння "цілої залежності":

$$\alpha^n + c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n = 0 \tag{1}$$

з цілими коефіцієнтами c_j. Насправді, зручнішою є інша характеризація цілих алгебричних чисел, яку дає наступне твердження.

Твердження I.3.1. *Елемент* $\alpha \in \mathsf{K}$ *є цілими алгебричним тоді й лише тоді, коли існує такий скінченний набір ненульових елементів* $\omega_1, \omega_2, \ldots, \omega_n \in \mathsf{K}$*, що*

$$\alpha\omega_j = \sum_{i=1}^{n} c_{ij}\omega_i \quad \text{для кожного } j = 1 \ldots n, \text{ де } c_{ij} \in \mathbb{Z}. \tag{2}$$

Про такий набір $\{\, \omega_j \,\}$ ми казатимемо, що він *визначає цілість елемента* α.

Доведення. Якщо α задовольняє рівняння (1), то, очевидно, досить покласти $\omega_j = \alpha^{j-1}$. Навпаки, припустимо, що знайдуться елементи ω_j, для яких виконуються рівності (2). Позначимо C матрицю розміру $n \times n$ з коефіцієнтами c_{ij} і $\overline{\omega}$ – вектор з координатами ω_j. Тоді рівності (2) означають, що α є власним числом матриці C, а $\overline{\omega}$ – відповідним власним вектором. Отже, α є коренем характеристичного многочлена $\chi(x)$ матриці C. Оскільки всі коефіцієнти цієї матриці – цілі числа, то і коефіцієнти $\chi(x)$ також є цілими, що і дає необхідну рівність вигляду (1). □

Наслідок I.3.2. *Для довільного скінченного набору цілих алгебричних елементів $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathsf{K}$ знайдеться такий скінченний набір $\omega_1, \omega_2, \ldots, \omega_n \in \mathsf{K}$, який визначає цілість одночасно всіх елементів α_k $(k = 1 \ldots s)$.*

Доведення. Скористаймося індукцією за s. База індукції, $s = 1$ – це твердження I.3.1. Припустимо, що ми вже побудували необхідний набір $\{\omega_k\}$, який визначає цілість $\alpha_1, \alpha_2, \ldots, \alpha_{s-1}$. Існує також набір $\{\theta_l\}$, який визначає цілість ω_s. Тоді очевидно, що набір $\{\omega_k \theta_l\}$ визначає цілість усіх елементів $\alpha_1, \alpha_2, \ldots, \alpha s$. □

Звідси безпосередньо випливає наступне важливе твердження.

Наслідок I.3.3. (1) *Цілі алгебричні елементи поля K утворюють підкільце A в цьому полі.*

(2) *Підкільце A є цілозамкненим у полі K, тобто якщо якийсь елемент $\beta \in \mathsf{K}$ задовольняє рівняння*

$$\beta^m + \alpha_1 \beta^{m-1} + \alpha_2 \beta^{m-2} + \cdots + \alpha_m = 0\,, \text{ де всі } \alpha_k \in \mathsf{A}\,, \tag{3}$$

то і сам елемент β належить A.

Доведення. Легко бачити, що коли деякий набір $\{\omega_j\}$ визначає цілість одночасно елементів α і β, то він визначає також цілість $\alpha + \beta$ і $\alpha\beta$, що доводить перше твердження. Для доведення другого, виберемо набір $\{\omega_j\}$, який визначає цілість усіх коефіцієнтів α_k рівняння (3). Тоді знов-таки безпосередньо перевіряється, що набір $\{\beta^l \omega_j \mid l < m\}$ визначає цілість елемента β. □

Зазначимо, що у застосуванні до *раціональних чисел* поняття цілого алгебричного числа не дає нічого нового.

Твердження I.3.4. *Якщо раціональне число є цілим алгебричним, то воно є цілим числом.*

Доведення. Запишемо раціональне число α у вигляді нескоротного дробу: $\alpha = a/b$, де a і b – співпервинні цілі числа. Якщо α задовольняє рівняння (1), то, домноживши його на b^n, маємо:

$$a^n + c_1 b a^{n-1} + c_2 b^2 a^{n-2} + \cdots + c_n b^n = 0\,,$$

звідки випливає, що a^n ділиться на b, що неможливо, якщо тільки $b \neq \pm 1$. $\square$

Нагадаємо, що *мінімальним многочленом* елемента $\alpha \in \mathsf{K}$ (над полем раціональних чисел) зветься многочлен $\mu_\alpha(x) \in \mathbb{Q}[x]$ зі старшим коефіцієнтом 1 і найменшого можливого ступеня, такий що $\mu_\alpha(\alpha) = 0$. З відсутності дільників нуля в полі, очевидно, випливає, що цей многочлен є незвідним. Крім того, легко перевірити, що мінімальний многочлен є дільником довільного многочлена $f(x)$, такого що $f(\alpha) = 0$.

Наслідок I.3.5. *Елемент $\alpha \in \mathsf{K}$ є цілим алгебричним тоді й лише тоді, коли всі коефіцієнти його мінімального многочлена є цілими.*

Доведення. Достатність цієї умови очевидна. Доведемо її необхідність. Нехай α є коренем многочлена $f(x)$ з цілими коефіцієнтами і старшим коефіцієнтом 1. Розглянемо поле розкладу цього многочлена над полем K (див. [**K**, гл.6, §3, п.2]). У цьому полі $f(x)$ розкладається на лінійні множники. Оскільки $\mu_\alpha(x)$ – дільник $f(x)$, він також розкладається на лінійні множники: $\mu_\alpha(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_m)$, причому всі α_j є коренями $f(x)$, тобто цілими алгебричними числами. З формул Вієта і наслідку I.3.3 випливає тоді, що всі коефіцієнти $\mu_\alpha(x)$ є цілими алгебричними, а оскільки вони раціональні, то й цілими числами. $\square$

Припустимо тепер, що розширення K поля $\mathbb{Q}$ є *алгебричним*, тобто кожен його елемент γ є коренем ненульового многочлена з раціональними коефіцієнтами. Домноживши на спільний знаменник, можна вважати, що всі коефіцієнти цього многочлена є цілими, тобто

$$c_0\gamma^n + c_1\gamma^{n-1} + c_2\gamma^{n-2} + \dots + c_n = 0$$

для деяких цілих c_j. Домноживши цю рівність на c_0^{n-1}, одержимо для елемента $\alpha = c_0\gamma$ рівняння цілої залежності:

$$\alpha^n + c_1\alpha^{n-1} + c_0c_2\alpha^{n-2} + \dots + c_0^{n-1}c_n = 0\,.$$

Отже, $\gamma = \alpha/c_0$, де елемент α – цілий алгебричний, а c_0 – ціле число. Зокрема, поле K збігається з *полем часток* кільця A.

Наприклад, усі комплексні числа, які є цілими алгебричними, утворюють підкільце в полі комплексних чисел – *кільце всіх цілих алгебричних чисел*, полем часток якого є все поле алгебричних чисел. Втім, кільце всіх цілих алгебричних чисел є надто великим. Нас найбільше цікавитимуть кільця алгебричних елементів у *скінченних розширеннях* K поля $\mathbb{Q}$, тобто таких, які мають скінченну розмірність $(\mathsf{K} : \mathbb{Q})$ як векторні простори над $\mathbb{Q}$ (ця розмірність зветься *ступенем* поля K як розширення поля раціональних чисел). *Надалі ми розглядатимемо лише скінченні розширення* (крім окремих випадків, які буде спеціально обумовлено).

Нагадаємо деякі факти, що стосуються таких розширень. З кожним елементом $\alpha \in \mathsf{K}$ пов'язується лінійне відображення $L_\alpha : \mathsf{K} \to \mathsf{K}$ "множення на α", яке переводить довільний елемент β в $\alpha\beta$. Позначимо $\chi_{\mathsf{K}}(\alpha; x)$ характеристичний многочлен цього відображення. Його звуть також *характеристичним многочленом елемента* α у полі K. Слід та детермінант лінійного відображення L_α звуть відповідно *слідом* і *нормою* елемента α поля K і позначають відповідно $\mathrm{Tr}_{\mathsf{K}}(\alpha)$ та $\mathrm{N}_{\mathsf{K}}(\alpha)$ [1]. Якщо поле K фіксоване, індекс K у позначеннях для сліду, норми і характеристичного многочлена часто будемо опускати. Встановимо зв'язок між характеристичним і мінімальним многочленами.

Твердження I.3.6. *Характеристичний многочлен довільного елемента поля* K *є ступенем його мінімального многочлена.*

Доведення. Позначимо $\mu(x) = \mu_\alpha(x) = x^m + c_1 x^{m-1} + \cdots + c_m$. Припустимо спочатку, що $\mathsf{K} = \mathbb{Q}(\alpha)$. Тоді $(\mathsf{K} : \mathbb{Q}) = \deg \mu(x)$ і елементи $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ утворюють базу простору K (див. [**K**, гл.9, §1, п.1]). У цій базі матриця відображення L_α має вигляд "клітини Фробеніуса" Φ_μ, де

$$\Phi_\mu = \begin{pmatrix} 0 & 0 & \ldots & 0 & -c_m \\ 1 & 0 & \ldots & 0 & -c_{m-1} \\ 0 & 1 & \ldots & 0 & -c_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_1 \end{pmatrix}$$

Безпосереднє обчислення дає тоді, що $\chi_{\mathsf{K}}(\alpha; x) = \mu(x)$.

У загальному випадку розглянемо в полі K підполе $\mathsf{L} = \mathbb{Q}(\alpha)$. Виберемо якусь базу $\theta_1, \theta_2, \ldots, \theta_m$ поля L над полем раціональних чисел і якусь базу $\omega_1, \omega_2, \ldots, \omega_l$ поля K як векторного простору над підполем L. Тоді всі добутки $\theta_i \omega_j$ утворюють базу поля K над $\mathbb{Q}$ (див. [**K**, гл.9, §1, п.1]). Знов-таки легко переконатися, що в цій базі матриця відображення L_α має вигляд:

$$\begin{pmatrix} L_0 & 0 & \ldots & 0 \\ 0 & L_0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & L_0 \end{pmatrix},$$

де L_0 – матриця відображення "множення на α" у полі L. Оскільки, як ми вже перевірили, $\chi_{\mathsf{L}}(\alpha; x) = \mu(x)$, звідси маємо, що $\chi_{\mathsf{K}}(\alpha; x) = \mu(x)^l$. □

Зауваження I.3.7. Останнє твердження (разом із доведенням) залишається справедливим для скінченного розширення довільного поля.

[1] Легко бачити, що функції N, застосовані в попередніх розділах, дійсно збігаються з нормами у відповідних полях.

Наслідок I.3.8. *Елемент α поля K є цілим алгебричним тоді й лише тоді, коли $\chi_{\mathsf{K}}(\alpha; x) \in \mathbb{Z}[x]$. Зокрема, слід і норма цілого алгебричного числа – цілі числа.*

Зауважимо, що з означення сліду і норми безпосередньо випливають наступні їхні властивості:

$$\begin{array}{rclrcl} \mathrm{Tr}(\alpha+\beta) &=& \mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)\,, & \mathrm{Tr}(c\alpha) &=& c\mathrm{Tr}(\alpha)\,; \\ \mathrm{N}(\alpha\beta) &=& \mathrm{N}(\alpha)\mathrm{N}(\beta)\,, & \mathrm{N}(c\alpha) &=& c^n\mathrm{N}(\alpha)\,; \\ \mathrm{Tr}(c) &=& nc\,, & \mathrm{N}(c) &=& c^n\,. \end{array} \tag{4}$$

Тут α, β – довільні елементи поля K, c – раціональне число, а $n = (\mathsf{K} : \mathbb{Q})$.

Визначимо на просторі K симетричну білінійну форму $\mathrm{T} = \mathrm{T}_{\mathsf{K}}$ – *форму сліду*, поклавши $\mathrm{T}(\alpha, \beta) = \mathrm{Tr}(\alpha\beta)$. Ця форма завжди є *невиродженою*, оскільки $\mathrm{T}(\alpha, \alpha^{-1}) = \mathrm{Tr}(1) = n \neq 0$. Звідси випливає наступна теорема, яка має принципове значення для вивчення цілих алгебричних чисел.

Теорема I.3.9. *Нехай K – розширення ступеня n поля раціональних чисел. Тоді адитивна група кільця A всіх цілих алгебричних елементів цього поля є вільною абелевою групою рангу n, тобто знайдуться такі елементи $\omega_1, \omega_2, \ldots, \omega_n \in \mathsf{A}$, що довільний елемент кільця A однозначно подається як лінійна комбінація $\sum_{i=1}^{n} c_i\omega_i$ з цілими коефіцієнтами c_i.*

Доведення. Виберемо деяку базу $\beta_1, \beta_2, \ldots, \beta_n$ поля K над $\mathbb{Q}$. Кожен елемент цієї бази можна подати у вигляді: $\beta_i = \alpha_i/d_i$, де $\alpha_i \in \mathsf{A}$, а $d_i \in \mathbb{Z}$. Домноживши на спільне кратне всіх знаменників d_i, можна вважати, що вже $\beta_i \in \mathsf{A}$ для всіх номерів i. Оскільки форма T є невиродженою, існує *двоїста база* $\beta_1^*, \beta_2^*, \ldots, \beta_n^*$, тобто така, що

$$\mathrm{T}(\beta_i, \beta_j^*) = \delta_{ij=} \begin{cases} 1 & \textit{при } i = j\,, \\ 0 & \textit{при } i \neq j\,. \end{cases}$$

Припустимо, що $\alpha \in \mathsf{A}$. Розкладемо α за базою $\left\{ \beta_j^* \right\}$: $\alpha = \sum_{j=1}^{n} a_j\beta_j^*$, де $a_j \in \mathbb{Q}$. Легко бачити, що тоді $a_i = \mathrm{T}(\beta_i, \alpha) = \mathrm{Tr}(\alpha\beta_i)$. За Наслідком I.3.8 усі числа a_i – цілі. Отже, A є підгрупою в групі, породженій елементами $\beta_1^*, \beta_2^*, \ldots, \beta_n^*$. Оскільки ці елементи лінійно незалежні, остання група є, очевидно, вільною абелевою рангу n. Але відомо (див., напр., [**Ф**]), що підгрупа вільної абелевої групи знов є вільною абелевою, причому її ранг не перевищує рангу всієї групи. Отже, адитивна група кільця A є вільною абелевою рангу не більшого за n. З іншого боку, A містить підгрупу, породжену елементами $\beta_1, \beta_2, \ldots, \beta_n$, яка теж є вільною абелевою рангу n. Тому ранг A не може бути меншим за n. □

Означення I.3.10. *Фундаментальною базою* поля K (або кільця A) зветься будь-яка база вільної абелевої групи A, тобто такий набір

$\omega_1, \omega_2, \ldots, \omega_n$ цілих алгебричних елементів, що довільне ціле алгебричне число з поля K однозначно розкладається в суму $\sum_{i=1}^{n} c_i\omega_i$ з цілими коефіцієнтами c_i.

Насправді останню теорему можна розповсюдити також на *ідеали* кільця A.

Наслідок I.3.11. *Якщо* $\mathbf{I}$ *– довільний ненульовий ідеал кільця* A *цілих алгебричних елементів деякого розширення ступеня* n *поля раціональних чисел, то його адитивна група є вільною абелевою рангу* n*, а факторкільце* $\mathsf{A}/\mathbf{I}$ *є скінченним.*

База адитивної групи ідеалу $\mathbf{I}$ зветься також *базою ідеалу* $\mathbf{I}$.

Доведення. Оскільки $\mathbf{I}$ – підгрупа в A, вона є вільною абелевою рангу $m \le n$. З іншого боку, якщо $\omega_1, \omega_2, \ldots, \omega_n$ – фундаментальна база кільця A, а $\alpha \in \mathbf{I}$ – ненульовий елемент, то елементи $\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_n$ лежать в ідеалі $\mathbf{I}$ і є лінійно незалежними. Звідси випливає, що $m \ge n$, тобто $m = n$. Скористаймося тепер теоремою про існування *узгоджених баз* у вільній абелевій групі та її підгрупі (див., напр., [**Ф**]). Оскільки ранги цих груп рівні, з цієї теореми випливає, що існують бази $\omega_1, \omega_2, \ldots, \omega_n$ в групі A та $\beta_1, \beta_2, \ldots, \beta_n$ в групі $\mathbf{I}$, такі що $\beta_i = d_i\omega_i$ для всіх номерів i, де d_i – натуральні числа. Але тоді, очевидно, кількість різних класів суміжності у факторгрупі $\mathsf{A}/\mathbf{I}$ дорівнює $d_1 d_2 \ldots d_n$. □

Вправи I.3. (1) Нехай K – *квадратичне поле*, тобто $(\mathsf{K} : \mathbb{Q}) = 2$.
   (a) Доведіть, що існує єдине ціле число d, яке не ділиться на квадрати первинних чисел, таке що $\mathsf{K} = \mathbb{Q}(\theta)$, де $\theta^2 = d$ (звичайно пишуть $\mathsf{K} = \mathbb{Q}(\sqrt{d})$).
   (b) Доведіть, що фундаментальною базою в K є $\{1, \theta\}$, якщо $d \not\equiv -1 \pmod 4$, і $\{1, (1+\theta)/2\}$, якщо $d \equiv -1 \pmod 4$ (скористайтесь тим, що в даному випадку $\alpha \in \mathsf{A}$ тоді й лише тоді, коли $\mathrm{Tr}(\alpha)$ і $\mathrm{N}(\alpha)$ – цілі числа).

(2) Доведіть, що довільне кільце без дільників нуля з однозначним розкладом на незвідні множники є цілозамкненим у своєму полі часток. (Це пояснює, зокрема, деякі з прикладів вправи I.2 (1), саме випадки $d = -3$ і $d = -7$).

(3) Нехай A – кільце цілих елементів деякого скінченного розширення поля раціональних чисел, $\alpha \in \mathsf{A}$. Довести, що $|\mathrm{N}(\alpha)| = (\mathsf{A} : \alpha\mathsf{A})$.

(4) Нехай D – евклідове кільце відносно деякої функції $\delta : \mathsf{D} \setminus \{0\} \to \mathbb{N} \cup \{0\}$ (див. [**K**, гл.5, §3, п.3]).
   (a) Довести, що елемент $\alpha \in \mathsf{D}$ є обертовним в D тоді й лише тоді, коли $\delta(\alpha) = \delta(1)$.
   (b) Нехай α – необертовний елемент з D з найменшим можливим значенням $\delta(\alpha)$. Довести, що для довільного елемента

$\beta \in \mathsf{D}$, який не ділиться на α, існує такий обертовний елемент ε, що $\beta \equiv \varepsilon \pmod{\alpha}$.

(c) Нехай $\mathsf{K} = \mathbb{Q}(\sqrt{d})$, де $d < 0$, A – кільце цілих елементів поля K. Довести, що коли кільце A є евклідовим, то в ньому існує елемент α, такий що $\mathrm{N}(\alpha) \leq 3$ (скористайтеся тим, що $\mathrm{N}(\alpha) = |\mathsf{A}/\alpha\mathsf{A}|$; випадки $d = -1$ та $d = -3$ зручно розглянути окремо).

(d) За умов попередньої вправи довести, що кільце A є евклідовим лише при $d \in \{-1, -2, -3, -7, -11\}$.

(5) Нехай $\mathsf{K} = \mathbb{Q}(\theta)$, де θ – корінь незвідного многочлена $f(x) \in \mathbb{Q}[x]$ ступеня n, $\mathsf{L} \supseteq \mathsf{K}$ – деяке поле розкладу многочлена $f(x)$ і $\theta_1, \theta_2, \ldots, \theta_n$ – всі корені цього многочлена в полі L. Позначимо $\varphi_j : \mathsf{K} \to \mathsf{L}$ гомоморфізм, який переводить θ в θ_j. Доведіть, що для довільного елемента $\alpha \in \mathsf{K}$

$\chi_{\mathsf{K}}(\alpha;\, x) = \prod_{j=1}^{n}(x - \varphi_j(\alpha))$;
$\mathrm{Tr}_{\mathsf{K}}(\alpha) = \sum_{j=1}^{n} \varphi_j(\alpha)$;
$\mathrm{N}_{\mathsf{K}}(\alpha) = \prod_{j=1}^{n} \varphi_j(\alpha)$.

(6) Нехай F – довільне поле, $\mathsf{K} \supseteq \mathsf{F}$ – його скінченне розширення ступеня $n = (\mathsf{K} : \mathsf{F})$.

(a) Означте *мінімальний* і *характеристичний многочлени*, *слід* і *норму* елемента $\alpha \in \mathsf{K}$ відносно поля F (якщо треба явно вказати поле F, то у відповідних позначеннях пишуть $\chi_{\mathsf{K}/\mathsf{F}}$ і т.п.).

(b) Доведіть наступні формули для випадку "башти полів" $\mathsf{F} \subseteq \mathsf{L} \subseteq \mathsf{K}$:

$$\begin{aligned} \mathrm{Tr}_{\mathsf{K}/\mathsf{F}}(\alpha) &= \mathrm{Tr}_{\mathsf{L}/\mathsf{F}}(\mathrm{Tr}_{\mathsf{K}/\mathsf{L}}(\alpha)); \\ \mathrm{N}_{\mathsf{K}/\mathsf{F}}(\alpha) &= \mathrm{N}_{\mathsf{L}/\mathsf{F}}(\mathrm{N}_{\mathsf{K}/\mathsf{L}}(\alpha)); \\ \chi_{\mathsf{K}/\mathsf{F}}(\alpha;\, x) &= \mathrm{N}_{\mathsf{L}(x)/\mathsf{F}(x)}(\chi_{\mathsf{K}/L}(\alpha;\, x)). \end{aligned}$$

(7) Нехай $\mathbf{k}$ – деяке поле, $\mathsf{P} = \mathbf{k}[x]$ – кільце многочленів і $\mathsf{F} = \mathbf{k}(x)$ – поле раціональних функцій від однієї змінної над $\mathbf{k}$. Скінченні розширення поля F звуться *полями алгебричних функцій* (від однієї змінної) над полем $\mathbf{k}$. Елемент $\alpha \in \mathsf{K}$ поля алгебричних функцій зветься *цілим*, якщо він задовольняє рівняння $\alpha^m + c_1\alpha^{m-1} + \cdots + c_m = 0$, де $c_i \in \mathsf{P}$. Сформулюйте і доведіть для цілих алгебричних функцій результати, аналогічні твердженням I.3.1 та I.3.6 і наслідкам з них (зокрема, наслідку I.3.3).

(8) Збережемо позначення і термінологію попередньої вправи.

(a) Нехай K – *сепарабельне розширення* поля F (див., напр., [**ВВ**] чи [**Л1**]), A – підкільце всіх цілих елементів поля K.

Доведіть, що A, розглянуте як *модуль* над кільцем многочленів P, є вільним модулем рангу $n = (\mathsf{K} : \mathsf{F})$. (Скористайтесь тим, що P є евклідовим кільцем і, наприклад, теоремою 2 з книги [**K**, гл.9, §3, п.2]).

(b) Якщо $\operatorname{char}\mathbf{k} = p > 0$, а $\mathsf{K} = \mathsf{F}(\theta)$, де $\theta^p \in \mathsf{F}$, доведіть, що $\mathsf{A} \subseteq \mathsf{K}\mathbf{k}'(\sqrt[p]{x})$, де $\mathbf{k}'$ – скінченне розширення поля $\mathbf{k}$.

(c) Доведіть, що результат вправи 8a залишається справедливим і для довільного поля алгебричних функцій.

(d) Доведіть, що довільний (ненульовий) ідеал $\mathbf{I}$ кільця A цілих алгебричних функцій також є вільним модулем рангу n над кільцем многочленів P, причому факторкільце $\mathsf{A}/\mathbf{I}$ є скінченновимірною алгеброю над полем $\mathbf{k}$.

(e) Припустимо, що $\operatorname{char}\mathbf{k} \neq 2$, а $(\mathsf{K} : \mathsf{F}) = 2$. Доведіть, що знайдеться єдиний многочлен $d(x)$, який не ділиться на квадрат жодного незвідного многочлена, такий що $\mathsf{K} = \mathsf{F}(\sqrt{d(x)})$, а $\mathsf{A} = \mathsf{P}[\sqrt{d(x)}]$.

База кільця A як P-модуля зветься *фундаментальною базою* поля алгебричних функцій K.

I.4. Дедекіндові кільця. Теорія ідеалів

Видатним відкриттям математиків XIX сторіччя був той факт, що однозначність розкладу на множники в кільцях алгебричних чисел можна відновити, якщо замість *елементів* розглядати *ідеали* цих кілець. Насправді, вже у "класичному" випадку кілець з однозначним розкладом ми фактично користувалися ідеалами, коли ототожнювали елементи, які відрізняються обертовним множником. Ясно, що це – ті елементи, які породжують один і той самий головний ідеал. І справжньою причиною виникнення неоднозначності розкладу в кільцях алгебричних чисел виявляється те, що, на відміну від кільця цілих чисел чи многочленів, в них вже не всі ідеали є головними.

Так само, як теорія подільності цілих чисел природно поширюється на досить великий клас кілець – кільця головних ідеалів (зокрема, евклідові кільця), теорію подільності для кілець алгебричних чисел також природно будувати у більш загальному контексті. Це приводить до наступного означення.

Означення I.4.1. Кільце[2] D без дільників нуля зветься *дедекіндовим*, якщо воно задовольняє наступні умови:

D1. Кільце D є *нетеровим*, тобто довільний ідеал у ньому має скінченну множину твірних.

D2. Кільце D є цілозамкненим у своєму полі часток.

D3. Довільний ненульовий первинний ідеал кільця D є максимальним.

[2]Нагадаємо, що всі кільця вважаються комутативними.

Нагадаємо, що *множиною твірних* ідеалу $\mathbf{I}$ кільця D зветься такий набір його елементів $\beta_1, \beta_2, \ldots, \beta_m$, що кожен елемент ідеалу $\mathbf{I}$ має вигляд $\sum_{i=1}^{m} \alpha_i \beta_i$ для деяких $\alpha_i \in \mathsf{D}$. Ідеал $\mathfrak{p} \subset \mathsf{D}$ зветься *первинним* (або *простим*), якщо у факторкільці $\mathsf{D}/\mathfrak{p}$ немає дільників нуля, тобто з того, що $ab \in \mathfrak{p}$, випливає, що $a \in \mathfrak{p}$ або $b \in \mathfrak{p}$. Ідеал $\mathfrak{p} \subset \mathsf{D}$ зветься *максимальним*, якщо не існує такого ідеалу $\mathbf{I}$, що $\mathfrak{p} \subset \mathbf{I} \subset \mathsf{D}$. Легко бачити, що остання умова рівносильна тому, що факторкільце $\mathsf{D}/\mathfrak{p}$ є полем (див. напр. [**K**, гл.9, §2, п.2]). Зокрема, максимальний ідеал завжди є первинним (але, звичайно, не навпаки: наприклад, у кільці без дільників нуля нульовий ідеал є первинним).

Теорема I.4.2. *Для довільного скінченного розширення* K *поля раціональних чисел кільце* A *всіх цілих елементів поля* K *є дедекіндовим.*

Доведення. Властивість *(D1)* безпосередньо випливає з наслідку I.3.11. Властивість *(D2)* для кільця A вже відома (наслідок I.3.3). Властивість *(D3)* випливає з наслідку I.3.11 і наступного простого факту.

Теорема I.4.3. *Скінченне кільце без дільників нуля є полем.*

Доведення. Нехай $\mathsf{F} = \{ a_1, a_2, \ldots, a_m \}$ – скінченне кільце, $b \in \mathsf{F}$ – довільний ненульовий елемент. Оскільки дільників нуля немає, всі елементи $ba_1, ba_2, \ldots, ba_m$ – різні, зокрема, серед них є й одиничний елемент. Отже, $ba_j = 1$ для деякого номера j, тобто $a_j = b^{-1}$. □

Отже, теорему I.4.2 повністю доведено. Сформулюємо тепер основну теорему про арифметику дедекіндових кілець. Нагадаємо, що *добутком* двох ідеалів, $\mathbf{I}$ та $\mathbf{J}$, зветься ідеал $\mathbf{IJ} = \left\{ \sum_j \alpha_j \beta_j \mid \alpha_j \in \mathbf{I},\ \beta_j \in \mathbf{J} \right\}$.

Теорема I.4.4. *Довільний ненульовий ідеал* $\mathbf{I} \neq \mathsf{D}$ *дедекіндова кільця* D *однозначно (з точністю до порядку співмножників) розкладається у добуток первинних ідеалів:* $\mathbf{I} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_s$.

Доведення розіб'ємо на ряд тверджень, які мають і самостійне значення.

Твердження I.4.5. *Нехай* D *– нетерове кільце. Тоді:*

(1) *Довільний зростаючий ланцюг ідеалів* $\mathbf{I}_1 \subset \mathbf{I}_2 \subset \ldots \subset \mathbf{I}_k \subset \ldots$ *є скінченним.*
(2) *Довільний ідеал* $\mathbf{I}$ *містить деякий добуток первинних ідеалів, кожен з яких, у свою чергу, містить* $\mathbf{I}$.

Доведення. *1.* Легко бачити, що об'єднання $\mathbf{I} = \bigcup_k \mathbf{I}_k$ знов є ідеалом. Оскільки кільце нетерове, він має скінченну множину твірних, кожен з елементів якої належить одному з ідеалів $\mathbf{I}_k$. Тоді, взявши найбільше значення k, ми бачимо, що $\mathbf{I} \subseteq \mathbf{I}_k$, тобто наш ланцюг закінчується на ідеалі $\mathbf{I}_k$.

2. Припустимо, що якийсь ідеал $\mathbf{I}$ не містить жодного добутку первинних ідеалів. Тоді, зокрема, сам $\mathbf{I}$ не первинний, тобто існують елементи $\alpha, \beta \notin \mathbf{I}$, такі що $\alpha\beta \in \mathbf{I}$. Розглянемо ідеали $\mathbf{I}' = \mathbf{I} + \alpha\mathsf{D}$ та $\mathbf{I}'' = \mathbf{I} + \beta\mathsf{D}$. Очевидно, $\mathbf{I}'\mathbf{I}'' \subseteq \mathbf{I}$. Тому, якщо $\mathbf{I}'$ містить добуток первинних $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_s$, де $\mathfrak{p}_i \supseteq \mathbf{I}'$, а $\mathbf{I}''$ містить добуток первинних $\mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_t$, де $\mathfrak{q}_j \supseteq \mathbf{I}''$, то й $\mathbf{I}$ містить добуток первинних $\mathfrak{p}_1 \dots \mathfrak{p}_s\mathfrak{q}_1 \dots \mathfrak{q}_t$, причому всі ці ідеали містять $\mathbf{I}$. Отже, принаймні один з ідеалів $\mathbf{I}', \mathbf{I}''$ теж не містить жодного добутку первинних. Позначимо цей ідеал $\mathbf{I}_1$. Зауважимо, що $\mathbf{I} \subset \mathbf{I}_1$. Застосувавши до ідеалу $\mathbf{I}_1$ ті самі міркування, побудуємо ще більший ідеал $\mathbf{I}_2 \supset \mathbf{I}_1$, який теж не містить жодного добутку первинних. Продовжуючи цю побудову, одержимо *нескінченний* ланцюг ідеалів $\mathbf{I} \subset \mathbf{I}_1 \subset \mathbf{I}_2 \dots$, що неможливо. □

Твердження I.4.6. *Нехай* D *– нетерове кільце без дільників нуля, цілозамкнене у своєму полі часток* F, $\mathbf{I}$ *– ненульовий ідеал в* D *а* $\gamma \in \mathsf{F}$ *– такий елемент, що* $\gamma\mathbf{I} \subseteq \mathbf{I}$. *Тоді* $\gamma \in \mathsf{D}$.

Доведення. Виберемо скінченну множину твірних $\{\omega_1, \omega_2, \ \dots, \omega_m\}$ ідеалу $\mathbf{I}$. Тоді $\gamma\omega_j = \sum_{i=1}^{m} \alpha_{ij}\omega_i$ для кожного номера j. Усі ці рівності разом можна записати у матричному вигляді: $\gamma\overline{\omega} = A\overline{\omega}$, де $\overline{\omega}$ – вектор з координатами ω_j, а A – матриця з коефіцієнтами α_{ij}. Звідси випливає, що γ є коренем характеристичного многочлена $h(x)$ матриці A. Але останній є многочленом з коефіцієнтами з D і старшим коефіцієнтом 1. Оскільки D є цілозамкненим, $\gamma \in \mathsf{D}$. □

Нехай тепер D – дедекіндове кільце, F – його поле часток. Надалі, кажучи "ідеал", ми завжди будемо вважати, що цей ідеал ненульовий. Для довільного ідеалу $\mathbf{I}$ позначимо $\mathbf{I}^{-1} = \{\, \gamma \in \mathsf{F} \,|\, \gamma\mathbf{I} \subseteq \mathsf{D} \,\}$. Очевидно, що $\mathbf{I}^{-1}$ є D-*підмодулем* в F, тобто підгрупою, яка переходить в себе при множенні на довільний елемент $\alpha \in \mathsf{D}$. Крім того, ясно, що $\mathbf{I}^{-1} \supseteq \mathsf{D}$. Тому добуток $\mathbf{I}^{-1}\mathbf{I}$ є ідеалом кільця D, який містить $\mathbf{I}$.

Твердження I.4.7. $\mathfrak{p}^{-1}\mathfrak{p} = \mathsf{D}$ *для довільного первинного ідеалу* $\mathfrak{p}$ *кільця* D.

Доведення. Візьмемо довільний ненульовий елемент $\alpha \in \mathfrak{p}$. Тоді за твердженням I.4.5 (2) ідеал $\alpha\mathsf{D}$ містить якийсь добуток первинних. Серед усіх таких добутків виберемо добуток $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m$ з найменшою кількістю співмножників m. Оскільки $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m \subseteq \mathfrak{p}$, а ідеал $\mathfrak{p}$ первинний, знайдеться номер i, для якого $\mathfrak{p}_i \subseteq \mathfrak{p}$. Але за умовою первинний ідеал $\mathfrak{p}_i$ є максимальним. Тому $\mathfrak{p}_i = \mathfrak{p}$. Для простоти вважаємо, що $i = 1$. Зауважимо, що $\mathfrak{p}_2 \dots \mathfrak{p}_m \not\subseteq \alpha\mathsf{D}$. Візьмемо якийсь елемент $\beta \in \mathfrak{p}_2 \dots \mathfrak{p}_m \setminus \alpha\mathsf{D}$. Тоді $\beta\eta \in \alpha\mathsf{D}$ для довільного елемента $\eta \in \mathfrak{p}$, звідки випливає, що $(\beta/\alpha) \in \mathfrak{p}^{-1}$. З іншого боку, $(\beta/\alpha) \notin \mathsf{D}$, отже, за твердженням I.4.6 $(\beta/\alpha)\mathfrak{p} \not\subseteq \mathfrak{p}$. Тому маємо: $\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathsf{D}$. Оскільки ідеал $\mathfrak{p}$ максимальний, звідси випливає, що $\mathfrak{p}^{-1}\mathfrak{p} = \mathsf{D}$. □

Будемо казати, що ідеал $\mathbf{I}$ *ділить* ідеал $\mathbf{J}$, якщо існує такий ідеал $\mathbf{I}'$, що $\mathbf{I}\mathbf{I}' = \mathbf{J}$. Ясно, що тоді $\mathbf{I} \supseteq \mathbf{J}$.

Наслідок I.4.8. *Якщо первинний ідеал* $\mathfrak{p}$ *містить ідеал* $\mathbf{I}$, *то він його ділить, а саме,* $\mathbf{I} = \mathfrak{p}(\mathfrak{p}^{-1}\mathbf{I})$.

Доведення. Дійсно, якщо $\mathfrak{p} \supseteq \mathbf{I}$, то $\mathfrak{p}^{-1}\mathbf{I}$ – ідеал в D, причому $\mathfrak{p}(\mathfrak{p}^{-1}\mathbf{I}) = (\mathfrak{p}\mathfrak{p}^{-1})\mathbf{I} = \mathsf{D}\mathbf{I} = \mathbf{I}$. □

Тепер ми вже можемо довести теорему I.4.4. Спочатку доведемо *існування* розкладу. Припустимо, що ненульовий ідеал $\mathbf{I}$ не розкладається у добуток первинних (зокрема, сам не є первинним). Із твердження I.4.5 (1) випливає, що $\mathbf{I} \subset \mathfrak{p}$ для деякого максимального, а тому первинного, ідеалу $\mathfrak{p}$. За Наслідком I.4.8, $\mathbf{I} = \mathfrak{p}\mathbf{I}_1$, де $\mathbf{I}_1 = \mathfrak{p}^{-1}\mathbf{I}$. Оскільки $\mathfrak{p}^{-1} \supset \mathsf{D}$, із твердження I.4.6 випливає, що $\mathbf{I} \subset \mathbf{I}_1$. Якщо $\mathbf{I}_1 = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_s$ для деяких первинних $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s$, то $\mathbf{I} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_s$, що протирічить припущенню. Отже, ідеал $\mathbf{I}_1$ теж не розкладається у добуток первинних. Ітеруючи цю побудову, ми одержимо нескінченний ланцюг $\mathbf{I} \subset \mathbf{I}_1 \subset \mathbf{I}_2 \subset \dots$, що протирічить твердженню I.4.5 (1). Отже, наше припущення невірне, тобто $\mathbf{I} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_s$ для деяких первинних $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s$.

Нехай дано ще якийсь розклад $\mathbf{I} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_t$. Тоді з того, що $\mathfrak{p}_1 \supseteq \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_t$, випливає, що $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$ для деякого номера j. Оскільки ми дозволили переставляти співмножники, вважаймо, що $j = 1$. Тоді $\mathfrak{p}_1 = \mathfrak{q}_1$ (оскільки ідеал $\mathfrak{q}_1$ максимальний). Домноживши на $\mathfrak{p}_1^{-1}$ рівність $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_s = \mathfrak{p}_1\mathfrak{q}_2 \dots \mathfrak{q}_t$, одержимо: $\mathfrak{p}_2 \dots \mathfrak{p}_s = \mathfrak{q}_2 \dots \mathfrak{q}_t$. Тепер очевидна індукція дає, що $s - 1 = t - 1$, тобто $s = t$, і з точністю до перестановки співмножників $\mathfrak{p}_i = \mathfrak{q}_i$ для всіх номерів i. □

З доведеної теореми та попередніх результатів безпосередньо випливають такі наслідки.

Наслідок I.4.9. *Для довільного ідеалу* $\mathbf{I}$ *дедекіндова кільця* D *має місце рівність* $\mathbf{I}^{-1}\mathbf{I} = \mathsf{D}$.

Наслідок I.4.10. *У дедекіндовому кільці ідеал* $\mathbf{I}$ *ділить ідеал* $\mathbf{J}$ *тоді й лише тоді, коли* $\mathbf{I} \supseteq \mathbf{J}$.

Вправи I.4. (1) (a) Доведіть, що скінченновимірна алгебра без дільників нуля є полем.

(b) Доведіть, що кільце цілих елементів довільного поля алгебричних функцій (див. вправу I.3 (7)) є дедекіндовим кільцем.

I.5. Дробові ідеали. Класи ідеалів

Останні два наслідки з попереднього розділу дають можливість занурити напівгрупу ідеалів дедекіндова кільця D у групу так званих *дробових ідеалів*.

Означення I.5.1. Ненульова підгрупа $\mathbf{I}$ адитивної групи поля F зветься *дробовим ідеалом* кільця D, якщо вона є D-підмодулем, тобто $\alpha\beta \in \mathbf{I}$ для довільних $\alpha \in \mathsf{D}$, $\beta \in \mathbf{I}$, причому існує такий елемент $\delta \in \mathsf{D}$, що $\delta\mathbf{I} \subseteq \mathsf{D}$.

Легко бачити, що остання умова рівносильна тому, що $\mathbf{I}$ є *скінченнопородженим* D-модулем, тобто існують такі елементи $\beta_1, \beta_2, \ldots, \beta_m \in \mathbf{I}$ (*твірні* $\mathbf{I}$), що довільний елемент з $\mathbf{I}$ записується як сума $\sum_{i=1}^{m} \alpha_i \beta_i$, де $\alpha_i \in \mathsf{D}$. Дійсно, якщо $\alpha\mathbf{I} \subseteq \mathsf{D}$, то $\alpha\mathbf{I}$ – ідеал у D. Тому він має скінченну множину твірних $\{\omega_1, \omega_2, \ldots, \omega_m\}$ і за твірні $\mathbf{I}$ можна взяти $\alpha^{-1}\omega_1, \alpha^{-1}\omega_2, \ldots, \alpha^{-1}\omega_m$. Навпаки, якщо $\beta_1, \beta_2, \ldots, \beta_m$ – твірні $\mathbf{I}$, то, записавши їх у вигляді дробів $\beta_j = \alpha_j/\delta_j$, де $\alpha_j, \delta_j \in \mathsf{D}$, ми бачимо, що $\delta\mathbf{I} \subseteq \mathsf{D}$, де $\delta = \delta_1 \ldots \delta_m$.

Теорема I.5.2. *Дробові ідеали дедекіндова кільця утворюють вільну абелеву групу відносно операції множення, базою якої є множина всіх первинних ідеалів.*

Цю групу звуть *групою дробових ідеалів,* або просто *групою ідеалів* дедекіндова кільця D і позначають $\mathcal{I}(\mathsf{D})$.

Доведення. Ясно, що множення дробових ідеалів асоціативне, а саме кільце D відіграє відносно нього роль одиниці. Нехай $\mathbf{I}$ – довільний дробовий ідеал. Тоді $\mathbf{I} = \alpha^{-1}\mathbf{J}$ для деякого ідеалу $\mathbf{J}$ кільця D і деякого $\alpha \in \mathsf{D}$. Покладемо $\mathbf{I}^{-1} = \alpha\mathbf{J}^{-1}$. Тоді за наслідком I.4.9 $\mathbf{I}^{-1}\mathbf{I} = \mathsf{D}$. Отже, дійсно, дробові ідеали утворюють групу. Більш того, якщо $\mathbf{J} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s$, а $\alpha\mathsf{D} = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_t$, де $\mathfrak{p}_i$ та $\mathfrak{q}_j$ – первинні ідеали, то $\mathbf{I} = \mathbf{J}(\alpha\mathsf{D})^{-1} = \mathfrak{p}_1 \ldots \mathfrak{p}_s\mathfrak{q}_1^{-1} \ldots \mathfrak{q}_t^{-1}$, тобто первинні ідеали – це множина твірних групи дробових ідеалів. Залишилося перевірити, що з рівності $\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2} \ldots \mathfrak{p}_s^{k_s} = \mathsf{D}$, де $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ – попарно різні первинні ідеали, випливає, що $k_1 = k_2 = \cdots = k_s = 0$. Припустимо, що це не так. Тоді можна вважати, що перші r показників додатні, а наступні t – від'ємні, причому $r + t > 0$. Але це дає рівність $\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r} = \mathfrak{p}_{r+1}^{-k_{r+1}} \ldots \mathfrak{p}_{r+t}^{-k_{r+t}}$, яка протирічить однозначності розкладу ідеалів у добуток первинних. □

Зокрема, для кожного ненульового елемента $\gamma \in \mathsf{F}$ можна розглянути *головний дробовий ідеал* $\gamma\mathsf{D}$. При цьому ясно, що $\gamma\mathsf{D} = \gamma'\mathsf{D}$ тоді й лише тоді, коли $\gamma' = \gamma\varepsilon$, де ε – обертовний елемент кільця D. Отже, ми одержуємо гомоморфізм ϕ_{D} з мультиплікативної групи F^* поля F до групи $\mathcal{I}(\mathsf{A})$ ідеалів кільця D. Образ цього гомоморфізма – це підгрупа головних дробових ідеалів. Факторгрупа $\mathcal{C}(\mathsf{D}) = \mathcal{I}(\mathsf{D})/Im\phi_{\mathsf{D}}$ зветься *групою класів ідеалів* дедекіндова кільця D. Якщо A – кільце цілих елементів деякого скінченного розширення K поля раціональних чисел, то його група класів ідеалів зветься також *групою класів ідеалів поля* K і позначається $\mathcal{C}(\mathsf{K})$. Очевидно, два дробових ідеали $\mathbf{I}$ та $\mathbf{J}$ мають однаковий образ у групі $\mathcal{C}(\mathsf{D})$, або, як кажуть, *належать одному класу* тоді й лише тоді, коли $\mathbf{J} = \gamma\mathbf{I}$ для деякого ненульового елемента $\gamma \in \mathsf{F}$.

Позначимо $\mathcal{P}(\mathsf{D})$ множину первинних ідеалів кільця D. Тоді теорема I.5.2 твердить, що довільний дробовий ідеал $\mathbf{I}$ однозначно розкладається у добуток

$$\mathbf{I} = \prod_{\mathfrak{p} \in \mathcal{P}(\mathsf{D})} \mathfrak{p}^{k_{\mathfrak{p}}}. \tag{5}$$

Звичайно, майже всі показники $k_{\mathfrak{p}}$ в цьому розкладі (тобто всі, крім скінченної кількості) дорівнюють 0.

Означення I.5.3. (1) Розклад (5) зветься *канонічним розкладом ідеалу* $\mathbf{I}$.

(2) *Показником* дробового ідеалу $\mathbf{I}$ відносно первинного ідеалу $\mathfrak{p}$ зветься показник $k_{\mathfrak{p}}$ у канонічному розкладі (5). Цей показник позначається $v_{\mathfrak{p}}(\mathbf{I})$.

(3) Зокрема, якщо $\mathbf{I} = \gamma\mathsf{D}$ – головний дробовий ідеал, то показник $v_{\mathfrak{p}}(\mathbf{I})$ зветься також *показником елемента* γ відносно первинного ідеалу $\mathfrak{p}$ і позначається $v_{\mathfrak{p}}(\gamma)$.

Ясно, що ідеал $\mathbf{I}$ однозначно визначається набором своїх показників $(\, v_{\mathfrak{p}}(\mathbf{I}) \,|\, \mathfrak{p} \in \mathcal{P}(\mathsf{D}) \,)$. Інколи буває зручно покласти $v_{\mathfrak{p}}(0) = \infty$, вважаючи, що символ ∞ підпорядковується звичайним правилам. Показники мають наступні очевидні властивості, нескладну перевірку яких ми залишаємо читачеві.

Твердження I.5.4. *Для довільних дробових ідеалів:*

(1) $v_{\mathfrak{p}}(\mathbf{I}) = \max\{\, k \,|\, \mathbf{I} \subseteq \mathfrak{p}^k \,\} = \min\{\, v_{\mathfrak{p}}(\gamma) \,|\, \gamma \in \mathfrak{p} \,\}$.

(2) $v_{\mathfrak{p}}(\mathbf{IJ}) = v_{\mathfrak{p}}(\mathbf{I}) + v_{\mathfrak{p}}(\mathbf{J})$ *і* $v_{\mathfrak{p}}(\mathbf{I}+\mathbf{J}) = \min\{\, v_{\mathfrak{p}}(\mathbf{I}),\, v_{\mathfrak{p}}(\mathbf{J}) \,\}$.

(3) *Зокрема,* $v_{\mathfrak{p}}(\alpha\beta) = v_{\mathfrak{p}}(\alpha) + v_{\mathfrak{p}}(\beta)$ *і* $v_{\mathfrak{p}}(\alpha+\beta) \geq \min\{\, v_{\mathfrak{p}}(\alpha),\, v_{\mathfrak{p}}(\beta) \,\}$ *для довільних елементів* $\alpha, \beta \in \mathsf{F}$, *причому якщо* $v_{\mathfrak{p}}(\alpha) \neq v_{\mathfrak{p}}(\beta)$, *то остання нерівність перетворюється на рівність.*

Вправи I.5. (1) Поняття дробового ідеалу має зміст для довільного кільця D без дільників нуля. При цьому дробовий ідеал $\mathbf{I}$ зветься *обертовним*, якщо існує такий дробовий ідеал $\mathbf{I}'$, що $\mathbf{II}' = \mathsf{D}$.

(a) Доведіть, що обертовний дробовий ідеал завжди має скінченну множину твірних.

(b) Доведіть рівносильність наступних умов для кільця D:

(i) Кільце D є дедекіндовим.

(ii) Дробові ідеали утворюють групу відносно операції множення.

(iii) Кожен первинний ідеал кільця D є обертовним.

(iv) Кільце D є нетеровим і кожен його максимальний ідеал є обертовним.

(2) Доведіть, що два дробових ідеали кільця D є ізоморфними D-модулями тоді й лише тоді, коли вони належать одному класу ідеалів.

(3) Нехай $\beta_1, \beta_2, \ldots, \beta_m$ – множина твірних деякого дробового ідеалу $\mathbf{I}$ кільця D без дільників нуля.

(a) Доведіть, що дробовий ідеал $\mathbf{I}$ є обертовним тоді й лише тоді, коли існують такі елементи $\gamma_1, \gamma_2, \ldots, \gamma_m$ поля часток F кільця D, для яких $\sum_{i=1}^{m} \gamma_i\beta_i = 1$. Перевірити, що тоді

$\gamma_i \in \mathbf{I}^{-1}$ для всіх i, де, як і вище

$$\mathbf{I}^{-1} = \{\, \gamma \in \mathsf{F} \,|\, \gamma\mathbf{I} \subseteq \mathsf{D} \,\} \ .$$

(b) Вивести, що в цьому випадку вільний D-модуль D^m рангу m ізоморфний прямій сумі $\mathbf{I} \oplus P$ для деякого модуля P.

(c) Доведіть, що обертовний ідеал $\mathbf{I}$ є *проективним* D-модулем, тобто для довільного епіморфізму D-модулів $\pi : M \to N$ і довільного гомоморфізму $\varphi : \mathbf{I} \to N$ існує такий гомоморфізм $\psi : \mathbf{I} \to M$, що $\varphi = \pi\psi$.

(d) Доведіть, що для довільного епіморфізму D-модулів $\pi : M \to \mathbf{I}$, де $\mathbf{I}$ – обертовний ідеал, $M \simeq \mathbf{I} \oplus \ker\varphi$.

(e) Нехай M – довільний D-модуль, T – його *періодична частина*, тобто множина всіх таких елементів $a \in M$, для яких існують такі ненульові елементи $\alpha \in \mathsf{D}$, що $\alpha a = 0$. Доведіть, що T – підмодуль в M, причому фактормодуль M/T є *модулем без скруту* (тобто його періодична частина дорівнює нулю).

(f) Нехай M – D-модуль без скруту. Наслідуючи побудову поля часток, вкласти M у *модуль часток* $\widetilde{M}$, який складається з "дробів" вигляду $\frac{x}{a}$, де $x \in M$, $a \in \mathsf{D}$ і $a \neq 0$ і є векторним простором над полем часток F кільця D. Якщо модуль M скінченнопороджений, довести, що простір $\widetilde{M}$ є скінченновимірним і тоді модуль M можна занурити у вільний D-модуль.

(g) У випадку, коли кільце D дедекіндове, довести, що кожен скінченнопороджений D-модуль без скруту ізоморфний прямій сумі ідеалів, а довільний скінченнопороджений D-модуль M ізоморфний $T \oplus M/T$, де T – його періодична частина.

I.6. Кільця лишків. Норма ідеалу

Починаючи з цього розділу, K позначатиме завжди скінченне розширення поля раціональних чисел, а A – кільце цілих алгебричних елементів поля K. За наслідком I.3.11, якщо $\mathbf{I}$ – ненульовий ідеал в A, то факторкільце $\mathsf{A}/\mathbf{I}$ є скінченним.

Означення I.6.1. Кількість елементів у факторкільці $\mathsf{A}/\mathbf{I}$ зветься *нормою ідеалу* $\mathbf{I}$ і позначається $\mathrm{N}(\mathbf{I})$.

Основний результат стосовно норми ідеалів полягає в її *мультиплікативності*.

Теорема I.6.2. $\mathrm{N}(\mathbf{IJ}) = \mathrm{N}(\mathbf{I})\mathrm{N}(\mathbf{J})$ *для довільних ненульових ідеалів* $\mathbf{I}$ *та* $\mathbf{J}$ *кільця* A.

Доведення знову розіб'ємо на кілька самостійних тверджень. Перш за все доведемо цю теорему в частинному випадку *співпервинних* ідеалів.

Означення I.6.3. Ідеали $\mathbf{I}$ та $\mathbf{J}$ деякого кільця D звуться *співпервинними*, якщо $\mathbf{I}+\mathbf{J}=\mathsf{D}$.

Мабуть, найважливішою властивістю співпервинних ідеалів є так звана "китайська теорема про лишки", яку ми сформулюємо в наступному вигляді.

Теорема I.6.4. *Нехай* $\mathbf{I}_1,\mathbf{I}_2,\ldots,\mathbf{I}_r$ – *попарно співпервинні ідеали кільця* D. *Тоді:*

(1) *Для довільних елементів* $\alpha_1,\alpha_2,\ldots,\alpha_r\in\mathsf{D}$ *знайдеться такий елемент* $\alpha\in\mathsf{D}$, *що* $\alpha\equiv\alpha_j\,(\mathrm{mod}\,\mathbf{I}_j)$ *для всіх номерів* $j=1\ldots r$.
(2) $\bigcap_{j=1}^{r}\mathbf{I}_j=\prod_{j=1}^{r}\mathbf{I}_j$.
(3) $\mathsf{D}/\prod_{j=1}^{r}\mathbf{I}_j\simeq\prod_{j=1}^{r}\mathsf{D}/\mathbf{I}_j$ *(справа символ* $\prod$ *позначає* прямий добуток *кілець).*

Доведення. Доведення тверджень *1* і *2* проведемо індукцією за r. Нехай спочатку $r=2$. Оскільки $\mathbf{I}_1+\mathbf{I}_2=\mathsf{D}$, знайдуться елементи $\beta_1\in\mathbf{I}_1$ та $\beta_2\in\mathbf{I}_2$, такі що $\beta_1+\beta_2=1$. Тоді легко перевірити, що елемент $\alpha=\alpha_1\beta_2+\alpha_2\beta_1$ задовольняє необхідні порівняння. Крім того, якщо $\gamma\in\mathbf{I}_1\cap\mathbf{I}_2$, то з рівності $\gamma=\gamma\beta_1+\gamma\beta_2$ випливає, що $\gamma\in\mathbf{I}_1\mathbf{I}_2$. Оскільки завжди $\mathbf{I}_1\mathbf{I}_2\subseteq\mathbf{I}_1\cap\mathbf{I}_2$, звідси $\mathbf{I}_1\cap\mathbf{I}_2=\mathbf{I}_1\mathbf{I}_2$.

Припустимо, що ми вже знайшли елемент $\beta\in\mathsf{D}$, для якого $\beta\equiv\alpha_j\,(\mathrm{mod}\,\mathbf{I}_j)$ при $j=1,\ldots,r-1$, і знаємо, що $\bigcap_{j=1}^{r-1}\mathbf{I}_j=\prod_{j=1}^{r-1}\mathbf{I}_j$. Позначимо цей добуток $\mathbf{J}$. Перемноживши рівності $\mathbf{I}_j+\mathbf{I}_r=\mathsf{D}$ з $j=1,\ldots,r-1$, одержимо, що $\mathbf{J}+\mathbf{I}_r=\mathsf{D}$, тобто ідеали $\mathbf{J}$ й $\mathbf{I}_r$ співпервинні. Тому, як ми вже довели, знайдеться елемент α, такий що $\alpha\equiv\beta\,(\mathrm{mod}\,\mathbf{J})$ і $\alpha\equiv\alpha_r\,(\mathrm{mod}\,\mathbf{I}_r)$. Але тоді α задовольняє всім необхідним порівнянням з пункту *1*. Крім того,

$$\bigcap_{j=1}^{r}\mathbf{I}_j=\mathbf{J}\cap\mathbf{I}_r=\mathbf{J}\mathbf{I}_r=\prod_{j=1}^{r}\mathbf{I}_j\,,$$

тобто виконується і твердження *2*.

Для доведення твердження *3* розглянемо гомоморфізм $\varphi:\mathsf{D}\to\prod_{j=1}^{r}\mathsf{D}/I_j$, який відображає елемент $\alpha\in\mathsf{D}$ у набір $(\alpha+\mathbf{I}_1,\alpha+\mathbf{I}_2,\ldots,\alpha+\mathbf{I}_r)$. Тоді пункт *1* означає, що відображення φ *сюр'єктивне*, а пункт *2* – що його ядро, яке є, очевидно, перетином усіх ідеалів $\mathbf{I}_j$, збігається з їхнім добутком. Тому твердження *3* випливає з теореми про гомоморфізм (див., напр., [**K**, гл.4, §4, п.4]). □

Для кільця цілих алгебричних чисел A звідси випливає наступний частинний випадок теореми I.6.2.

Наслідок I.6.5. *Рівність* $\mathrm{N}(\mathbf{IJ}) = \mathrm{N}(\mathbf{I})\mathrm{N}(\mathbf{J})$ *справжнюється, якщо ідеали* $\mathbf{I}$ *та* $\mathbf{J}$ *кільця* A *співпервинні.*

Розглянемо тепер випадок *головних ідеалів*. Для них норма виявляється пов'язаною з нормами елементів, які було введено в розділі I.3. Доведемо спочатку наступний результат.

Твердження I.6.6. *Нехай* F *– вільна абелева група з базою* $e_1, e_2, \ldots, e_n$, F' *– її підгрупа з базою* $f_1, f_2, \ldots, f_n$, *причому* $f_j = \sum_{i=1}^{n} a_{ij} e_i$ *(*$a_{ij} \in \mathbb{Z}$*). Тоді порядок факторгрупи* F/F' *дорівнює* $|\det A|$, *де* A *– матриця з коефіцієнтами* a_{ij}.

Доведення. Відомо, що можна вибрати нові бази $e'_1, e'_2, \ldots, e'_n$ у групі F і $f'_1, f'_2, \ldots, f'_n$ у підгрупі F', такі що $f'_i = d_i e'_i$ $(d_i \in \mathbb{N})$ для всіх номерів $i = 1 \ldots n$. Тоді, очевидно, $|F/F'| = d_1 d_2 \ldots d_n = \det D$, де $D = \mathrm{diag}\,(d_1, d_2, \ldots, d_n)$ (діагональна матриця). Але, як відомо, при зміні базисів у F і F' матриця A замінюється на SAT, де S і T – цілочисельні матриці з визначниками ± 1. Отже, $|\det A| = |\det D|$. □

Тепер можна довести теорему I.6.2 для випадку, коли один з ідеалів головний.

Твердження I.6.7. $\mathrm{N}(\alpha\mathbf{I}) = |\mathrm{N}(\alpha)|\mathrm{N}(\mathbf{I})$ *для довільного елемента* $\alpha \in \mathsf{A}$ *і довільного ідеалу* $\mathbf{I} \subseteq \mathsf{A}$. *Зокрема,* $\mathrm{N}(\alpha\mathsf{D}) = |\mathrm{N}(\alpha)|$.

Доведення. Виберемо базу $\beta_1, \beta_2, \ldots, \beta_n$ ідеалу $\mathbf{I}$. Тоді $\alpha\beta_1$ $\alpha\beta_2, \ldots, \alpha\beta_n$ – база ідеалу $\alpha\mathbf{I}$ причому $\alpha\beta_j = \sum_{i=1}^{n} a_{ij}\beta_j$ для деяких $a_{ij} \in \mathbb{Z}$. Зауважимо, що елементи $\beta_1, \beta_2, \ldots, \beta_n$ утворюють, зокрема, базу поля K і матриця $A = (a_{ij})$ – це матриця відображення L_α у цій базі. Отже, $\det A = \mathrm{N}(\alpha)$. Але за твердженням I.6.6,

$$|\det A| = |\mathbf{I}/\alpha\mathbf{I}| = \frac{|\mathsf{A}/\mathbf{I}|}{|\mathsf{A}/\alpha\mathbf{I}|} = \frac{\mathrm{N}(\mathbf{I})}{\mathrm{N}(\alpha\mathbf{I})}\,.$$

□

Наслідок I.6.8. *Для довільного елемента* $\gamma \in \mathbf{I}^{-1}$ *має місце рівність* $\mathrm{N}(\gamma\mathbf{I}) = |\mathrm{N}(\gamma)|\mathrm{N}(\mathbf{I})$.

Доведення. Нехай $\gamma = \alpha/\beta$, де $\alpha, \beta \in \mathsf{A}$, $\mathbf{J} = \gamma\mathbf{I}$. Тоді $\beta\mathbf{J} = \alpha\mathbf{I}$, звідки

$$\mathrm{N}(\beta\mathbf{J}) = |\mathrm{N}(\beta)|\mathrm{N}(\mathbf{J}) = \mathrm{N}(\alpha\mathbf{I}) = |\mathrm{N}(\alpha)|\mathrm{N}(\mathbf{I})\,.$$

Отже, $\mathrm{N}(\mathbf{J}) = |\mathrm{N}(\alpha)/\mathrm{N}(\beta)|\mathrm{N}(\mathbf{I}) = |\mathrm{N}(\gamma)|\mathrm{N}(\mathbf{I})$. □

Доведемо, нарешті, наступний результат, який дозволяє звести загальний випадок до вже розглянутих.

Твердження I.6.9. *Нехай* D *– дедекіндове кільце. Тоді для довільних ідеалів* $\mathbf{I}, \mathbf{J} \subseteq \mathsf{A}$ *знайдеться такий елемент* $\gamma \in \mathbf{I}^{-1}$, *що ідеали* $\gamma\mathbf{I}$ *та* $\mathbf{J}$ *співпервинні.*

Доведення. Скористаємося наступною "теоремою про апроксимацію", яка є безпосереднім наслідком китайської теореми про лишки.

Теорема I.6.10. *Нехай* D *– дедекіндове кільце,* F *– його поле часток і* $P = \{\,\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\,\}$ *– скінченний набір первинних ідеалів з* D. *Для довільних елементів* $\gamma_1, \gamma_2, \ldots, \gamma_m \in \mathsf{F}$ *і довільних цілих чисел* $k_1, k_2, \ldots, k_m$ *існує такий елемент* $\gamma \in \mathsf{F}$, *що* $v_{\mathfrak{p}_i}(\gamma - \gamma_i) \ge k_i$ *для всіх* $i = 1 \ldots m$ *і* $v_{\mathfrak{p}}(\gamma) \ge 0$ *для всіх первинних ідеалів* $\mathfrak{p} \notin P$.

Доведення. Припустимо спочатку, що всі числа k_i невід'ємні, а $\gamma_i \in \mathsf{D}$. Тоді $\mathfrak{p}_i^{k_i}$ – попарно співпервинні ідеали кільця D. За теоремою I.6.4 знайдеться елемент $\gamma \in \mathsf{D}$, такий що $\gamma \equiv \gamma_i \,(\mathrm{mod}\, \mathfrak{p}_i^{k_i})$ при $i = 1 \ldots m$, тобто γ задовольняє всі необхідні умови.

У загальному випадку знайдемо такий елемент $\beta \in \mathsf{D}$, що всі добутки $\alpha_i = \beta\gamma_i$ лежать у D і, крім того, $v_{\mathfrak{p}_i}(\beta) \ge -k_i$ для всіх номерів i. Нехай $Q = \{\,\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_l\,\}$ – множина всіх тих первинних ідеалів, які не належать P і містять β. Як ми вже довели, знайдеться елемент $\alpha \in \mathsf{D}$, такий що:

$$v_{\mathfrak{p}_i}(\alpha - \alpha_i) \ge k_i + v_{\mathfrak{p}_i}(\beta) \quad \text{для всіх} \quad i = 1 \ldots m\,;$$
$$v_{\mathfrak{q}_j}(\alpha) \ge v_{\mathfrak{q}_j}(\beta) \quad \text{для всіх} \quad j = 1 \ldots l\,;$$
$$v_{\mathfrak{p}}(\alpha) \ge 0\,, \quad \text{якщо} \quad \mathfrak{p} \notin P \cup Q\,.$$

Тоді, очевидно, можна покласти $\gamma = \alpha/\beta$. □

Наслідок I.6.11. *За умов теореми I.6.10 для довільних цілих чисел* k_i $(i = 1 \ldots m)$ *знайдеться такий елемент* $\gamma \in F$, *що* $v_{\mathfrak{p}_i}(\gamma) = k_i$ *при* $i = 1 \ldots m$ *і* $v_{\mathfrak{p}}(\gamma) \ge 0$ *при* $\mathfrak{p} \notin P$.

Доведення. Виберемо для кожного номера i якийсь елемент $\gamma_i \in \mathfrak{p}_i^{k_i} \setminus \mathfrak{p}_i^{k_i+1}$ і знайдемо такий елемент $\gamma \in F$, що $v_{\mathfrak{p}_i}(\gamma - \gamma_i) \ge k_i + 1$ при $i = 1 \ldots m$ і $v_{\mathfrak{p}}(\gamma) \ge 0$ при $\mathfrak{p} \notin P$. Очевидно, γ і буде шуканим елементом. □

Повернемось до доведення твердження I.6.9. Нехай $\mathbf{J} = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2} \ldots \mathfrak{p}_m^{k_m}$ – канонічний розклад ідеалу $\mathbf{J}$. Знайдемо такий елемент $\gamma \in \mathsf{F}$, для якого $v_{\mathfrak{p}_i}(\gamma) = -v_{\mathfrak{p}_i}(\mathbf{I})$ при $i = 1 \ldots m$ і $v_{\mathfrak{p}}(\gamma) \ge 0$, якщо $\mathfrak{p} \ne \mathfrak{p}_i$ для жодного номера i. Тоді очевидно, що $\gamma \in \mathbf{I}^{-1}$ і $v_{\mathfrak{p}_i}(\gamma\mathbf{I}) = 0$ для всіх $i = 1 \ldots m$. Отже, ідеали $\gamma\mathbf{I}$ та $\mathbf{J}$ співпервинні. □

Тепер ми можемо завершити доведення теореми I.6.2. Виберемо $\gamma \in \mathbf{I}^{-1}$ так, щоб ідеали $\gamma\mathbf{I}$ та $\mathbf{J}$ були співпервинними. Тоді

$$\mathrm{N}(\gamma\mathbf{I}\mathbf{J}) = \mathrm{N}(\gamma\mathbf{I})\mathrm{N}(\mathbf{J}) = |\mathrm{N}(\gamma)|\mathrm{N}(\mathbf{I})\mathrm{N}(\mathbf{J})\,.$$

Оскільки також $\mathrm{N}(\gamma\mathbf{I}\mathbf{J}) = |\mathrm{N}(\gamma)|\mathrm{N}(\mathbf{I}\mathbf{J})$, звідси маємо, що $\mathrm{N}(\mathbf{I}\mathbf{J}) = \mathrm{N}(\mathbf{I})\mathrm{N}(\mathbf{J})$. □

Мультиплікативність дає змогу розповсюдити означення норми і на дробові ідеали. Саме, довільний дробовий ідеал $\mathbf{I}$ можна подати у вигляді $\mathbf{I}_1\mathbf{I}_2^{-1}$, де $\mathbf{I}_1$ і $\mathbf{I}_2$ – ідеали кільця A. Покладемо тоді $\mathrm{N}(\mathbf{I}) =$

$\mathrm{N}(\mathbf{I}_1)/\mathrm{N}(\mathbf{I}_2)$. З теореми I.6.2 одразу випливає, що ця величина не залежить від вибору ідеалів $\mathbf{I}_1$ і $\mathbf{I}_2$, себто таке означення є коректним. Більш того, очевидно, що рівність $\mathrm{N}(\mathbf{IJ}) = \mathrm{N}(\mathbf{I})\mathrm{N}(\mathbf{J})$ залишається справедливою і для дробових ідеалів. Нарешті, очевидним є наступний корисний факт.

Твердження I.6.12. *Якщо* $\mathbf{I} \subseteq \mathbf{J}$, *де* $\mathbf{I}, \mathbf{J}$ – *дробові ідеали кільця* A, *то* $|\mathbf{I}/\mathbf{J}| = \mathrm{N}(\mathbf{I})/\mathrm{N}(\mathbf{J})$.

Скористаємось ще теоремою про апроксимацію для доведення такої властивості факторкілець дедекіндова кільця.

Теорема I.6.13. *Для довільного ідеалу* $\mathbf{I}$ *дедекіндова кільця* D *факторкільце* $\mathsf{D}/\mathbf{I}$ *є кільцем головних ідеалів.*

Доведення. Відомо, що довільний ідеал кільця $\mathsf{D}/\mathbf{I}$ має вигляд $\mathbf{J}/\mathbf{I}$ для деякого ідеалу $\mathbf{J} \supseteq \mathbf{I}$ кільця D. Тому досить довести, що знайдеться такий елемент $\alpha \in \mathsf{D}$, що $\mathbf{J} = \mathbf{I} + \alpha\mathsf{D}$: тоді його клас $\alpha + \mathbf{I}$, очевидно, буде твірним ідеалу $\mathbf{J}/\mathbf{I}$. Нехай $\mathbf{I} = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\mathfrak{p}_m^{k_m}$ – канонічний розклад ідеалу $\mathbf{I}$. За наслідком I.6.11 існує елемент $\alpha \in \mathsf{D}$, такий що $v_{\mathfrak{p}_i}(\alpha) = v_{\mathfrak{p}_i}(\mathbf{J})$ для всіх $i = 1\ldots m$. Але тоді з властивостей показників (твердження I.5.4) безпосередньо випливає, що дійсно $\mathbf{I} + \alpha\mathsf{D} = \mathbf{J}$. $\square$

Наслідок I.6.14. *Довільний ідеал дедекіндова кільця* D *має не більше* 2 *твірних. Точніше, якшо* β – *довільний елемент ідеалу* $\mathbf{I}$, *то знайдеться такий елемент* $\alpha \in \mathbf{I}$, *що* $\{\alpha, \beta\}$ *є множиною твірних ідеалу* $\mathbf{I}$.

Вправи I.6.

(1) Доведіть, що дедекіндове кільце зі *скінченною* множиною первинних ідеалів є кільцем головних ідеалів.

(2) Нехай D – дедекіндове кільце.
   (a) Доведіть, що для довільних двох ідеалів кільця D має місце ізоморфізм D-модулів $\mathbf{I} \oplus \mathbf{J} \simeq (\mathbf{I} + \mathbf{J}) \oplus (\mathbf{I} \cap \mathbf{J})$. Скориставшись твердженням I.6.9, виведіть звідси, що $\mathbf{I} \oplus \mathbf{J} \simeq \mathsf{A} \oplus \mathbf{IJ}$.
   (b) Доведіть, що довільний скінченнопороджений D-модуль без скруту ізоморфний прямій сумі вільного D-модуля і деякого ідеалу, причому клас цього ідеалу визначається однозначно.

   (Скористайтеся результатами вправи I.5 (3)).

(3) Нехай D – дедекіндове кільце.
   (a) Доведіть, що $\mathbf{I}/\mathbf{IJ} \simeq \mathsf{D}/\mathbf{J}$ для довільних ідеалів $\mathbf{I}$ і $\mathbf{J}$.
   (b) Доведіть, що $M/\mathbf{I}M \simeq (\mathsf{A}/\mathbf{I})^n$ для довільного ідеалу $\mathbf{I}$ і довільного скінченнопородженого D-модуля M без скруту рангу n.

(4) Для довільної підмножини S ненульових елементів дедекіндова кільця D позначимо $\mathsf{D}[S^{-1}]$ підкільце в полі часток F, яке складається з усіх тих елементів, які можна подати у вигляді α/β, де β є добутком деяких елементів з множини S.

(a) Доведіть, що кільце $\mathsf{D}[S^{-1}]$ також є дедекіндовим, причому існує взаємно однозначна відповідність між первинними ідеалами кільця $\mathsf{D}[S^{-1}]$ і такими первинними ідеалами $\mathfrak{p}$ кільця D, що $\mathfrak{p} \cap S = \emptyset$.

(b) Доведіть, що для довільного первинного ідеалу $\mathfrak{p} \subset \mathsf{D}$ існує такий ненульовий елемент $\alpha \in \mathsf{D} \setminus \mathfrak{p}$, що у кільці $\mathsf{D}' = \mathsf{D}[\alpha^{-1}]$ ідеал $\mathfrak{p}\mathsf{D}'$ є головним.

(c) Нехай D' – довільне підкільце поля F, яке містить D. Доведіть, що $\mathsf{D}' = \mathsf{D}[S^{-1}]$ для деякої підмножини $S \subset \mathsf{D}$ (зокрема, D' теж є дедекіндовим кільцем).

(5) Нехай $\mathfrak{p}$ – первинний ідеал у кільці без дільників нуля D, $S = \mathsf{D}\setminus\mathfrak{p}$. У цьому випадку кільце $\mathsf{D}[S^{-1}]$ позначається $\mathsf{D}_\mathfrak{p}$ і зветься *локалізацією кільця* D за ідеалом $\mathfrak{p}$.

(a) Доведіть, що кільце $\mathsf{D}_\mathfrak{p}$ має єдиний максимальний ідеал $\mathfrak{p}^* = \{\, \alpha/\beta \,|\, \alpha \in \mathfrak{p}, \beta \notin \mathfrak{p} \,\}$, причому факторкільце $\mathsf{D}_\mathfrak{p}/\mathfrak{p}^*$ ізоморфне полю часток факторкільця $\mathsf{D}/\mathfrak{p}$ (зокрема, якщо ідеал $\mathfrak{p}$ був максимальним, то $\mathsf{D}_\mathfrak{p}/\mathfrak{p}^* \simeq \mathsf{D}/\mathfrak{p}$).

(b) Якщо D – дедекіндове кільце, доведіть, що ідеал $\mathfrak{p}^*$ є головним: $\mathfrak{p}^* = \pi\mathsf{D}_\mathfrak{p}$, і довільний ненульовий ідеал кільця $\mathsf{D}_\mathfrak{p}$ збігається з $(\mathfrak{p}^*)^k = \pi^k\mathsf{D}$ для деякого натурального k, причому $\mathsf{D}_\mathfrak{p}/(\mathfrak{p}^*)^k \simeq \mathsf{D}/\mathfrak{p}^k$.

(6) Нехай $\mathfrak{p}$ – максимальний ідеал кільця D. D-модуль M зветься $\mathfrak{p}$-*примарним*, якщо для довільного $a \in M$ існує натуральне k, таке що $\mathfrak{p}^k a = 0$. Надалі вважаємо, що кільце D не має дільників нуля.

(a) Доведіть, що довільний $\mathfrak{p}$-примарний D-модуль M можна перетворити в $\mathsf{D}_\mathfrak{p}$-модуль, поклавши для $\alpha/\beta \in \mathsf{D}_\mathfrak{p}$ і $a \in M$ $(\alpha/\beta)a = \alpha b$, де b – єдиний елемент модуля M, такий що $\beta b = a$. Більш того, довільний гомоморфізм $\mathfrak{p}$-примарних модулів є також гомоморфізмом $\mathsf{D}_\mathfrak{p}$-модулів. Зокрема, два $\mathfrak{p}$-примарні модулі ізоморфні тоді й лише тоді, коли вони ізоморфні як $\mathsf{D}_\mathfrak{p}$-модулі.

(b) Довести, що над дедекіндовим кільцем довільний періодичний модуль M ізоморфний прямій сумі $\bigoplus_{\mathfrak{p}\in\mathcal{P}} M_\mathfrak{p}$, де $M_\mathfrak{p} = \{\, a \in M \,|\, \mathfrak{p}^k a = 0 \text{ для деякого натурального } k \,\}$ є $\mathfrak{p}$-примарним модулем.

(c) Скориставшись описом модулів над областями головгих ідеалів, доведіть, що довільний періодичний скінченнопороджений модуль над дедекіндовим кільцем D однозначно розкладається у пряму суму *примарних циклічних модулів*, тобто модулів вигляду $\mathsf{D}/\mathfrak{p}^k$, де $\mathfrak{p}$ – деякий первинний ідеал.

(7) Нехай D – дедекіндове кільце, M – скінченнопороджений D-модуль без скруту, N – такий його підмодуль, що фактормодуль M/N є періодичним. Розкладемо згідно з результатом останньої вправи модуль M/N у пряму суму циклічних: $M/N = \oplus_{i=1}^{m} \mathsf{D}/\mathbf{I}_i$. Доведіть, що добуток $\mathbf{I}_1\mathbf{I}_2\ldots\mathbf{I}_m$ не залежить від вибору такого розкладу. Цей добуток зветься *індексом підмодуля* N в модулі M і позначається $(M:N)_{\mathsf{D}}$.

(8) Нехай $\mathsf{L} \subseteq \mathsf{K}$ – скінченні розширення поля раціональних чисел, A і B – кільця цілих елементів відповідно в K і L. Для довільного ідеалу $\mathbf{I} \subseteq \mathsf{A}$ його *нормою відносно поля* L L зветься індекс $(\mathsf{A}:\mathbf{I})_{\mathsf{B}}$. Ця норма позначається $\mathrm{N}_{\mathsf{K}/\mathsf{L}}(\mathbf{I})$.

(a) Доведіть, що так визначена норма є мультиплікативною, тобто

$$\mathrm{N}_{\mathsf{K}/\mathsf{L}}(\mathbf{IJ}) = \mathrm{N}_{\mathsf{K}/\mathsf{L}}(\mathbf{I})\mathrm{N}_{\mathsf{K}/\mathsf{L}}(\mathbf{J}).$$

Користуючись цим, розповсюдьте цю норму на дробові ідеали поля K.

(b) Доведіть, що "відносна" норма пов'язана з "абсолютною" правилом:

$$\mathrm{N}(\mathbf{I}) = \mathrm{N}(\mathrm{N}_{\mathsf{K}/\mathsf{L}}(\mathbf{I})).$$

(Тут зліва N позначає норму в полі K, а справа – в полі L).

(9) Нехай $\mathsf{P} = \mathbf{k}[x]$ – кільце многочленів від однієї змінної над полем $\mathbf{k}$, M – вільний P-модуль з базою $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ і N – його підмодуль з базою $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_n$, де $\mathbf{f}_j = \sum_{i=1}^{n} a_{ij}\mathbf{e}_i$ ($a_{ij} \in \mathsf{P}$). Доведіть, що фактормодуль M/N є векторним простором над полем $\mathbf{k}$ розмірності $\deg(\det A)$, де A – матриця, складена з коефіцієнтів a_{ij}.

(10) Нехай A – кільце цілих елементів деякого поля алгебричних функцій K (див. вправу I.3 (7)), причому $(\mathsf{K}:\mathsf{F}) = n$ ($\mathsf{F} = \mathbf{k}(x)$). Для довільного ідеалу $\mathbf{I} \subseteq \mathsf{A}$ позначимо $\operatorname{cod}\mathbf{I} = \dim(\mathsf{A}/\mathbf{I})$ (усі розмірності є розмірностями над полем $\mathbf{k}$). Число $\operatorname{cod}\mathbf{I}$ зветься *корозмірністю ідеалу* $\mathbf{I}$.

(a) Доведіть, що для довільного елемента $\alpha \in \mathsf{A}$ має місце рівність: $\operatorname{cod}(\alpha\mathbf{I}) = \deg \mathrm{N}(\alpha) + \operatorname{cod}\mathbf{I}$.

(b) Доведіть *адитивність корозмірності*, тобто формулу:

$$\operatorname{cod}(\mathbf{IJ}) = \operatorname{cod}\mathbf{I} + \operatorname{cod}\mathbf{J}.$$

(c) Припустимо, що поле $\mathbf{k}$ скінченне. Означимо тоді норму $\mathrm{N}(\mathbf{I})$ ідеалу $\mathbf{I}$ як порядок факторкільця $\mathsf{A}/\mathbf{I}$. Доведіть, що $\mathrm{N}(\mathbf{I}) = q^{\operatorname{cod}\mathbf{I}}$, де q – кількість елементів у полі $\mathbf{k}$ і виведіть звідси мультиплікативність так визначеної норми.

(d) Розповсюдити поняття корозмірності й норми на дробові ідеали поля K і довести їх відповідно адитивність і мультиплікативність.

(11) Введіть для полів алгебричних функцій поняття "відносної норми" аналогічно вправі 8. У випадку скінченного поля констант $\mathbf{k}$ встановіть звязок цього поняття з поняттям норми, введеним у попередній вправі.

I.7. Розклад первинних чисел. Дискримінант

Вже у розділі I.1 ми бачили, що важливо знати, які є первинні ідеали в кільці A і як розкладаються в ньому первинні натуральні числа (звичайно, число p ми маємо замінити головним ідеалом $p\mathsf{A}$). Зі скінченності кілець лишків випливають насамперед такі факти.

Твердження I.7.1. (1) *Довільний ідеал кільця A містить свою норму (яка є, звичайно, натуральним числом).*

(2) *Довільний первинний ідеал $\mathfrak{p}$ містить едине первинне число p. При цьому $\mathrm{N}(\mathfrak{p}) = p^f$ для деякого натурального f.*

Доведення. *1.* Якщо $N = \mathrm{N}(\mathbf{I}) = |\mathsf{A}/\mathbf{I}|$, то $N \cdot \alpha \in \mathbf{I}$ для всіх елементів $\alpha \in \mathsf{A}$. Зокрема, $N = N \cdot 1 \in \mathbf{I}$.

2. Якщо ідеал $\mathfrak{p}$ первинний, то $\mathsf{A}/\mathfrak{p}$ – скінченне поле. Тому кількість елементів у ньому дорівнює p^f для деякого первинного числа p (див., напр., [**K**, гл.9, §1, п.3]). Отже, $\mathrm{N}(\mathfrak{p}) = p^f$. Тоді $p^f \in \mathfrak{p}$ і, оскільки ідеал $\mathfrak{p}$ первинний, також $p \in \mathfrak{p}$. Якщо $q \neq p$ – інше первинне число, то воно співпервинне з p, тобто $pa + qb = 1$ для деяких цілих a, b. Оскільки $1 \notin \mathfrak{p}$, неможливо, щоб $q \in \mathfrak{p}$. □

Наслідок I.7.2. *Нехай $p\mathsf{A} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_s^{e_s}$ – канонічний розклад у кільці A головного ідеалу, породженого первинним натуральним числом p. Тоді:*

(1) $\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$ *для кожного номера $i = 1 \dots s$, де f_i – деякі натуральні числа.*

(2) $\sum_{i=1}^{s} e_i f_i = (\mathsf{K} : \mathbb{Q})$.

Доведення. Доводити потрібно лише друге твердження: перше ми вже довели. Але з мультиплікативності норми маємо:

$$\mathrm{N}(p\mathsf{A}) = |\mathrm{N}(p)| = p^n = \prod_{i=1}^{s} \mathrm{N}(\mathfrak{p}_i)^{e_i} = p^{\sum_{i=1}^{s} e_i f_i},$$

де $n = (\mathsf{K} : \mathbb{Q})$. □

Означення I.7.3. (1) Якщо $p\mathsf{A} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_s^{e_s}$ – канонічний розклад головного ідеалу, породженого первинним числом, то показник e_i зветься *індексом розгалуження* первинного ідеалу $\mathfrak{p}_i$, а число f_i, таке що $\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$ – його *ступенем інерції*.

(2) Первинний ідеал зветься *розгалуженим*, якщо його індекс розгалуження $e > 1$, і *нерозгалуженим*, якщо $e = 1$. Первинний ідеал зветься *первинним ідеалом першого ступеня*, якщо $f = 1$.
(3) Первинне число p зветься *нерозгалуженим у полі* K, якщо нерозгалуженими є всі первинні ідеали кільця A, які його містять, і *розгалуженим* у цьому полі, якщо хоч би один з них є розгалуженим.
(4) Первинне число p зветься *цілком розкладним у полі* K, якщо воно є нерозгалуженим, а всі первинні ідеали кільця A, які його містять, є первинними ідеалами першого ступеня.

Зауважимо, що ці означення коректні, оскільки первинний ідеал може містити лише одне первинне натуральне число. Наступне просте твердження, дає корисну ознаку розгалуженості

Твердження I.7.4. *Первинне число p є розгалуженим у полі K тоді й лише тоді, коли кільце лишків $\mathsf{A}/p\mathsf{A}$ має ненульові нільпотентні елементи*[3].

Доведення. Клас $a + p\mathsf{A}$ є нільпотентним у фактор-кільці тоді й лише тоді, коли $a^k \in p\mathsf{A}$ для деякого $k > 0$. Нехай $p\mathsf{A} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_s^{e_s}$ – канонічний розклад ідеалу $p\mathsf{A}$. Тоді $a \in \mathfrak{p}_i$ для всіх i, звідки $a \in \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_s$. Якщо всі $e_i = 1$, це означає, що $a \in p\mathsf{A}$, тобто $a + p\mathsf{A} = 0$. Отже, у цьому випадку фактор-кільце не містить ненульових нільпотентів. Якщо ж, наприклад, $e_1 > 1$, то вибравши $a \in p\mathsf{A} = \mathfrak{p}_1^{e_1-1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_s^{e_s}$, але $a \notin p\mathsf{A}$, ми одержимо у фактор-кільці ненульовий нільпотентний елемент.

□

Розгалуженість чи нерозгалуженість первинного числа виявляється пов'язаною з так званим *дискримінантом* поля.

Означення I.7.5. (1) Нехай $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$ – база поля K (як векторного простору над полем раціональних чисел). *Дискримінантом* цієї бази зветься визначник $D(\Omega)$ матриці $\mathrm{T}(\Omega) = (\mathrm{Tr}(\omega_i\omega_j))$.
(2) *Дискримінантом дробового ідеалу* $\mathbf{I}$ зветься дискримінант його бази. Він позначається $D(\mathbf{I})$.
(3) *Дискримінантом поля* K зветься дискримінант $D(\mathsf{A})$ його кільця цілих елементів, тобто дискримінант деякої фундаментальної бази. Він позначається також $D(\mathsf{K})$.

Наступне твердження виправдовує означення дискримінанту ідеалу (зокрема, дискримінанту поля).

Твердження I.7.6. *Дискримінанти всіх баз деякого дробового ідеалу $\mathbf{I}$ збігаються.*

[3]Нагадаємо, що елемент a зветься *нільпотентним*, якщо $a^m = 0$ для деякого натурального m.

Доведення. Дійсно, дискримінант бази Ω – це визначник матриці білінійної форми $\mathrm{T}(\alpha,\beta)=\mathrm{Tr}(\alpha\beta)$. Тому, якщо Ω' – деяка інша база, то $D(\Omega')=|\det S|^2 D(\Omega)$, де S – матриця переходу від бази Ω до бази Ω'. Але якщо і Ω, і Ω' – бази того самого дробового ідеалу, то $|\det S|=\pm 1$ і $D(\Omega)=D(\Omega')$. □

Дискримінанти ідеалів пов'язані наступною формулою з їхніми нормами.

Твердження I.7.7. *$D(\mathbf{I})=\mathrm{N}(\mathbf{I})^2 D(\mathsf{K})$ для довільного дробового ідеалу $\mathbf{I}$.*

Доведення. Якщо $\mathbf{I}\subseteq\mathsf{A}$, то, за твердженням I.6.6, $\mathrm{N}(\mathbf{I})$ – це модуль визначника матриці переходу A від фундаментальної результат. Загальний випадок одразу зводиться до цього, якщо зауважити, що знайдеться таке (звичайне) ціле число b, що $b\mathbf{I}\subseteq\mathsf{A}$: тоді

$$D(\mathbf{I})=b^{-2n}D(b\mathbf{I})=\mathrm{N}(b)^{-2}\mathrm{N}(b\mathbf{I})^2 D(\mathsf{K})=\mathrm{N}(\mathbf{I})^2 D(\mathsf{K}).$$

□

За допомогою дискримінанту можна дати *ознаку розгалуженості*.

Теорема I.7.8. *Первинне число p є розгалуженим у полі K тоді й лише тоді, коли воно ділить дискримінант цього поля.*

Доведення. Розглянемо кільце лишків $\Lambda=\mathsf{A}/p\mathsf{A}$. Воно є комутативною алгеброю над полем лишків $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$. Якщо $\Omega=\{\omega_1,\omega_2,\ldots,\omega_n\}$ – фундаментальна база поля K, тобто база адитивної групи кільця A, то класи лишків $\overline{\omega}_i=\omega_i+p\mathsf{A}$ $(i=1\ldots n)$ утворюють базу $\overline{\Omega}$ алгебри Λ над полем $\mathbb{Z}_p$. Для довільного елемента γ цієї алгебри можна означити лінійне відображення $L_\gamma:\Lambda\to\Lambda$, який переводить $\alpha\in\Lambda$ в $\gamma\alpha$. Тому знов-таки можна означити *слід* $\mathrm{Tr}(\gamma)$ елемента γ як слід цього відображення і означити *дискримінант* $D(\Theta)$ деякої бази $\Theta=\{\theta_1,\theta_2,\ldots,\theta_n\}$ алгебри Λ як визначник матриці $(\mathrm{Tr}(\theta_i\theta_j))$. Зокрема очевидно, що $D(\overline{\Omega})=D+p\mathsf{A}$, де $D=D(\Omega)$ – дискримінант поля K. Зауважимо також, що дискримінанти різних баз алгебри Λ відрізняються ненульовим множником (квадратом визначника матриці переходу). Тому або всі вони рівні нулю, або жоден з них нулю не дорівнює. Зокрема, зважаючи на твердження I.3.4, ми бачимо, що D ділиться на p тоді й лише тоді, коли дискримінант *якоїсь* бази алгебри Λ дорівнює нулю.

Припустимо, що первинне число p є розгалуженим, тобто за твердженням I.7.4 алгебра Λ містить ненульовий нільпотентний елемент β. Очевидно, можна вважати, що вже $\beta^2=0$. Виберемо базу $\theta_1,\theta_2,\ldots,\theta_r$ ідеалу $\beta\Lambda$ і доповнимо її до бази $\Theta=\{\theta_1,\theta_2,\ldots,\ \theta n\}$ алгебри Λ. У цій базі матриця відображення L_γ для довільного елемента $\gamma\in\beta\Lambda$ має вигляд:

$$\begin{pmatrix}0 & X\\ 0 & 0\end{pmatrix}$$

для деякої матриці X розміру $r \times (n-r)$, звідки $\mathrm{Tr}(\gamma) = 0$. Зокрема, $\mathrm{Tr}(\theta_i\theta_j) = 0$ при $i \le r$, а тому $D(\Theta) = 0$ і D ділиться на p.

Нехай тепер p нерозгалужене, тобто $p\mathsf{A} = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_s$, де всі співмножники – попарно різні. Тоді за теоремою I.6.4 $\Lambda \simeq \prod_{i=1}^{s}\Lambda_i$, де $\Lambda_i = \mathsf{A}/\mathfrak{p}_i$ є полем. Вибравши базу Θ алгебри Λ, яка є об'єднанням баз Θ_i співмножників, легко бачити, що $D(\Theta) = \prod_{i=1}^{s} D(\Theta_i)$. Отже, нам залишилося довести наступне твердження.

Твердження I.7.9. *Якщо* L *– скінченне розширення поля лишків* $\mathbb{Z}_p$*, то дискримінант його бази ненульовий.*

Доведення. Якщо дискримінант якоїсь бази поля L нульовий, то білінійна форма $\mathrm{T}(\alpha,\beta) = \mathrm{Tr}(\alpha\beta)$ на просторі L є виродженою, тобто існує ненульовий елемент α_0, для якого $\mathrm{T}(\alpha_0,\beta) = 0$ для довільного β. Звідси маємо, що для довільного $\alpha \in L$

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha_0\cdot\alpha_0^{-1}\alpha) = \mathrm{T}(\alpha_0,\,\alpha_0^{-1}\alpha) = 0\,.$$

Позначимо $m = (\mathsf{L} : \mathbb{Z}_p)$. Тоді, зокрема, $\mathrm{Tr}(1) = m\cdot 1 = 0$, тобто m ділиться на p. Добре відомо, що $\mathsf{L} = \mathbb{Z}_p(\theta)$, де θ – корінь незвідного многочлена $f(x) \in \mathbb{Z}_p[x]$ ступеня m (див., напр., [**K**, гл.9, §1, теорема 5]). Крім того, цей многочлен не має кратних коренів. Позначимо його корені $\theta_1,\theta_2,\dots,\theta_m$. Нехай $f(x) = x^m + a_1x^{m-1} + \dots + a_m$. Тоді $1,\theta,\theta^2\dots,\theta^{m-1}$ – база L, в якій матриця лінійного відображення L_θ має вигляд:

$$\Phi_\theta = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_m \\ 1 & 0 & \dots & 0 & -a_{m-1} \\ 0 & 1 & \dots & 0 & -a_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}$$

Характеристичним многочленом цієї матриці є $f(x)$. Він має m різних коренів $\theta_1,\theta_2,\dots,\theta_m$, а тому матриця Φ_θ подібна до діагональної матриці $\mathrm{diag}\,(\theta_1,\theta_2,\dots,\theta_m)$. Отже, $\mathrm{Tr}\theta = \mathrm{Tr}\Phi_\theta = \sum_{i=1}^{m}\theta_i$. Так само $\mathrm{Tr}\theta^k = \mathrm{Tr}\Phi_\theta^k = \sum_{i=1}^{m}\theta_i^k$ для довільного k. Якщо всі ці сліди нульові, то бачимо, що ненульовий вектор $(1,1,\dots,1)$ є розв'язком однорідної квадратної системи лінійних рівнянь:

$$\sum_{i=1}^{m}\theta_i^k x_i = 0 \quad (k = 0,1,\dots,m-1)\,.$$

Але визначник цієї системи – це визначник Вандермонда попарно різних елементів $\theta_1,\theta_2,\dots,\theta_m$, який не дорівнює 0. Одержане протиріччя показує, що не всі сліди елементів з поля L нульові, тобто дискримінант довільної бази поля L не дорівнює нулю. □

Зауважимо, що, оскільки $\mathrm{Tr}(1) = n \ne 0$, дискримінант поля K не дорівнює нулю.

Наслідок I.7.10. *Для кожного скінченного розширення поля раціональних чисел існує лише скінченна кількість первинних чисел, розгалужених у ньому.*

У багатьох випадках "закони розкладу" первинних чисел у полі K можна одержати за допомогою міркувань, цілком аналогічних тим, які були застосовані в розділі I.1 при пошуку первинних ґауссових чисел. Відомо, що довільне скінченне розширення K поля раціональних чисел є його *простим розширенням*, тобто містить такий елемент θ, що $\mathsf{K} = \mathbb{Q}(\theta)$ (див., напр., [**Ф**]). Припустимо, що елемент θ можна вибрати так, що $\mathsf{A} = \mathbb{Z}[\theta]$, тобто елементи $1, \theta, \theta^2, \dots, \theta^{n-1}$ утворюють фундаментальну базу. Тоді для довільного первинного числа p класи лишків $\overline{\theta}^i$, де $\overline{\theta} = \theta + p\mathsf{A}$, при $i = 0 \dots n-1$ утворюють базу алгебри $\Lambda = \mathsf{A}/p\mathsf{A}$ над полем лишків $\mathbb{Z}_p$. Отже, $\Lambda \simeq \mathbb{Z}_p[x]/\overline{\mu}(x)\mathbb{Z}_p[x]$, де $\mu(x)$ – мінімальний многочлен елемента θ над полем раціональних чисел, а $\overline{\mu}(x)$ – його редукція за модулем p (нагадаємо, що, за наслідком I.3.5, $\mu(x)$ має цілі коефіцієнти). Розкладемо многочлен $\overline{\mu}(x)$ на незвідні множники. Інакше кажучи, знайдемо такі многочлени $\varphi_j(x) \in \mathbb{Z}[x]$ зі старшими коефіцієнтами 1, що їхні редукції $\overline{\varphi}_j(x)$ за модулем p є попарно різними многочленами, незвідними над полем лишків, причому $\overline{\mu}(x) = \prod_{j=1}^{s} \overline{\varphi}_j^{e_j}$. Позначимо $\mathfrak{p}_j = p\mathsf{A} + \varphi_j(\theta)\mathsf{A}$ для $j = 1 \dots s$.

Теорема I.7.11. *В описаній вище ситуації всі ідеали $\mathfrak{p}_j$ є первинними і канонічний розклад ідеалу $p\mathsf{A}$ має вигляд: $p\mathsf{A} = \prod_{j=1}^{s} \mathfrak{p}_j^{e_j}$.*

Доведення. Ми весь час будемо ототожнювати факторкільце $\Lambda = \mathsf{A}/p\mathsf{A}$ з $\mathbb{Z}_p[x]/\overline{\mu}(x)\mathbb{Z}_p[x]$. У цьому кільці ідеал $\mathfrak{p}_j/p\mathsf{A}$ є головним, породженим елементом $\overline{\varphi}(\overline{\theta})$. Інакше кажучи, він збігається з $\overline{\varphi}(x)\mathbb{Z}_p[x]/\overline{\mu}(x)\mathbb{Z}_p[x]$. Але ідеал $\mathfrak{q}_j = \overline{\varphi}(x)\mathbb{Z}_p[x]$ – первинний у кільці многочленів $\mathbb{Z}_p[x]$, тому $\Lambda/\mathfrak{p}_j \simeq \mathbb{Z}_p[x]/\mathfrak{q}_j$ є полем, тобто $\mathfrak{p}_j$ – первинний ідеал. Крім того очевидно, що $\prod_{j=1}^{s} \mathfrak{p}_j^{e_j} \subseteq p\mathsf{A}$. З іншого боку, ніякий добуток $\prod_{j=1}^{s} \mathfrak{p}_j^{l_j}$, в якому $l_j < e_j$ хоч би для одного номера j, не міститься в $p\mathsf{A}$, оскільки $\prod_{j=1}^{s} \overline{\varphi}_j(\overline{\theta})^{l_j} \neq 0$. Це свідчить про те, що дійсно $p\mathsf{A} = \prod_{j=1}^{s} \mathfrak{p}_j^{e_j}$. □

Вправи I.7.

(1) Нехай $\mathsf{K} = \mathbb{Q}(\theta)$, де θ – корінь незвідного многочлена $f(x) \in \mathbb{Q}[x]$ ступеня n зі старшим коефіцієнтом 1. Доведіть, шо дискримінант бази $1, \theta, \theta^2, \dots, \theta^{n-1}$ дорівнює дискримінанту цього многочлена, тобто добутку $\prod_{i<j}(\theta_i - \theta_j)^2$, де $\theta_1, \theta_2, \dots, \theta_n$ – всі корені многочлена $f(x)$ в деякому його полі розкладу.

(2) Нехай $f(x) \in \mathbb{Z}[x]$ – незвідний многочлен зі старшим коефіцієнтом 1, $\mathsf{K} = \mathbb{Q}(\theta)$, де θ – корінь $f(x)$, і D – дискримінант многочлена $f(x)$. Доведіть, що теорема I.7.11 залишається вірною для довільного первинного числа p, яке не ділить D.

(3) Нехай $\mathsf{K} = \mathbb{Q}(\sqrt{d})$, де d – ціле число, яке не ділиться на квадрати первинних чисел, $D = D(\mathsf{K})$ – його дискримінант.

(a) Доведіть, що $D = d$, якщо $d \equiv 1 \pmod 4$, і $D = 4d$, якщо $d \not\equiv 1 \pmod 4$.

(b) Доведіть, що первинне непарне число p розкладається в полі K в наступний спосіб:

$$p\mathsf{A} = \begin{cases} \mathfrak{p}^2\,, & \text{де } \mathrm{N}(\mathfrak{p}) = p\,, & \text{якщо } p \text{ ділить } d \\ \mathfrak{p}_1\mathfrak{p}_2\,, & \text{де } \mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p\,, & \text{якщо } \left(\frac{d}{p}\right) = 1 \\ \mathfrak{p}\,, & \text{де } \mathrm{N}(\mathfrak{p}) = p^2\,, & \text{якщо } \left(\frac{d}{p}\right) = -1 \end{cases}$$

(c) Користуючись квадратичним законом взаємності, виведіть звідси, що закон розкладу первинного непарного p залежить лише від його залишку за модулем D.

(d) Виведіть закон розкладу в полі K для первинного числа 2.

(Скористайтеся результатом вправи I.3 (1) і Теоремою I.7.11).

(4) Нехай $\Omega = \{\,\omega_1, \omega_2, \ldots, \omega_n\,\}$ – деяка база поля K, $\Omega^* = \{\,\omega_1^*, \omega_2^*, \ldots, \omega_n^*\,\}$ – *двоїста база*, тобто така, що $\mathrm{T}(\omega_i, \omega_j) = \delta_{ij}$.

(a) Доведіть, що коли $\omega_j = \sum_{i=1}^n c_{ij}\omega_i^*$ $(j = 1, \ldots, n)$, то $D(\Omega)$ дорівнює визначнику матриці (c_{ij}).

(b) Виведіть звідси, що коли всі числа c_{ij} є цілими, то $|D(\Omega)|$ дорівнює індексу $(A^* : A)$, де A і A^* – це відповідно підгрупи, породжені елементами $\omega_1, \omega_2, \ldots, \omega_n$ і $\omega_1^*, \omega_2^*, \ldots, \omega_n^*$.

(5) Нехай A – кільце цілих елементів деякого поля алгебричних чисел K. Позначимо

$$\mathsf{A}^* = \{\,\gamma \in \mathsf{K} \mid \mathrm{Tr}(\gamma\alpha) \in \mathbb{Z} \text{ для всіх } \alpha \in \mathsf{A}\,\}\,.$$

(a) Перевірте, що A^* – дробовий ідеал поля K, причому $(\mathsf{A}^*)^{-1}$ є цілим ідеалом. Останній звуть *диферентою* поля K і позначають $\mathbf{d}(\mathsf{K})$.

(b) Доведіть, що $|D(\mathsf{K})| = \mathrm{N}(\mathbf{d}(\mathsf{K}))$.

(c) Виведіть звідси, що розгалуженими первинними ідеалами кільця A є первинні дільники диференти і лише вони.

(6) Нехай L – підполе поля K, B і A – кільця цілих елементів відповідно в L і K.

(a) Доведіть, що довільний первинний ідеал $\mathfrak{p}$ кільця A містить єдиний первинний ідеал Π кільця B. При цьому $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\Pi)^f$ для деякого натурального f.

(b) Нехай Π – первинний ідеал кільця B, $q = \mathrm{N}(\Pi)$ і $\Pi\mathsf{A} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_s^{e_s}$ – канонічний розклад у кільці A ідеалу $\Pi\mathsf{A}$. Довести, що

(i) $\mathrm{N}(\mathfrak{p}_i) = q^{f_i}$ для кожного номера i;

(ii) $\sum_{i=1}^s e_i f_i = (\mathsf{K} : \mathsf{L})$.

(Скористайтесь вправою I.6 (3b)).

Звісно, показники e_i та f_i звуться відповідно *індексом розгалуження* і *ступенем інерції* первинного ідеалу $\mathfrak{p}_i$ відносно

підполя L. Визначте аналогічно означенню I.7.3 *розгалужені* ідеали та ідеали *першого ступеня* відносно підполя L, а також ідеали кільця B, *нерозгалужені* та *цілком розкладні* в полі K.

(7) Ми зберігаємо позначення і термінологію попередньої вправи.
   (a) Доведіть, що первинне число p, розгалужене в полі L, є також розгалуженим у полі K, а первинне число, цілком розкладне в полі K, є також цілком розкладним у полі L.
   (b) Доведіть, що первинне число p є нерозгалуженим у полі K тоді й лише тоді, коли воно є нерозгалуженим у полі L і всі первинні ідеали кільця B, які містить p, є нерозгалуженими в полі K.
   (c) Доведіть, що первинне число p є цілком розкладним у полі K тоді й лише тоді, коли воно є цілком розкладним у полі L і всі первинні ідеали кільця B, які містять p, є цілком розкладними в полі K.
   (d) Узагальніть ці результати на випадок *башти полів* $\mathsf{L} \subset \mathsf{F} \subset \mathsf{K}$.

(8) У тих же позначеннях, що і в попередніх вправах, нехай

$$\mathsf{A}' = \left\{ \gamma \in \mathsf{K} \,|\, \mathrm{Tr}_{\mathsf{K}/\mathsf{L}}(\gamma\alpha) \in \mathsf{B} \text{ для всіх } \alpha \in \mathsf{A} \right\} .$$

   (a) Перевірте, що A' – дробовий ідеал поля K, причому $(\mathsf{A}')^{-1} \subseteq \mathsf{A}$. Останній ідеал зветься *диферентою поля* K *відносно підполя* L і позначається $\mathbf{d}(\mathsf{K}/\mathsf{L})$, а його норма відносно підполя L зветься *дискримінантом поля* K *відносно підполя* L і позначається $D(\mathsf{K}/\mathsf{L})$.
   (b) Доведіть, що первинний ідеал $\mathfrak{p} \subset \mathsf{A}$ є розгалуженим відносно підполя L тоді й лише тоді, коли він є дільником $\mathbf{d}(\mathsf{K}/\mathsf{L})$.
   (c) Доведіть, що первинний ідеал $\Pi \subset \mathsf{B}$ є розгалуженим у полі K тоді й лише тоді, коли він є дільником $D(\mathsf{K}/\mathsf{L})$.

(9) У позначеннях попередніх вправ доведіть наступні формули для диферент і дискримінантів:

$$\begin{aligned} \mathbf{d}(\mathsf{K}) &= \mathbf{d}(\mathsf{L})\mathbf{d}(\mathsf{K}/\mathsf{L}) ; \\ D(\mathsf{K}) &= D(\mathsf{L})^m \mathrm{N}_L(D(\mathsf{K}/\mathsf{L})) . \end{aligned}$$

Перенесіть ці результати на випадок "відносних" диферент і дискримінантів $\mathbf{d}(\mathsf{K}/F)$ і $D(\mathsf{K}/F)$, де $\mathsf{F} \subset \mathsf{L} \subset \mathsf{K}$.

(10) Перенесіть результати цього розділу на випадок *кілець алгебричних функцій*.

Розділ II

Геометричні методи

II.1. Геометричне зображення алгебричних чисел

У цьому і наступних розділах K позначатиме скінченне розширення поля раціональних чисел ступеня $n = (\mathsf{K} : \mathbb{Q})$, A – кільце цілих елементів поля K.

Введемо перш за все деяку систему позначень. Виберемо такий елемент $\theta \in \mathsf{K}$, що $\mathsf{K} = \mathsf{K}(\theta)$. Нехай $\mu(x) \in \mathbb{Q}[x]$ – мінімальний многочлен елемента θ. Це незвідний над полем раціональних чисел многочлен ступеня n, тому він має n різних коренів у полі комплексних чисел. Більш того, *уявні* корені, тобто ті, які не є дійсними, розбиваються на пари попарно спряжених. Нехай $\theta_1, \theta_2, \ldots, \theta_r$ – попарно різні *дійсні корені* многочлена $\mu(x)$, θ_{r+1}, $\overline{\theta}_{r+1}, \ldots, \theta_{r+t}, \overline{\theta}_{r+t}$ – попарно різні пари його спряжених уявних коренів (очевидно, $r + 2t = n$). Тоді $\mathsf{K} \simeq \mathbb{Q}(\theta_i)$ для кожного $i = 1, \ldots, r + t$ і при цьому ізоморфізмі θ переходить у θ_i. Отже, одержуємо r різних занурень $\sigma_i : \mathsf{K} \to \mathbb{R}$ $(i = 1, \ldots, r)$ і t різних і попарно неспряжених занурень $\sigma_i : \mathsf{K} \to \mathbb{C}$ $(i = r+1, \ldots, r+t)$, образи яких не містяться в полі дійсних чисел. Будемо звати σ_i при $1 \le i \le r$ *дійсними зануреннями*, а при $r + 1 \le i \le r + t$ – *уявними зануреннями* поля K. Зауважимо, що, додавши до $\sigma_1, \sigma_2, \ldots, \sigma_{r+t}$ ще *спряжені* занурення $\overline{\sigma}_j$ $(j = r + 1, \ldots, r + t)$, де за означенням $\overline{\sigma}_j(\alpha) = \overline{\sigma_j(\alpha)}$, ми одержимо *всі* занурення поля K в поле комплексних чисел.

Позначимо $\sigma : \mathsf{K} \to \mathbb{R}^r \times \mathbb{C}^t$ відображення, яке ставить елементу $\alpha \in \mathsf{K}$ у відповідність набір $(\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{r+t}(\alpha))$. Цей набір зветься *геометричним зображенням* елемента α. Звичайно, простір $\mathfrak{G} = \mathbb{R}^r \times \mathbb{C}^t$, в якому всі ці зображення лежать, ми розглядатимемо як n-вимірний простір над полем дійсних чисел. Зафіксуємо в цьому просторі евклідову (а тому й метричну) структуру, вважаючи ортонормованою його "стандартну" базу

$$\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{r+t}, i\mathbf{e}_{r+1}, i\mathbf{e}_{r+2}, \ldots, i\mathbf{e}_{r+t}, \tag{6}$$

де $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 на j-му місці). Більш того, $\mathfrak{G}$ є алгеброю над полем дійсних чисел (з покоординатними операціями) і відображення σ є, очевидно, гомоморфізмом кілець. Знов-таки, для довільного елемента $\mathbf{a} \in \mathfrak{G}$ можна означити лінійне відображення $L_{\mathbf{a}} : \mathfrak{G} \to \mathfrak{G}$, а тому *характеристичний многочлен* $\chi(\mathbf{a}; x)$, *слід* $\mathrm{Tr}(\mathbf{a})$ і *норму* $\mathrm{N}(\mathbf{a})$. Обчислюючи їх у стандартній базі (6), безпосередньо одержуємо такий результат.

Твердження II.1.1. *Для довільного елемента* $\mathbf{a} = (a_1, a_2, \dots, a_{r+t}) \in \mathfrak{G}$

$$\begin{aligned} \chi(\mathbf{a};\, x) &= \prod_{j=1}^{r+t}(x - a_j) \prod_{j=r+1}^{r+t} (x - \overline{a_j})\,; \\ \mathrm{Tr}(\mathbf{a}) &= \sum_{j=1}^{r} a_j + \sum_{j=r+1}^{r+t} 2\Re a_j\,; \\ \mathrm{N}(\mathbf{a}) &= \prod_{j=1}^{r+t} \mathrm{N}_j(\mathbf{a})\,, \end{aligned}$$

де позначено:

$$\mathrm{N}_j(\mathbf{a}) = \begin{cases} a_j & \text{при } 1 \le j \le r \\ |a_j|^2 & \text{при } r+1 \le j \le r+t \end{cases}$$

а $\Re z$ *– дійсна частина комплексного числа* z*.*

Якщо $\mathbf{a} = \sigma(\gamma)$, де $\gamma \in \mathsf{K}$, то замість $\mathrm{N}_j(\sigma(\gamma))$ ми будемо писати просто $\mathrm{N}_j(\gamma)$. Наступне важливе твердження закладає основу застосування геометричних методів до вивчення арифметики алгебричних чисел.

Твердження II.1.2. *Для довільної бази* $\Omega = \{\, \omega_1, \omega_2, \dots,\ \omega n \,\}$ *поля* K *над полем раціональних чисел елементи* $\sigma(\omega_1)$, $\sigma(\omega_2), \dots, \sigma(\omega_n)$ *утворюють базу простору* $\mathfrak{G}$ *над полем дійсних чисел.*

Доведення. Нехай $\sigma_j(\omega_k) = a_{kj} + ib_{kj}$, де, звичайно, $b_{kj} = 0$ при $j \le r$. Припустимо, що вектори $\{\, \sigma(\omega_j) \,|\, j = 1 \dots r+t \,\}$ лінійно залежні над полем дійсних чисел. Переходячи до координат у "стандартній" базі (6), бачимо, що матриця

$$\sigma(\Omega) = \begin{pmatrix} a_{11} & \dots & a_{1r} & a_{1,r+1} & b_{1,r+1} & \dots & a_{1,r+t} & b_{1,r+t} \\ a_{21} & \dots & a_{2r} & a_{2,r+1} & b_{2,r+1} & \dots & a_{2,r+t} & b_{2,r+t} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \dots & a_{nr} & a_{n,r+1} & b_{n,r+1} & \dots & a_{n,r+t} & b_{n,r+t} \end{pmatrix} \tag{7}$$

є виродженою. Отже, її стовпчики є лінійно залежними, тобто знайдуться дійсні числа $c_1, c_2, \dots, c_{r+t}$ і $d_{r+1}, \dots, d_{r+t}$, які не всі дорівнюють нулю, такі що для всіх номерів $k = 1 \dots n$

$$\sum_{j=1}^{r+t} c_j a_{kj} + \sum_{j=r+1}^{r+t} d_j b_{kj} = 0\,,$$

або

$$\sum_{j=1}^{r} c_j \sigma_j(\omega_k) + \sum_{j=r+1}^{r+t} d_j^- \sigma_j(\omega_k) + \sum_{j=r+1}^{r+t} d_j^+ \overline{\sigma}_j(\omega_k) = 0\,, \tag{8}$$

де $d_j^{\pm} = (c_j \pm d_j i)/2$. Оскільки $\omega_1, \omega_2, \ldots, \omega_n$ – база поля K, рівність (8) залишиться вірною, якщо в ній замінити ω_k на довільний елемент з цього поля. Підставляючи в неї по черзі ступені θ^k $(k = 0, \ldots, n-1)$, одержимо, що визначник Вандермонда чисел $\theta_1, \theta_2, \ldots, \theta_r, \theta_{r+1}, \overline{\theta}_{r+1}, \ldots, \theta_{r+t}, \overline{\theta}_{r+t}$ дорівнює нулю, що неможливо, оскільки ці елементи попарно різні. Отже, наше припущення несправедливе і вектори $\sigma(\omega_k)$ лінійно незалежні. Оскільки їхня кількість дорівнює розмірності простору $\mathfrak{G}$, вони утворюють його базу. □

Обчислюючи в цій базі матрицю відображення $L_{\sigma(\alpha)}$, одержуємо наступні рівності.

Наслідок II.1.3. *Для довільного елемента $\alpha \in \mathsf{K}$ мають місце рівності:*

$$\begin{aligned} \chi(\alpha;\, x) &= \chi(\sigma(\alpha);\, x)\,, \\ \mathrm{N}(\alpha) &= \mathrm{N}(\sigma(\alpha)) = \prod_{j=1}^{r+t} \mathrm{N}_j(\alpha)\,, \\ \mathrm{Tr}(\alpha) &= \mathrm{Tr}(\sigma(\alpha))\,. \end{aligned}$$

Наслідок II.1.4. *Для довільної бази $\Omega = \{\, \omega_1, \omega_2, \ldots, \omega_n \,\}$ поля K має місце рівність:*

$$D(\Omega) = (-1)^t 2^{2t} (\det \sigma(\Omega))^2\,,$$

де матриця $\sigma(\Omega)$ визначається рівністю (7).

Доведення. Зробимо з матрицею $\sigma(\Omega)$ наступні перетворення:

(1) До кожного стовпчика, що містить елементи a_{kj} при $j > r$, додамо стовпчик, що містить відповідні елементи b_{kj}, домноживши його на i (при цьому визначник матриці не зміниться).
(2) Домножимо кожен стовпчик, що містить елементи b_{kj}, на $-2i$ (при цьому визначник домножиться на $(-2i)^t$).
(3) До кожного з одержаних після такого домноження стовпчиків додамо відповідний стовпчик, який тепер містить елементи $a_{kj} + ib_{kj}$ (при цьому також визначник не зміниться).

У результаті одержимо матрицю A, рядками якої є вектори

$$(\sigma_1(\omega_k), \ldots, \sigma_r(\omega_k), \sigma_{r+1}(\omega_k), \overline{\sigma}_{r+1}(\omega_k), \ldots, \sigma_{r+t}(\omega_k), \overline{\sigma}_{r+t}(\omega_k))\,,$$

а визначник дорівнює $(-2i)^t \det \sigma(\Omega)$. Розглянемо матрицю $AA^{\top}$. На місці з номером (kl) в ній стоїть число

$$\sum_{j=1}^{r+t} \sigma_j(\omega_k \omega_l) + \sum_{j=r+1}^{r+t} \overline{\sigma}_j(\omega_k \omega_l)\,,$$

яке дорівнює $\mathrm{Tr}(\omega_k \omega_l)$ за твердженням II.1.1 і наслідком II.1.3. Отже, $\det AA^{\top} = D(\Omega)$, звідки

$$D(\Omega) = (\det A)^2 = (-2i)^{2t} (\det \sigma(\Omega))^2 = (-1)^t 2^{2t} (\det \sigma(\Omega))^2\,.$$

□

Зауважимо, що, як відомо, $|\det\sigma(\Omega)|$ дорівнює *об'єму n-вимірного паралелепіпеда*, утвореного базисними векторами $\sigma(\omega_k)$. Позначимо цей об'єм $V(\Omega)$. Тоді останній наслідок можна переписати у вигляді наступної формули:

$$V(\Omega) = \frac{\sqrt{|D(\Omega)|}}{2^t}\,.$$

Наостанок для довільних додатних дійсних чисел $C_1, C_2, \ldots, C_{r+t}$ розглянемо у просторі $\mathfrak{G}$ підмножину $\mathcal{X} = \mathcal{X}(C_1, C_2, \ldots, C_{r+t})$, визначену умовами:

$$\mathcal{X} = \{\, \mathbf{a} \in \mathfrak{G} \,|\, |\mathrm{N}_j(\mathbf{a})| \le C_j \text{ для всіх номерів } j \,\}\,. \tag{9}$$

(у позначеннях твердження II.1.1).

Твердження II.1.5. *Об'єм тіла $\mathcal{X}\,(C_1, C_2, \ldots, C_{r+t})$ дорівнює $2^r\pi^t C_1 C_2 \ldots C_{r+t}$.*

Доведення. Позначимо $dx_1, dx_2, \ldots, dx_{r+t}, dy_{r+1}, \ldots, dy_{r+t}$ координати у "стандартній базі" (6) простору $\mathfrak{G}$. Нагадаємо, що за означенням об'єм V тіла $\mathcal{X} = \mathcal{X}\,(C_1, C_2, \ldots, C_{r+t})$ дорівнює інтегралу

$$V = \int_{\mathcal{X}} dx_1 dx_2 \ldots dx_{r+t} dy_{r+1} \ldots dy_{r+t}\,,$$

який одразу перетворюється на добуток інтегралів:

$$\begin{aligned} V \;=\; & \int_{-C_1}^{C_1} dx_1 \ldots \int_{-C_r}^{C_r} dx_r \int_{x_{r+1}^2 + y_{r+1}^2 \le C_{r+1}} dx_{r+1} dy_{r+1} \ldots \cdot \\ & \cdot \int_{x_{r+t}^2 + y_{r+t}^2 \le C_{r+t}} dx_{r+t} dy_{r+t}\,. \end{aligned}$$

Але перші r інтегралів тут дорівнюють відповідно $2C_1, \ldots, 2C_r$, а останні t – $\pi C_{r+1}, \ldots, \pi C_{r+t}$ (площа круга радіусу $\sqrt{C_j}$), звідки і одержуємо необхідну формулу. □

Вправи II.1. (1) Позначимо $\mathcal{Y} = \mathcal{Y}(C)$, де C – додатне дійсне число, тіло в $\mathfrak{G}$, задане умовою:

$$\mathcal{Y} = \left\{ (a_1, a_2, \ldots, a_{r+t}) \mid \sum_{j=1}^{r} |a_j| + 2 \sum_{j=r+1}^{r+t} |a_j| \le C \right\}.$$

Доведіть, що об'єм тіла $\mathcal{Y}(C)$ дорівнює

$$\frac{2^r}{n!} \left(\frac{\pi}{2}\right)^t C^n\,.$$

(див., напр., [**Л2**, гл.V, §3]).

II.2. Лема Мінковського

Вирішальну роль у наступних розділах (і в багатьох інших застосуваннях геометричних методів у теорії чисел) відіграє результат, відомий під назвою "леми Мінковського". Нагадаємо спочатку деякі поняття.

Означення II.2.1. Підмножина $\mathcal{M}$ у векторному просторі над полем дійсних чисел зветься *опуклою*, якщо з того, що $\mathbf{a}, \mathbf{b} \in \mathcal{M}$, випливає, що $\lambda\mathbf{a} + (1-\lambda)\mathbf{b} \in \mathcal{M}$ для довільного λ з інтервалу $(0,1)$.

Надалі, кажучи *"тіло"*, ми завжди матимемо на увазі таку підмножину $\mathcal{M}$ у деякому евклідовому просторі, яка *має об'єм*, тобто існує інтеграл

$$\mathrm{vol}\,(\mathcal{M}) = \int_{\mathcal{M}} dx_1 dx_2 \dots dx_n\,,$$

(який і зветься *об'ємом тіла* $\mathcal{M}$). Тут, звичайно, $x_1, x_2, \dots, x_n$ – координати в деякій ортонормованій базі даного простору.

Означення II.2.2. (1) *m-вимірною ґраткою* в дійсному векторному просторі зветься довільна множина $\mathbf{L}$ вигляду

$$\mathbf{L} = \left\{ \sum_{j=1}^{m} a_j \mathbf{v}_j \,|\, a_j \in \mathbb{Z} \right\},$$

де $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ – деякий набір лінійно незалежних векторів цього простору, який зветься *базою ґратки* $\mathbf{L}$.

(2) Множина

$$\left\{ \sum_{j=1}^{m} \lambda_j \mathbf{v}_j \,|\, 0 \le \lambda_j < 1 \right\}$$

зветься *базовим паралелепіпедом* ґратки $\mathbf{L}$, а її (m-вимірний) об'єм – *базовим об'ємом* цієї ґратки.

Звичайно, та сама ґратка має безліч різних баз і відповідно безліч базових паралелепіпедів, але, як легко бачити, базовий об'єм ґратки не залежить від вибору бази. Надалі в основному ми матимемо справу з так званими *повними ґратками*, тобто такими, що їхня розмірність m дорівнює розмірності всього простору. Тоді базовий об'єм обчислюється як $|\det A|$, де A – матриця, складена з координат базових векторів ґратки $\mathbf{v}_j$ відносно деякої ортонормованої бази простору. Термін "базовий паралелепіпед" пояснюється наступним очевидним фактом.

Твердження II.2.3. *Нехай $\mathbf{L}$ – повна ґратка в деякому просторі $\mathbf{V}$, $\mathbf{P}$ – її базовий паралелепіпед. Тоді $\mathbf{V} = \bigsqcup_{\mathbf{a}\in\mathbf{L}} \mathbf{a} + \mathbf{P}$ (незв'язне об'єднання), де, як звичайно, $\mathbf{a} + \mathbf{P} = \{\, \mathbf{a} + \mathbf{v} \,|\, \mathbf{v} \in \mathbf{P} \,\}$.*

Нагадаємо також, що підмножина $\mathcal{M}$ у векторному просторі зветься *центрально симетричною*, якщо з того, що $\mathbf{v} \in \mathcal{M}$, випливає, що

$-\mathbf{v} \in \mathcal{M}$. Зауважимо, що коли ця підмножина є також і *опуклою*, то обов'язково $0 \in \mathcal{M}$ і $\lambda\mathbf{a} \in \mathcal{M}$ для довільного вектора $\mathbf{a} \in \mathcal{M}$ і довільного дійсного числа $\lambda < 1$.

Теорема II.2.4 (Лема Мінковського). *Нехай $\mathcal{M}$ – центрально симетричне опукле тіло в n-вимірному евклідовому просторі, а $\mathbf{L}$ – повна ґратка в цьому просторі з базовим об'ємом V. Якщо $\mathrm{vol}(\mathcal{M}) > 2^n V$, то тіло $\mathcal{M}$ містить деякий ненульовий елемент ґратки $\mathbf{L}$.*

Доведення. Нехай $\mathbf{P}$ – базовий паралелепіпед даної ґратки. Розглянемо "вдвічи зменшене тіло" $\mathcal{M}/2 = \{\, \mathbf{v}/2 \mid \ \mathbf{v} \in \mathcal{M} \,\}$. Тоді його об'єм дорівнює $2^{-n}\mathrm{vol}(\mathcal{M}) > V$. За твердженням II.2.3 $\mathcal{M}/2 = \bigsqcup_{\mathbf{a}\in\mathbf{L}} \mathcal{M}_\mathbf{a}$, де $\mathcal{M}_\mathbf{a} = (\mathcal{M}/2) \cap (\mathbf{a}+\mathbf{P})$, звідки маємо: $2^{-n}\mathrm{vol}(\mathcal{M}) = \sum_{\mathbf{a}\in\mathbf{L}} \mathrm{vol}(\mathcal{M}_\mathbf{a})$. Позначимо $\mathcal{M}'_\mathbf{a} = \mathcal{M}_\mathbf{a} - \mathbf{a}$. Очевидно $\mathcal{M}'_\mathbf{a} \subseteq \mathbf{P}$ і $\mathrm{vol}(\mathcal{M}'_\mathbf{a}) = \mathrm{vol}(\mathcal{M}_\mathbf{a})$. Оскільки $\sum_{\mathbf{a}\in\mathbf{L}} \mathrm{vol}(\mathcal{M}'_\mathbf{a}) > V$, знайдуться два *різні* вектори $\mathbf{a}, \mathbf{a}' \in \mathbf{L}$, для яких $\mathcal{M}_\mathbf{a} \cap \mathcal{M}_{\mathbf{a}'} \neq \emptyset$. Інакше кажучи, знайдуться такі вектори $\mathbf{v}, \mathbf{v}' \in \mathcal{M}$, що $\mathbf{a} + \mathbf{v}/2 = \mathbf{a}' + \mathbf{v}'/2$. Тоді $\mathbf{a} - \mathbf{a}' = \mathbf{v}/2 + (-\mathbf{v}'/2) \in \mathcal{M}$, оскільки тіло $\mathcal{M}$ є центрально симетричним і опуклим. Але $\mathbf{a} - \mathbf{a}'$ – ненульовий вектор з ґратки $\mathbf{L}$. □

Часом корисним є також наступне уточнення леми Мінковського.

Наслідок II.2.5. *Якщо тіло $\mathcal{M}$ є обмеженим і замкненим, то твердження теореми II.2.4 залишається вірним і за умови, що $\mathrm{vol}(\mathcal{M}) = 2^n V$.*

Доведення. В обмеженому тілі, звичайно, може міститись лише скінченна кількість векторів даної ґратки. Для довільного дійсного числа $\rho > 1$ тіло $\rho\mathcal{M}$ містить ненульовий вектор $\mathbf{a} \in \mathbf{L}$. Позначимо для кожного такого вектора $\lambda(\mathbf{a}) = \sup\{\, \lambda \in \mathbb{R} \mid \lambda\mathbf{a} \in \mathcal{M} \,\}$. Оскільки тіло замкнене, $\lambda(\mathbf{a})\mathbf{a} \in \mathcal{M}$. Ясно, що коли $\mathbf{a} \in \rho\mathcal{M}$, то $\lambda(\mathbf{a}) \geq \rho^{-1}$. Фіксуємо деяке $\rho > 1$ і позначимо $\lambda_0 = \min\{\, \lambda(\mathbf{a}) \mid \ \mathbf{a} \neq 0 \text{ і } \mathbf{a} \in \mathbf{L} \cap \rho\mathcal{M} \,\}$. Якщо $\lambda_0 < 1$, то, вибравши число ρ_0 так, щоб $\lambda_0^{-1} > \rho_0 > 1$, ми одержимо, що в тілі $\rho_0\mathcal{M}$ немає ненульових векторів ґратки $\mathbf{L}$, що неможливо. Отже, $\lambda_0 \geq 1$, а тоді той вектор $\mathbf{a} \in \mathbf{L}$, для якого $\lambda_0 = \lambda(\mathbf{a})$, лежить у $\mathcal{M}$. □

II.3. Скінченність групи класів ідеалів

Скористаймося геометричним зображенням алгебричних чисел і лемою Мінковського для того, щоб довести одну з основних теорем алгебричної теорії чисел. Нагадаємо, що *група класів ідеалів* поля K – це факторгрупа групи всіх дробових ідеалів цього поля за підгрупою головних дробових ідеалів. °ї елементи звуться *класами ідеалів* поля K.

Теорема II.3.1. *Для довільного скінченного розширення K поля раціональних чисел група класів ідеалів $\mathcal{C}(\mathsf{K})$ є скінченною.*

Доведення. Встановимо деякі факти щодо норм алгебричних чисел та ідеалів. Як і раніше, позначимо $n = (\mathsf{K} : \mathbb{Q})$, A – кільце цілих

алгебричних елементів поля K та $\sigma : \mathsf{K} \to \mathfrak{G} = \mathbb{R}^r \times \mathbb{C}^t$ – його геометричне зображення, де r – число дійсних занурень, а t – число пар спряжених уявних занурень поля K. Спочатку виведемо наступний наслідок з результатів попередніх розділів.

Твердження II.3.2. *Нехай* $\mathbf{L}$ *– ґратка у просторі* $\mathfrak{G}$ *з фундаментальним об'ємом* V, *а* $C_1, C_2, \ldots, C_{r+t}$ *– довільний набір додатніх дійсних чисел, такий що* $C_1 C_2 \ldots C_{r+t} \geq (4/\pi)^t V$. *Тоді в ґратці* $\mathbf{L}$ *є ненульовий елемент, який належить тілу* $\mathcal{X} = \mathcal{X}(C_1, C_2, \ldots, C_{r+t})$, *визначеному формулою (9).*

Доведення. Згідно з твердженням II.1.5 $\mathrm{vol}(\mathcal{X}) = 2^r \pi^t C_1 C_2 \ldots C_{r+t}$. Очевидно, тіло $\mathcal{X}$ є центрально симетричним, опуклим, обмеженим і замкненим, тобто до нього можна застосувати Наслідок II.2.5. Отже, якщо $\mathrm{vol}(\mathcal{X}) \geq 2^n V$, у ґратці $\mathbf{L}$ існує ненульовий елемент, який належить тілу $\mathcal{X}$. Оскільки $n = r + 2t$, остання нерівність рівносильна тій, яка наведена в умові. □

Означення II.3.3. *Дискримінантом* $D(\mathbf{L})$ *повної ґратки* $\mathbf{L}$ у просторі $\mathfrak{G}$ зветься дискримінант деякої її бази.

Легко бачити, що цей дискримінант знов-таки не залежить від вибору бази в ґратці. Зокрема, це означення можна застосувати до геометричних зображень дробових ідеалів поля K, які за твердженням II.1.2 і наслідком I.3.11 є повними ґратками в $\mathfrak{G}$. З наслідку II.1.3 випливає, що для довільного дробового ідеалу дискримінант його геометричного зображення збігається з дискримінантом цього ідеалу, означеним у розділі I.7. Крім того, за наслідком II.1.4 дискримінант ґратки $\mathbf{L}$ пов'язаний з її фундаментальним об'ємом $V(\mathbf{L})$ формулою:

$$V(\mathbf{L}) = \frac{\sqrt{|D(\mathbf{L})|}}{2^t}. \tag{10}$$

Тому твердження II.3.2 можна переформулювати в наступному вигляді.

Твердження II.3.4. *Якщо*

$$C_1 C_2 \ldots C_{r+t} \geq (2/\pi)^t \sqrt{|D(\mathbf{L})|},$$

то тіло $\mathcal{X}(C_1, C_2, \ldots, C_{r+t})$ *містить ненульовий елемент з ґратки* $\mathbf{L}$.

Зважаючи на твердження II.1.1, маємо такий наслідок.

Наслідок II.3.5. *Кожна повна ґратка* $\mathbf{L}$ *простору* $\mathfrak{G}$ *містить ненульовий елемент* $\mathbf{a}$, *такий що* $|\mathrm{N}(\mathbf{a})| \leq (2/\pi)^t \cdot \sqrt{|D(\mathbf{L})|}$.

Виведемо звідси наступне твердження, з якого вже безпосередньо випливає теорема II.3.1 і яке є насправді деяким її уточненням.

Теорема II.3.6. *Кожен клас ідеалів поля* K *містить ідеал, норма якого не перебільшує* $(2/\pi)^t \sqrt{|D(\mathsf{K})|}$.

Доведення. Нехай $\mathbf{I}$ – довільний дробовий ідеал, $\mathrm{N} = \mathrm{N}(\mathbf{I})$. Тоді згідно з теоремою I.6.2 $\mathrm{N}(\mathbf{I}^{-1}) = \mathrm{N}^{-1}$. За твердженням I.7.7 тоді $D(\mathbf{I}^{-1}) = \mathrm{N}^{-2}D(\mathsf{K})$. Отже, у ґратці $\sigma(\mathbf{I}^{-1})$ міститься ненульовий елемент $\mathbf{a}$, такий що $|\mathrm{N}(\mathbf{a})| \le (2/\pi)^t \mathrm{N}^{-1}\sqrt{|D(\mathsf{K})|}$. Але $\mathbf{a} = \sigma(\gamma)$ для деякого $\gamma \in \mathbf{I}^{-1}$, причому $\mathrm{N}(\mathbf{a}) = \mathrm{N}(\gamma)$. Тоді $\mathbf{J} = \gamma\mathbf{I}$ – ідеал кільця A, який лежить у тому самому класі, що й дробовий ідеал $\mathbf{I}$, причому

$$\mathrm{N}(\mathbf{J}) = |\mathrm{N}(\gamma)|\mathrm{N}(\mathbf{I}) \le (2/\pi)^t \mathrm{N}^{-1}\sqrt{|D(\mathsf{K})|} \cdot \mathrm{N} = (2/\pi)^t\sqrt{|D(\mathsf{K})|}\,.$$

□

Для доведення теореми II.3.1 тепер досить нагадати, що кожен ідеал $\mathbf{I}$ містить ціле число $\mathrm{N} = \mathrm{N}(\mathbf{I})$, тобто ділить головний ідеал NA, а кожен ідеал має лише скінченну кількість дільників. Отже, кількість ідеалів з обмеженою нормою є скінченною. □

Виведемо з одержаних результатів ще наступний наслідок, відомий як “Теорема Мінковського про монодромію”.

Наслідок II.3.7. *Якщо* $\mathsf{K} \ne \mathbb{Q}$, *то* $|D(\mathsf{K})| > 1$, *а тому існують первинні числа, розгалужені в полі* K (див. теорему I.7.8).

Доведення. Якщо $t > 0$, необхідна нерівність одразу випливає з теореми II.3.6. Якщо ж $t = 0$, то $r = n > 1$ і результат витікає з наступного підсилення наслідку II.3.5 і теореми II.3.6.

Твердження II.3.8. *Припустимо, що* $r + t > 1$. *Тоді:*

(1) *Кожна повна ґратка* $\mathbf{L}$ *простору* $\mathfrak{G}$ *містить ненульовий елемент* $\mathbf{a}$, *такий що* $|\mathrm{N}(\mathbf{a})| < (2/\pi)^t\sqrt{|D(\mathbf{L})|}$.

(2) *Кожен клас ідеалів поля* K *містить ідеал кільця* A, *норма якого менша за* $(2/\pi)^t\sqrt{|D(\mathsf{K})|}$.

Доведення. Досить довести лише перше твердження: друге випливає з нього так само, як теорема II.3.6 випливає з наслідку II.3.5. Скористаймося міркуваннями і позначеннями з доведення наслідку II.2.5 у застосуванні до тіла $\mathcal{X} = \mathcal{X}(C_1, C_2, \ldots, C_{r+t})$, де $C_1C_2\ldots C_{r+t} = (2/\pi)^t\sqrt{|D(\mathsf{K})|}$. Нехай $\lambda(\mathbf{a}) = \sup\{\,\lambda \in \mathbb{R} \mid \lambda\mathbf{a} \in \mathcal{X}\,\}$ і $\lambda_0 = \min\{\,\lambda(\mathbf{a}) \mid \mathbf{a} \ne 0 \text{ і } \mathbf{a} \in \mathbf{L} \cap \rho\mathcal{X}\,\}$, де $\rho > 1$ – деяке фіксоване число. Відомо, що $\lambda_0 \ge 1$. Нам треба довести, що, можливо змінивши числа C_j (при збереженні їхнього добутку), можна добитися, щоб було $\lambda_0 > 1$. Припустимо, що $\lambda_0 = 1$. Множина

$$M = \{\,\mathbf{a} \in \mathbf{L} \mid \mathbf{a} \in \rho\mathcal{X} \text{ і } \mathbf{a} \notin \mathcal{X}\,\}$$

є скінченною, тому $\min\{\,\lambda(\mathbf{a}) \mid \mathbf{a} \in M\,\} = \lambda_1 < 1$. Виберемо число ρ_1 так, щоб $1 < \rho_1 < \lambda_1^{-1}$, зокрема, $\mathbf{L} \cap \rho_1\mathcal{X} = \mathbf{L} \cap \mathcal{X}$. Фіксуємо ненульовий елемент $\mathbf{b} \in \mathbf{L} \cap \mathcal{X}$. Тоді знайдеться номер j_1, для якого $|\mathrm{N}_{j_1}(\mathbf{b})| = C_{j_1}$. Оскільки $r + t > 1$, знайдеться номер $j_2 \ne j_1$. Означимо тоді числа C'_j рівностями:

$$C'_j = \begin{cases} C_{j_1}/\rho_1 & \text{при } j = j_1 \\ \rho_1 C_{j_2} & \text{при } j = j_2 \\ C_j & \text{при } j \ne j_1,\ j \ne j_2 \end{cases}$$

Тоді знову $C'_1C'_2\dots C'_{r+t} = (2/\pi)^t\sqrt{|D(\mathsf{K})|}$, але в тілі $\mathcal{X}' = \mathcal{X}(C'_1, C'_2, \dots, C'_{r+t})$ вже міститься *менше* елементів ґратки $\mathbf{L}$, ніж у тілі $\mathcal{X}$. Дійсно, $\mathcal{X}' \subseteq \rho_1\mathcal{X}$, тому $\mathbf{L}\cap\mathcal{X}' \subseteq \mathbf{L}\cap\mathcal{X}$. Але елемент $\mathbf{b}$ вже не належить $\mathbf{L}\cap\mathcal{X}'$, бо $|\mathrm{N}_{j_1}(\mathbf{b})| > C'_{j_1}$. Тепер доведення завершується очевидною індукцією за кількістю елементів у перетині $\mathbf{L}\cap\mathcal{X}$. $\square$

Вправи II.2. (1) Скориставшись результатом вправи II.1(1), довести, що:

(a) Кожна повна ґратка $\mathbf{L}$ простору $\mathfrak{G}$ містить такий ненульовий елемент $\mathbf{a}$, що $|\mathrm{N}(\mathbf{a})| \le M(r,t)\sqrt{|D(\mathbf{L})|}$, де

$$M(r,t) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t$$

(*константа Мінковського*).

(b) Кожен клас ідеалів поля K містить ідеал, норма якого не перебільшує $M(r,t)\sqrt{|D(\mathsf{K})|}$.

(c) Виведіть звідси теорему II.3.7, не вдаючись до твердження II.3.8.

(2) (a) Використовуючи *формулу Стірлінга*:

$$n! = \frac{n}{e}\sqrt{2\pi n}e^{\frac{\lambda}{12n}},$$

де $0 < \lambda < 1$, і попередню вправу, дайте наступну оцінку дискримінанта поля:

$$|D(\mathsf{K})| > \frac{1}{2\pi n}\left(\frac{\pi}{4}\right)^{2t} e^{\frac{2n-1}{6n}}.$$

(b) Виведіть звідси, що $|D(\mathsf{K})| \to \infty$ при $n \to \infty$.

(3) (a) Нехай $\mathcal{M}$ – тіло у просторі $\mathfrak{G}$, визначене при $r > 0$ нерівностями:

$$|\mathrm{N}_1(\mathbf{a})| < \sqrt{D+1},\ \ |\mathrm{N}_j(\mathbf{a})| < 1 \text{ при } j > 1,$$

а при $r = 0$ нерівностями:

$$|x_1| < 1,\ \ |y_1| < \sqrt{D},\ \ |\mathrm{N}_j(\mathbf{a})| < 1 \text{ при } j > 1,$$

де $D = |D(\mathsf{K})|$. Доведіть, що в цьому тілі міститься елемент $\sigma(\theta)$ для якогось ненульового $\theta \in \mathsf{A}$.

(b) Доведіть, що для елемента θ, побудованого вище, $\sigma_1(\theta) \ne \sigma_j(\theta)$ при $j > 1$, а якщо занурення σ_1 уявне (тоді $r = 0$), то також $\sigma_1(\theta) \ne \overline{\sigma}_1(\theta)$. Виведіть звідси, що θ – первісний елемент поля K, тобто $\mathsf{K} = \mathbb{Q}(\theta)$.

(c) Дайте оцінку коефіцієнтів мінімального многочлена елемента θ, побудованого вище, і виведіть з одержаних результатів *теорему Ерміта*:

Існує лише скінченна кількість полів K з даним значенням дискримінанта.

(4) Нехай $\mathsf{K} = \mathbb{Q}(\sqrt{-d})$, де $d > 0$ – уявне квадратичне поле, A – кільце цілих елементів поля K.
   (a) Використовуючи той факт, що рівняння $\mathrm{N}(\alpha) = n$ має лише скінченну кількість розв'язків $\alpha \in \mathsf{A}$, і теореми II.3.6 та I.7.11, розробіть ефективний спосіб обчислення числа класів ідеалів поля K.
   (b) Застосуйте розроблений метод до полів $\mathbb{Q}(\sqrt{-d})$ при $d = 5, 6, 10, 13, 15$.
   (c) Доведіть, що число класів ідеалів поля $\mathbb{Q}(\sqrt{-19})$ дорівнює 1, тобто кільце цілих елементів цього поля є кільцем головних ідеалів (Нагадаємо, що згідно зі вправою I.3 (4) воно не є евклідовим).

(Зараз доведено, що число класів ідеалів уявного квадратичного поля $\mathbb{Q}(\sqrt{-d})$ дорівнює 1 лише для 9 значень d, а саме: $1, 2, 3, 7, 11, 19, 43, 67, 163$).

II.4. Група одиниць

Іншим важливим застосуванням геометричних методів, зокрема леми Мінковського, є вивчення *групи одиниць* $\mathsf{U} = \mathsf{U}(\mathsf{K})$ поля K, тобто групи обертовних елементів кільця A. Зауважимо, що група одиниць, очевидно, збігається з ядром гомоморфізму $\phi_{\mathsf{K}} : \mathsf{K}^* \to \mathcal{I}(\mathsf{K})$, який зіставляє елементу γ головний дробовий ідеал $\gamma\mathsf{A}$. *Періодична частина* $\mathsf{E} = \mathsf{E}(\mathsf{K})$ групи одиниць – це група *коренів з одиниці*, які містяться в K (оскільки всі корені з одиниці – цілі алгебричні). Сформулюємо основну теорему про будову групи одиниць. Ми зберігаємо всі припущення і позначення стосовно поля K, введені в попередніх розділах.

Теорема II.4.1 (Теорема Діріхле про одиниці). *Група одиниць* $\mathsf{U} = \mathsf{U}(\mathsf{K})$ *є прямим добутком скінченної циклічної групи* $\mathsf{E} = \mathsf{E}(\mathsf{K})$ *та вільної абелевої групи рангу* $r + t - 1$, *де* r *і* t *відповідно кількість дійсних і уявних занурень поля* K.

Доведення. Нам буде потрібне, разом зі звичним вже геометричним зображенням алгебричних чисел, також їхнє *логарифмічне зображення* $\ell : \mathsf{K}^* \to \mathfrak{L} = \mathbb{R}^{r+t}$, яке переводить елемент γ у вектор

$$\ell(\gamma) = (\ell_1(\gamma), \ell_2(\gamma), \dots, \ell_{r+t}(\gamma)),$$

де $\ell_j(\gamma) = \ln|\mathrm{N}_j(\gamma)|$. Ўз твердження II.1.1 і наслідку II.1.3 безпосередньо випливає, що

$$\sum_{j=1}^{r+t} \ell_j(\gamma) = \ln|\mathrm{N}(\gamma)| \tag{11}$$

для довільного ненульового елемента $\gamma \in \mathsf{K}$. Якщо $\zeta \in \mathsf{U}$, то з рівності $1 = \mathrm{N}(1) = \mathrm{N}(\zeta)\mathrm{N}(\zeta^{-1})$ випливає, що $\mathrm{N}(\zeta) = \pm 1$, отже, логарифмічне зображення довільної одиниці ζ лежить у підпросторі $\mathfrak{L}_0$ простору

$\mathfrak{L}$, виділеному рівнянням $\sum_{j=1}^{r+t} z_j = 0$ (тут z_j позначають компоненти елемента $\mathbf{z} \in \mathfrak{L}$).

Якщо $\zeta \in \mathsf{E}$, тобто $\zeta^m = 1$ для деякого натурального m, то й $\sigma_j(\zeta)^m = 1$ для довільного індексу j, звідки $|\sigma_j(\zeta)| = 1$ і $\ell_j(\zeta) = 0$, тобто $\zeta \in \ker \ell$. Отже, $\mathsf{E} \subseteq \ker \ell$. Обернене включення випливає з наступного твердження.

Твердження II.4.2. *Для довільної підмножини $M \subset \mathfrak{L}$, обмеженої зверху, множина $\ell^{-1}(M) \cap \mathsf{A}$ є скінченною.*

Доведення. Нехай $z_j \le C$ $(j = 1, \dots, r+t)$ для довільного вектора $\mathbf{z} \in M$, де C – деяка додатна константа. Тоді, якщо $\ell(\gamma) \in M$, то $|\mathrm{N}_j(\gamma)| \le e^C$ $(j = 1, \dots, r+t)$. Але у довільній обмеженій підмножині простору $\mathfrak{G}$ лежить лише скінченна кількість зображень цілих алгебричних чисел. □

Отже, $\mathsf{E} = \ker \ell$ – скінченна підгрупа мультиплікативної групи поля K. Тому вона циклічна (див. [**K**, гл.9, §1, п.3]). Наступний факт є вирішальним у доведенні теореми.

Твердження II.4.3. *Підгрупа $\ell(\mathsf{U}) \simeq \mathsf{U}/\mathsf{E}$ є повною ґраткою у підпросторі $\mathfrak{L}_0$.*

Доведення. Перш за все встановимо ознаку того, що підгрупа векторного простору є ґраткою.

Твердження II.4.4. *Підгрупа $\mathbf{L}$ векторного простору $\mathbf{V}$ над полем дійсних чисел є ґраткою тоді й лише тоді, коли кожна обмежена підмножина простору $\mathbf{V}$ містить лише скінченну кількість векторів з підгрупи $\mathbf{L}$.*

Доведення. Необхідність цієї умови очевидна (і ми вже нею користувались). При доведенні достатності, очевидно, можна вважати, що підгрупа $\mathbf{L}$ не міститься в жодному власному підпросторі, тобто $\mathbf{L}$ містить якусь базу $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_m$ всього простору $\mathbf{V}$. У паралелепіпеді

$$\mathbf{P} = \left\{ \sum_{j=1}^{m} \lambda_j \mathbf{e}_j \;\mid\; 0 \le \lambda < 1 \right\}$$

лежить скінченна кількість векторів групи $\mathbf{L}$. Але кожен елемент простору $\mathbf{V}$ має вигляд $\mathbf{v}_0 + \mathbf{v}_1$, де $\mathbf{v}_0$ належить підгрупі $\mathbf{L}_0$ з базою $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_m$, а $\mathbf{v}_1$ – паралелепіпеду $\mathbf{P}$. Тому факторгрупа $\mathbf{L}/\mathbf{L}_0$ скінченна, а тоді група $\mathbf{L}$ є скінченнопородженою групою без скруту, тобто вільною абелевою групою рангу m. Очевидно, що її база $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_m$ складається з векторів, лінійно незалежних над $\mathbb{R}$, тобто $\mathbf{L}$ є ґраткою. □

Ўз тверджень II.4.2 і II.4.4 випливає, що $\ell(\mathsf{U})$ є ґраткою. Залишилось перевірити, що вона містить $r+t-1$ лінійно незалежних векторів (це – розмірність підпростору $\mathfrak{L}_0$). Для цього встановимо наступний факт.

Твердження II.4.5. *Для кожного номера* $j = 1, \dots, r+t$ *у підгрупі* $\ell(\mathsf{U})$ *знайдеться такий вектор* $\mathbf{z}$, *що* $z_j > 0$, *а* $z_k < 0$ *при всіх* $k \neq j$.

Доведення. Побудуємо спочатку для довільного ненульового елемента $\alpha \in \mathsf{A}$ такий ненульовий елемент $\beta \in \mathsf{A}$, що $|\mathrm{N}_k(\beta)| < |\mathrm{N}_k(\alpha)|$ для всіх номерів $k \neq j$ і $|\mathrm{N}(\beta)| \leq \Delta = (2/\pi)^t \sqrt{|D(\mathsf{K})|}$. Для цього виберемо для кожного такого номера k якесь додатне число $C_k < |\mathrm{N}_k(\alpha)|$ і покладемо $C_j = \Delta / \prod_{k \neq j} C_k$. Тоді за твердженням II.3.4 знайдеться ненульовий елемент $\beta \in \mathsf{A} \cap \mathcal{X}(C_1, C_2, \dots, C_{r+t})$, який і задовольняє необхідні нерівності.

Ітеруючи цю побудову, ми одержимо послідовність $\alpha_1, \alpha_2, \dots, \alpha_m, \dots$ елементів кільця A, для яких виконуються нерівності:

$$\begin{aligned} |\mathrm{N}_k(\alpha_m)| &> |\mathrm{N}_k(\alpha_{m+1})| \text{ для всіх } m \text{ і всіх } k \neq j; \\ |\mathrm{N}(\alpha_m)| &\leq \Delta \quad \text{для всіх } m. \end{aligned}$$

Зокрема, серед норм $\mathrm{N}(\alpha_m)$ є лише скінченна кількість різних. Тому серед побудованих чисел існує безліч з якоюсь однаковою нормою N. Залишивши лише їх, можна вважати, що $\mathrm{N}(\alpha_m) = \mathrm{N}$ для всіх номерів m. Оскільки факторкільце $\mathsf{A}/\mathrm{N}\mathsf{A}$ скінченне, знайдуться такі номери $l > m$, що $\alpha_l \equiv \alpha_m \pmod{\mathrm{N}}$, тобто $\alpha_l = \alpha_m + \beta\mathrm{N}$ для деякого $\beta \in \mathsf{A}$. Але за твердженням I.7.1 кожне число ділить свою норму. Звідси випливає, що числа $\zeta = \alpha_l/\alpha_m$ і $\zeta^{-1} = \alpha_m/\alpha_l$ обидва лежать в A, тобто $\zeta \in \mathsf{U}$. Покладемо $\mathbf{z} = \ell(\zeta)$. За побудовою $z_k < 0$ при $k \neq j$. Оскільки ж $\mathbf{z} \in \mathfrak{L}_0$, тоді $z_j > 0$. □

Тепер ми вже в змозі довести повноту ґратки $\ell(\mathsf{U})$. Побудуємо для кожного номера j такий вектор $\mathbf{z}_j = (z_{j1}, z_{j2}, \dots, z_{j,r+t}) \in \ell(\mathsf{U})$, що $z_{jk} < 0$ при $k \neq j$ і $z_{jj} > 0$. Позначимо $m = r + t - 1$ і розглянемо матрицю

$$Z = \begin{pmatrix} z_{1\,1} & z_{1\,2} & \cdots & z_{1m} \\ z_{2\,1} & z_{2\,2} & \cdots & z_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ z_{m1} & z_{m2} & \cdots & z_{mm} \end{pmatrix}$$

У ній сума елементів кожного рядка додатна, оскільки в сумі з *від'ємним* числом $z_{j,r+t}$ вона дорівнює 0. Діагональні елементи цієї матриці додатні, а всі інші від'ємні. Отже, Z є "матрицею з діагональною перевагою", тобто в ній $|z_{jj}| > \sum_{k \neq j} |z_{jk}|$. Але добре відомо, що така матриця завжди невироджена, тобто $\det Z \neq 0$ і вектори $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m$ лінійно незалежні. □

Завершують доведення теореми II.4.1 вже нескладні теоретико-групові міркування. Дійсно, ми маємо епіморфізм $\ell : \mathsf{U} \to \ell(\mathsf{U})$ з ядром E. Нехай $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m$, де $m = r + t - 1$ – база ґратки $\ell(\mathsf{U})$, причому $\mathbf{z}_j = \ell(\zeta_j)$. Тоді, очевидно, довільний елемент $\eta \in \mathsf{U}$ можна подати як добуток $\varepsilon \prod_{j=1}^m \zeta_j^{a_j}$, де a_j – ті цілі числа, для яких $\ell(\eta) = \sum_{j=1}^m \mathbf{z}_j$, а

$\varepsilon \in \mathsf{E}$. З іншого боку, якщо $\prod_{j=1}^m \zeta_j^{b_j} \in \mathsf{E}$ для деяких цілих b_j, то, застосувавши відображення ℓ, матимемо, що $\sum_{j=1}^m b_j \mathbf{z}_j = 0$, звідки $b_j = 0$ для всіх номерів j. Отже, U є прямим добутком підгрупи E і підгрупи U_0, породженої елементами $\zeta_1, \zeta_2, \dots, \zeta_m$, причому останні утворюють базу цієї підгрупи. □

Наслідок II.4.6. *Група одиниць є скінченною тоді й лише тоді, коли або* $\mathsf{K} = \mathbb{Q}$, *або* K – *уявне квадратичне розширення* $\mathbb{Q}$, *тобто* $\mathsf{K} = \mathbb{Q}(\sqrt{d})$ *для деякого цілого* $d < 0$.

Теорема Діріхле про одиниці означає, що в групі одиниць існують такі елементи $\zeta_1, \zeta_2, \dots, \zeta_m$, де $m = r + t - 1$, що кожна одиниця однозначно подається у вигляді $\varepsilon \prod_{j=1}^m \zeta_j^{a_j}$ для деякого кореня з одиниці ε і деяких цілих чисел a_j. Одиниці $\zeta_1, \zeta_2, \dots, \zeta_m$ звуться *основними одиницями поля* K.

Будемо розглядати логарифмічний простір $\mathfrak{L}$ як евклідів, вважаючи, що звичайні координати в ньому є координатами в ортонормованій базі. Тоді ми можемо говорити про об'єми паралелепіпедів у цьому просторі.

Твердження II.4.7. (1) *Одиниці* $\zeta_1, \zeta_2, \dots, \zeta_m$, *де* $m = r + t - 1$, *є основними одиницями поля* K *тоді й лише тоді, коли їхні логарифмічні зображення утворюють базу ґратки* $\ell(\mathsf{U})$.

(2) *Фундаментальний об'єм ґратки* $\ell(\mathsf{U})$ *дорівнює* $\mathrm{R}\sqrt{r+t}$, *де* $\mathrm{R} = \mathrm{R}(\mathsf{K})$ – *модуль якогось мінору порядку* m *матриці розміру* $m \times (m+1)$, *укладеної з координат* $\ell_{kj} = \ell_j(\zeta_k)$, *де* $\zeta_1, \zeta_2, \dots, \zeta_m$ – *основні одиниці поля* K. (Зокрема, всі ці мінори є рівними за модулем і R не залежить від вибору основних одиниць).

Число $\mathrm{R} = \mathrm{R}(\mathsf{K})$ зветься *регулятором* поля K.

Доведення. Перше твердження є очевидним. Для доведення другого зауважимо, що вектор $\mathbf{v}$, усі координати якого дорівнюють $1/\sqrt{r+t}$, ортогональний до підпростору $\mathfrak{L}_0$ і має довжину 1. Тому фундаментальний об'єм ґратки $\ell(\mathsf{U})$ дорівнює об'єму $(m+1)$-вимірного паралелепіпеда, утвореного векторами $\mathbf{v}, \ell(\zeta_1), \dots, \ell(\zeta_m)$, тобто модулю визначника, складеного з координат цих векторів. Але з того, що сума координат кожного з векторів $\ell(\zeta_k)$ дорівнює 0, легко випливає, що цей визначник дорівнює $\mathrm{R}\sqrt{r+t}$. □

Вправи II.3. (1) Доведіть, що мультиплікативна група скінченного розширення поля раціональних чисел є прямим добутком скінченної циклічної групи і вільної абелевої групи зліченого рангу.

(2) Нехай A – кільце цілих елементів деякого поля K алгебричних чисел, A' – його підкільце, таке що індекс $(\mathsf{A} : \mathsf{A}')$ є скінченним. Довести, що теорема Діріхле про одиниці залишається справедливою і для групи обертовних елементів кільця A'.

(3) Нехай d – додатне ціле число, яке не є повним квадратом. Скористайтеся теоремою Діріхле для доведення наступних результатів:
   (a) *Рівняння Пелля* $x^2 - dy^2 = 1$ *має безліч розв'язків у цілих числах.*
   (b) *Серед цілочисельних розв'язків цього рівняння існує такий розв'язок* (a_0, b_0) *, з яким усі інші розв'язки* (a, b) *пов'язані формулою:* $a + b\sqrt{d} = \pm(a_0 + b_0\sqrt{d})^k$ *для деякого цілого* k *.*

Розділ III

Аналітичні методи

III.1. Ряди Діріхле

У застосуванні аналітичних методів у теорії чисел виключно важливу роль відіграють так звані *ряди Діріхле*.

Означення III.1.1. Нехай $f(n)$ – деяка комплексна функція натурального аргументу. *Рядом Діріхле*, що відповідає функції $f(n)$, зветься ряд

$$L(f,s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\,.$$

Зокрема, якщо $f(n)=1$ для всіх n, маємо добре відому *дзета-функцію Рімана*:

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\,, \tag{12}$$

з якої, власне, і почалась аналітична теорія чисел.

Встановимо наступні факти щодо збіжності рядів Діріхле та властивостей їхніх сум на границі області збіжності.

Теорема III.1.2. *Нехай $f(x)$ – деяка комплексна функція натурального аргументу, $L(f,s)$ – відповідний ряд Діріхле. Позначимо $F(x)=\sum_{n\le x}f(n)$. Припустимо, що*

$$\lim_{x\to\infty}\frac{F(x)}{x^m}=c\,,$$

Тоді:

(1) *Ряд $L(f,s)$ збігається при дійсних $s>m$, причому збігається рівномірно при $s\ge s_0$ для довільного $s_0>m$.*
(2) $\lim_{s\to m+0}(s-m)L(f,s)=mc$.

Доведення. Перепишемо ряд $L(f,s)$ у вигляді:

$$\begin{aligned} L(f,s) &= \sum_{n=1}^{\infty} F(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right) = s\sum_{n=1}^{\infty}\int_n^{n+1}\frac{F(x)}{x^{s+1}}dx \\ &= cs\sum_{n=1}^{\infty}\int_n^{n+1}\frac{x^m}{x^{s+1}}dx + s\sum_{n=1}^{\infty}\int_n^{n+1}\frac{g(x)x^m}{x^{s+1}}dx \\ &= cs\int_1^{\infty}\frac{dx}{x^{s-m+1}} + s\int_1^{\infty}\frac{g(x)}{x^{s-m+1}}dx\,, \end{aligned}$$

де $g(x)\to 0$, коли $x\to\infty$. Обидва інтеграли в останній сумі збігаються при $s>m$ і рівномірно збігаються при $s\ge s_0$ для довільного $s_0>m$. Більш того, функція $g(x)$ обмежена: $|g(x)|<A$ для деякої константи A, і для довільного $\varepsilon>0$ існує таке $B>1$, що $|g(x)|<\varepsilon$ при $x>B$. Перепишемо другий інтеграл у вигляді:

$$I_2=\int_1^{\infty}\frac{g(x)}{x^{s-m+1}}dx=\int_1^{B}\frac{g(x)}{x^{s-m+1}}dx+\int_B^{\infty}\frac{g(x)}{x^{s-m+1}}dx\,.$$

Тоді

$$|I_2|<\frac{A}{s-m}\left(1-\frac{1}{B^{s-m}}\right)+\frac{\varepsilon}{(s-m)B^{s-m}}\,,$$

звідки

$$|(s-m)I_2|<A\left(1-\frac{1}{B^{s-m}}\right)+\frac{\varepsilon}{B^{s-m}}\,.$$

Тут перший доданок є нескінченно малою, коли $s\to m+0$, а другий не перебільшує ε/m. Отже, для довільного $\varepsilon>0$ маємо:

$$(s-m)L(f,s)=cs+u(s)+sv(s)\,,$$

де $u(s)\to 0$, коли $s\to m+0$, а $|v(s)|<\varepsilon$. Звідси, очевидно, випливає твердження теореми. □

Зауваження III.1.3. Оскільки всі функції, які зустрічаються в рядах та інтегралах з наведеного вище доведення, є *аналітичними функціями* від змінної s, то насправді за умов теореми III.1.2 ряд Діріхле також являє собою *аналітичну функцію* аргументу s при довільних комплексних значеннях s, таких що $\Re s>m$.

Зокрема, для дзета-функції Рімана $F(x)=[x]$ (ціла частина числа x), звідки маємо такий (добре відомий) наслідок.

Наслідок III.1.4. (1) *Ряд (12) збігається при всіх дійсних $s>1$, причому на множині $s\ge s_0$, де $s_0>1$ – деяке фіксоване число, він збігається рівномірно.*

(2) $\lim_{s\to 1+0}(s-1)\zeta(s)=1$,

III.2. Рівномірний розподіл ідеалів за класами

Мета цього розділу – довести, що в деякому розумінні ідеали поля алгебричних чисел *рівномірно розподілені* за класами. Звичайно, оскільки кількість ідеалів у кожному класі Є нескінченною, точне твердження потребує деякої технічної підготовки.

Фіксуємо надалі деяке скінченне розширення K поля раціональних чисел ступеня $k = (\mathsf{K} : \mathbb{Q})$, яке має r дійсних і t уявних занурень у поле комплексних чисел ($k = r + 2t$). Будемо використовувати всі терміни і позначення, які було введено в попередніх розділах щодо геометричного і логарифмічного зображень елементів поля K та його кільця цілих елементів A. Зокрема позначимо $\Delta = \sqrt{|D(\mathsf{K})|}$, R – регулятор поля K і w – порядок групи E коренів з одиниці, які лежать у полі K. Точний сенс слів "ідеали рівномірно розподілені за класами" міститься у наступній теоремі (та наслідку з неї).

Теорема III.2.1. *Нехай $C \in \mathcal{C}(\mathsf{K})$ – деякий клас ідеалів поля K. Позначимо $Z(C, x)$, де x – додатне дійсне число, кількість таких ідеалів $\mathbf{I} \subseteq \mathsf{A}$, які належать класу C і для яких $\mathrm{N}(\mathbf{I}) \le x$. Тоді*

$$\lim_{x\to\infty} \frac{Z(C,x)}{x} = \frac{2^{r+t}\pi^t \mathrm{R}}{w\Delta}.$$

Наслідок III.2.2. *Позначимо $Z(x)$, де x – додатне дійсне число, кількість ідеалів $\mathbf{I} \subseteq \mathsf{A}$, таких що $\mathrm{N}(\mathbf{I}) \le x$. Тоді*

$$\lim_{x\to\infty} \frac{Z(x)}{x} = \frac{2^{r+t}\pi^t \mathrm{R}}{w\Delta}\mathrm{h},$$

де h – число класів ідеалів поля K.

Доведення. Фіксуємо деякий ідеал $\mathbf{J}$ із класу C. Тоді довільний ідеал $\mathbf{I}$ з того ж класу має вигляд $\gamma\mathbf{J}$, де $\gamma \in \mathbf{J}^{-1}$. При цьому $\mathrm{N}(\mathbf{I}) = |\mathrm{N}(\gamma)|\mathrm{N}(\mathbf{J})$ і, крім того, $\gamma\mathbf{J} = \gamma'\mathbf{J}$ тоді й лише тоді, коли числа γ і γ' *асоційовані*, тобто $\gamma' = \zeta\gamma$, де $\zeta \in \mathsf{U}$ – одиниця поля K. Отже, число $Z(C, x)$ дорівнює кількості попарно неасоційованих чисел γ з дробового ідеалу $\mathbf{J}^{-1}$, для яких $|\mathrm{N}(\gamma)| \le x\mathrm{N}$, де $\mathrm{N} = \mathrm{N}(\mathbf{J}^{-1})$.

Скористаймося логарифмічним зображенням та теоремою про одиниці. Саме, нехай $\zeta_1, \zeta_2, \dots, \zeta_m$, де $m = r + t - 1$ – основні одиниці поля K, $\mathbf{z}_j = \ell(\zeta_j)$ і

$$\mathbf{e} = (\underbrace{1, \dots, 1}_{r}, \underbrace{2, \dots, 2}_{t}).$$

Вектори $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m, \mathbf{e}$ утворюють базу логарифмічного простору $\mathfrak{L}$. Тому, якщо $\mathbf{v}$ – довільний елемент простору $\mathfrak{L}$, його можна однозначно подати у вигляді $\mathbf{z} + b\mathbf{e} + \sum_{j=1}^{m} \lambda_j \mathbf{z}_j$, де $\lambda_1, \lambda_2, \dots, \lambda_m$ і b – дійсні числа, причому $0 \le \lambda_j < 1$ для всіх j, а $\mathbf{z} = \ell(\zeta)$ для деякої одиниці ζ. Звідси випливає, що в кожному класі асоційованих елементів поля K

міститься такий елемент γ, що

$$\ell(\gamma) = b\mathbf{e} + \sum_{j=1}^{m} \lambda_j \mathbf{z}_j\,, \text{ де } 0 \le \lambda_j < 1 \text{ для всіх } j\,. \tag{13}$$

Елемент γ з таким логарифмічним зображенням назвемо *зведеним*. Згадаймо також, що $\ell(\gamma) = \ell(\gamma')$ тоді й лише тоді, коли $\gamma' = \varepsilon\gamma$ для деякого кореня з одиниці ε. Інакше кажучи, в кожному класі асоційованих елементів містяться рівно w зведених елементів. Нарешті, оскільки усі вектори $\mathbf{z}_j$ належать підпростору $\mathfrak{L}_0$, ми маЄмо, що для елемента $\gamma \in \mathsf{K}$ з логарифмічним зображенням вигляду (13) $|\mathrm{N}(\gamma)| = e^{kb}$. Зокрема, обмеження $|\mathrm{N}(\gamma)| \le \tau$, де $\tau > 0$ – дійсна константа, рівносильне для зведеного елемента нерівності $kb \le \ln\tau$.

Розглянемо у просторі $\mathfrak{G}$ тіло $\mathcal{M}(\tau)$, яке складаЄться з усіх таких точок $\mathbf{a} = (a_1, a_2, \dots, a_{r+t})$, у яких $a_j \ne 0$ для всіх номерів j і вектор

$$\ell(\mathbf{a}) = (\ell_1(a_1), \ell_2(a_2), \dots, \ell_{r+t}(a_{r+t}))$$

маЄ вигляд $\ell(\mathbf{a}) = b\mathbf{e} + \sum_{j=1}^{m} \lambda_j \mathbf{z}_j$, де $0 \le \lambda_j < 1$ для всіх j і $|\mathrm{N}(\mathbf{a})| = e^k b \le \tau$. Зі сказаного вище виплива Є, що кількість точок ґратки $\mathbf{L} = \sigma(\mathbf{J}^{-1})$ (геометричного зображення ідеалу $\mathbf{J}^{-1}$), які належать тілу $\mathcal{M}(x\mathrm{N})$, дорівнюЄ $wZ(C,x)$. Крім того, якщо $\mathbf{a} \in \mathcal{M}(\tau)$, то для довільного додатнього числа ξ маЄмо: $\ell(\xi\mathbf{a}) = \ell(\mathbf{a}) + \ln\xi\,\mathbf{e}$, звідки $\xi\mathbf{a} \in \mathcal{M}(\xi^k\tau)$. Інакше кажучи, $\xi\mathcal{M}(\tau) = \mathcal{M}(\xi^k\tau)$. Зокрема, якщо покласти $\xi^k = x\mathrm{N}$, одержимо, що $\mathcal{M}(x\mathrm{N}) = \xi\mathcal{M}$, де $\mathcal{M} = \mathcal{M}(1)$. Отже, $wZ(C,x)$ дорівнюЄ кількості $\nu(\xi)$ точок ґратки $\mathbf{L}$ у тілі $\xi\mathcal{M}$.

Позначимо v об'Єм тіла $\mathcal{M}$ і V – фундаментальний об'Єм ґратки $\mathbf{L}$. Розглянемо ґратку $\mathbf{L}_\xi = \xi^{-1}\mathbf{L}$. °ї фундаментальний об'Єм дорівнює $\xi^{-k}V$, а кількість точок ґратки $\mathbf{L}_\xi$, які належать тілу $\mathcal{M}$, очевидно, дорівнює кількості точок ґратки $\mathbf{L}$, які належать тілу $\xi\mathcal{M}$. Але фактично з означення об'Ємів виплива Є, що

$$v = \lim_{\xi\to\infty} \nu(\xi) V_\xi\,, \tag{14}$$

де $V_\xi = \xi^{-k}V$ – фундаментальний об'Єм ґратки $\xi^{-1}\mathbf{L}$.

Обчислимо об'Єм v. За означенням,

$$v = \int_{\mathcal{M}} dx_1 dx_2 \dots dx_{r+t} dy_{r+1} \dots dy_{r+t}\,,$$

де $x_1, x_2, \dots, x_{r+t}, y_{r+1}, \dots, y_{r+t}$ – "стандартні" координати у просторі $\mathfrak{G}$, тобто, точка простору $\mathfrak{G}$ записуЄться у вигляді

$$\mathbf{a} = (x_1, x_2, \dots, x_r, x_{r+1} + iy_{r+1}, \dots, x_{r+t} + iy_{r+t})\,.$$

Замінимо для уявних компонент декартові координати x_j, y_j $(j > r)$ на полярні координати ρ_j, φ_j, де $x_j = \rho_j\cos\varphi_j$, $y_j = \rho_j\sin\varphi_j$. Якобіан ціЄї заміни дорівнюЄ $\rho_{r+1}\dots\rho_{r+t}$, отже,

$$v = \int_{\mathcal{M}} \rho_{r+1}\dots\rho_{r+t} dx_1 \dots dx_r d\rho_{r+1} \dots d\rho_{r+t} d\varphi_1 \dots d\varphi_t\,.$$

Зауважимо, що в означенні тіла $\mathcal{M}$ обмеження накладаються лише на *модулі* координат, тобто на $|x_1|,\dots,|x_r|$ і $\rho_{r+1},\dots,\rho_{r+t}$. Тому інтегрування за кожним $d\varphi_j$ даЄ внесок 2π, що разом становить $(2\pi)^t$. Крім того, інтегрування можна обмежити на ту частину тіла $\mathcal{M}$, де $x_j>0$ для всіх $j=1,\dots r$, винесши множник 2^r. Отже, позначивши $\rho_j=|x_j|$ при $j=1,\dots r$ і враховуючи, що $\rho d\rho = d\rho^2/2$, маЄмо:

$$\begin{aligned} v &= 2^{r+t}\pi^t \int_{\widetilde{\mathcal{M}}} \rho_{r+1}\rho_{r+2}\dots\rho_{r+t} d\rho_1 d\rho_2 \dots d\rho_{r+t} = \\ &= 2^r\pi^t \int_{\widetilde{\mathcal{M}}} d\rho_1\dots d\rho_r d\rho_{r+1}^2\dots d\rho_{r+t}^2 , \end{aligned}$$

де $\widetilde{\mathcal{M}}$ – тіло у просторі $\mathbb{R}^{r+t}$ (з координатами $\rho_1,\rho_2\dots\rho_t$), що складаЄться з усіх точок $\mathbf{r}=(\rho_1,\rho_2,\dots,\rho_{r+t})$, які задовольняють вимоги:

- $\rho_j>0$ для всіх $j=1,\dots,r+t$;
- вектор $\ell(\mathbf{r})=(\ln\rho_1,\dots,\ln\rho_r,\ln\rho_{r+1}^2,\dots,\ln\rho_{r+t}^2)$ можна подати у "зведеному вигляді" (13) з $b\le 0$.
  (Звичайно, ми розглядаЄмо $\ell(\rho)$ як елемент логарифмічного простору $\mathfrak{L}$).

Перейдемо тепер до логарифмічного зображення заміною

$$z_j=\begin{cases} \ln\rho_j & \text{при } j=1,\dots r \\ \ln\rho_j^2 & \text{при } j=r+1,\dots,r+t \end{cases}$$

Тоді одержимо:

$$v=2^r\pi^t\int_{\ell(\mathcal{M})} e^{z_1+z_2+\dots+z_{r+t}} dz_1 dz_2\dots dz_{r+t} ,$$

де $\ell(\mathcal{M})$ – образ тіла $\widetilde{\mathcal{M}}$ у логарифмічному просторі. З означення випливаЄ, що тіло $\ell(\mathcal{M})$ складаЄться з усіх тих векторів $\mathbf{v}$, які можна подати у "зведеному" вигляді: $\mathbf{v}=b\mathbf{e}+\sum_{j=1}^m\lambda_j\mathbf{z}_j$, де $0\le\lambda_j<1$ для всіх j, а $b\le 0$. Зауважимо, що число kb збігаЄться із сумою координат $\sum_{j=1}^{r+t} z_j$ вектора $\mathbf{v}$. Перейдемо, нарешті, в логарифмічному просторі до координат $b,\lambda_1,\lambda_2,\dots,\lambda_m$ ("координат у базі $\mathbf{e},\mathbf{z}_1,\mathbf{z}_2,\dots,\mathbf{z}_m$"). Якобіан J такої заміни дорівнюЄ визначнику, складеному з координат нової бази, тобто

$$J=\begin{vmatrix} 1 & \dots & 1 & 2 & \dots & 2 \\ \ell_{11} & \dots & \ell_{1r} & \ell_{1,r+1} & \dots & \ell_{1,r+t} \\ \ell_{21} & \dots & \ell_{2r} & \ell_{2,r+1} & \dots & \ell_{2,r+t} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \ell_{m1} & \dots & \ell_{mr} & \ell_{m,r+1} & \dots & \ell_{m,r+t} \end{vmatrix} ,$$

де $\ell_{kj}=\ell_j(\zeta_k)$. Додавши всі стовпчики цього визначника до останнього і враховуючи, що всі рядки його, крім першого, належать підпростору

$\mathfrak{L}_0$, бачимо, що, згідно з означенням регулятора, $|J| = k\mathrm{R}$. Звідси

$$v = 2^r \pi^t k\mathrm{R} \int_0^1 \dots \int_0^1 \int_{-\infty}^0 e^{kb} d\lambda_1 \dots d\lambda_m db = 2^r \pi^t \mathrm{R}\,.$$

Згадаймо тепер вираз для фундаментального об'Єму V ґратки $\mathbf{L} = \sigma(\mathbf{J}^{-1})$ (див. формулу (10) і твердження I.7.7):

$$V = \frac{\sqrt{|D(\mathbf{L})}}{2^t} = \frac{\mathrm{N}\Delta}{2^t}\,.$$

Тому формула (14) переписуЄться у вигляді:

$$\lim_{\xi\to\infty} \frac{\nu(\xi)}{\xi^k} = \frac{2^{r+t}\pi^t \mathrm{R}}{\mathrm{N}\Delta}\,.$$

Зробивши в останній формулі заміну $\xi^k = x\mathrm{N}$ і згадавши, що кількість точок ґратки $\mathbf{L}$ у тілі $\mathcal{M}(x\mathrm{N}) = \xi\mathcal{M}$ дорівнюЄ $wZ(C,x)$, ми й одержуЄмо:

$$\lim_{x\to\infty} \frac{Z(C,x)}{x} = \frac{2^{r+t}\pi^t \mathrm{R}}{w\Delta}\,.$$

□

III.3. Дзета-функції Дедекінда

Введемо зараз "головний персонаж" ціЄї глави – *дзета-функцію Дедекінда* деякого поля алгебричних чисел K. Ми зберігаЄмо припущення і позначення попереднього розділу.

Означення III.3.1. *Дзета-функцією поля* K зветься ряд Діріхле

$$\zeta_{\mathsf{K}}(s) = \sum_n \frac{\nu(n)}{n^s}\,,$$

де $\nu(n)$ позначаЄ кількість таких ідеалів $\mathbf{I} \subseteq \mathsf{A}$, що $\mathrm{N}(\mathbf{I}) = n$.

Оскільки $\sum_{n\le x} \nu(n) = Z(x)$, то із загальних властивостей рядів Діріхле (теорема III.1.2) та теореми про граничну поведінку функції Z (наслідок III.2.2) безпосередньо випливають наступні властивості дзета-функції.

Наслідок III.3.2. (1) *Ряд Діріхле* $\zeta_{\mathsf{K}}(s)$ *збігаЄться при дійсних* $s > 1$, *причому на множині* $s \ge s_0$ *для довільного* $s_0 > 1$ *він збігаЄться рівномірно.*

(2) $\lim_{s\to 1+0}(s-1)\zeta_{\mathsf{K}}(s) = \kappa\mathrm{h}$, *де*

$$\kappa = \frac{2^{r+t}\pi^t \mathrm{R}}{w\Delta}\,,$$

а h – *число класів ідеалів поля* K.

Зауважимо, що дзета-функцію Дедекінда часто зручніше записувати у вигляді:

$$\zeta_{\mathsf{K}}(s) = \sum_{\mathbf{I}} \frac{1}{\mathrm{N}(\mathbf{I})^s}\,,$$

де $\mathbf{I}$ пробігає всі ідеали кільця A. Важливою властивістю дзета-функції, яка дає можливість реально застосовувати граничну формулу з наслідку III.3.2, є те, що її можна обчислювати "локально". Це пов'язано з так званим *Ойлеровим добутком*.

Теорема III.3.3. *Для довільного $s > 1$ має місце рівність:*

$$\zeta_{\mathsf{K}}(s) = \prod_{\mathfrak{p}\in\mathcal{P}} \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}}\,,$$

де $\mathcal{P}$ – множина всіх первинних ідеалів кільця A (зокрема, останній нескінченний добуток збігається).

Доведення. Збіжність нескінченного добутку випливає, як добре відомо, зі збіжності ряду $\sum_{\mathfrak{p}} 1/\mathrm{N}(\mathfrak{p})^s$, який збігається принаймні не гірше, ніж ряд для дзета-функції. Фіксуємо тепер довільне натуральне число N і розглянемо частковий добуток

$$\Pi_N = \prod_{\mathrm{N}(\mathfrak{p})\le N} \frac{1}{1-\frac{1}{\mathrm{N}(\mathfrak{p})^s}}$$

і суму

$$\Sigma_N = \sum_{\mathrm{N}(\mathbf{I})\le N} \frac{1}{\mathrm{N}(\mathbf{I})^s}\,,$$

в яких $\mathbf{I}$ пробігає всі, а $\mathfrak{p}$ – первинні ідеали кільця A. Перетворимо Π_N у такий спосіб:

$$\begin{aligned}\Pi_N &= \prod_{\mathrm{N}(\mathfrak{p})\le N}\left(1+\frac{1}{\mathrm{N}(\mathfrak{p})^s}+\frac{1}{\mathrm{N}(\mathfrak{p})^{2s}}+\dots\right) = \\ &= \sum_{\mathrm{N}(\mathfrak{p}_k)\le N} \frac{1}{\mathrm{N}(\mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\dots\mathfrak{p}_l^{m_l})^s}\,,\end{aligned}$$

де остання сума береться за всіма можливими наборами первинних ідеалів $\mathfrak{p}_1,\mathfrak{p}_2,\dots,\mathfrak{p}_l$ і довільними показниками m_k. Але з однозначності розкладу на первинні множники випливає, що серед добутків $\mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\dots\mathfrak{p}_l^{m_l}$ зустрічаються (і кожен по одному разу) ті й тільки ті ідеали, усі первинні дільники яких мають норму не більшу, ніж N. Позначимо множину таких ідеалів $\mathcal{I}_N$. Зокрема, серед них містяться *всі* ідеали, з нормою не більшою, ніж N. Отже, маємо рівність:

$$\Pi_N = \Sigma_N + \Sigma_N^*\,,$$

де

$$\Sigma_N^* = \sum_{\substack{\mathbf{I} \in \mathcal{I}_N \\ \mathrm{N}(\mathbf{I}) > N}} \frac{1}{\mathrm{N}(\mathbf{I})^s},$$

Але Σ_N^* не перебільшує залишка, який утвориться, якщо від ряду Діріхле $\zeta_{\mathsf{K}}(s)$ залишити лише доданки з номерами, більшими за N. Отже, $\Sigma_N^* \to 0$, коли $N \to \infty$. Оскільки за означенням $\Sigma_N \to \zeta_{\mathsf{K}}(s)$, коли $N \to \infty$, звідси випливає твердження теореми. □

Зокрема, для звичайної дзета-функції Рімана одержуємо класичний результат Ойлера:

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

де p пробігає первинні натуральні числа.

III.4. Існування первинних ідеалів першого ступеня

Скористаймося розкладом дзета-функції в Ойлерів добуток для того, щоб одержати інформацію про розподіл первинних ідеалів. Перш за все, враховуючи граничну поведінку дзета-функції при $s \to 1$, маємо наступний наслідок.

Наслідок III.4.1. *При* $s \to 1 + 0$

$$\ln \zeta_{\mathsf{K}}(s) = \ln \frac{1}{s-1} + O(1).$$

Звідси виведемо такий результат, вперше відкритий для звичайних цілих чисел ще Ойлером.

Теорема III.4.2. *При* $s \to 1 + 0$

$$\sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{\mathrm{N}(\mathfrak{p})^s} = \ln \frac{1}{s-1} + O(1).$$

Доведення. Безпосередньо прологарифмувавши Ойлерів добуток, одержимо:

$$\begin{aligned} \ln \zeta_{\mathsf{K}}(s) &= -\sum_{\mathfrak{p} \in \mathcal{P}} \ln \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}\right) = \sum_{\mathfrak{p} \in \mathcal{P}} \sum_{k=1}^{\infty} \frac{1}{k \mathrm{N}(\mathfrak{p})^{ks}} = \\ &= \sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{\mathrm{N}(\mathfrak{p})^s} + \sum_{\mathfrak{p} \in \mathcal{P}} \sum_{k=2}^{\infty} \frac{1}{k \mathrm{N}(\mathfrak{p})^{ks}}. \end{aligned}$$

Враховуючи, що $\mathrm{N}(\mathfrak{p}) \geq 2$, оцінимо члени останньої суми:

$$\sum_{k=2}^{\infty} \frac{1}{k \mathrm{N}(\mathfrak{p})^{ks}} < \frac{1}{\mathrm{N}(\mathfrak{p})^{2s}} \sum_{k=0}^{\infty} \frac{1}{2^s} < \frac{2}{\mathrm{N}(\mathfrak{p})^{2s}}.$$

Отже, оскільки ряд для дзета-функції збігаЄться при $s > 1$, остання сума збігаЄться при $s > 1/2$, тобто залишаЄться обмеженою при $s \to 1$. □

НагадаЄмо, що первинний ідеал $\mathfrak{p}$ зветься *первинним ідеалом першого ступеня*, якщо $\mathrm{N}(\mathfrak{p})$ – первинне натуральне число. В іншому разі $\mathrm{N}(\mathfrak{p}) = p^f$ для деякого простого p і $k \le 2$. Позначимо $\mathcal{P}_1$ множину всіх первинних ідеалів першого ступеня і $\mathcal{P}' = \mathcal{P} \setminus \mathcal{P}_1$. Тоді ряд

$$\sum_{\mathfrak{p}\in\mathcal{P}'} \frac{1}{\mathrm{N}(\mathfrak{p})^s},$$

очевидно, збігаЄться вже при $s > 1/2$, звідки одержуЄмо ще такий наслідок.

Наслідок III.4.3. *При* $s \to 1+0$

$$\sum_{\mathfrak{p}\in\mathcal{P}_1} \frac{1}{\mathrm{N}(\mathfrak{p})^s} = \ln\frac{1}{s-1} + O(1).$$

Зокрема, у кожному полі алгебричних чисел існуЄ безліч первинних ідеалів першого ступеня.

III.5. Поля поділу кола

У цьому розділі ми застосуЄмо загальну техніку до вивчення спеціального класу полів – полів поділу кола. НагадаЄмо, що *поле поділу кола на* m *частин* – це поле $\mathsf{K} = \mathbb{Q}(\varepsilon)$, де ε – первісний корінь ступеня m з одиниці, тобто $\varepsilon^m = 1$ і $\varepsilon^l \ne 1$ для довільного натурального $l < m$. Звичайно, ε Є цілим алгебричним числом. Тому кільце A цілих алгебричних елементів поля K містить підкільце $\mathbb{Z}[\varepsilon]$, яке складаЄться з усіх многочленів від ε з цілими коефіцієнтами.

Позначимо $\Phi_m(x)$ *многочлен поділу кола на* m *частин*, тобто многочлен зі старшим коефіцієнтом 1, коренями якого Є всі первісні корені ступеня m з одиниці. З очевидної рівності

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

індукцією за m легко вивести, що многочлен $\Phi_m(x)$ маЄ цілі коефіцієнти. За означенням, $\deg\Phi_m(x) = \varphi(m)$, де $\varphi(m)$ – *функція Ойлера*, тобто кількість класів лишків за модулем m, співпервинних з m. Тому $k = (\mathsf{K} : \mathbb{Q}) \le \varphi(m)$. Числа $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{k-1}$ лінійно незалежні над полем раціональних чисел (вони утворюють базу поля K). Тому вони утворюють також базу адитивної групи кільця $\mathbb{Z}[\varepsilon]$. Оскільки ранги групи A та її підгрупи $\mathbb{Z}[\varepsilon]$ рівні, індекс $\delta = (\mathsf{A} : \mathbb{Z}[\varepsilon])$ Є скінченним.

Твердження III.5.1. *Припустимо, що первинне число* p *не ділить* $m\delta$. *Тоді,для довільного елемента* $\alpha \in \mathsf{A}$:

(1) *ІснуЄ елемент* $\beta \in \mathbb{Z}[\varepsilon]$, *такий що* $\alpha \equiv \beta \pmod{p}$.

(2) $\alpha^{p^f} \equiv \alpha \,(\mathrm{mod}\, p)$, *де* f *– найменший показник, для якого* $p^f \equiv 1 \,(\mathrm{mod}\, m)$ *(тобто порядок залишку числа* p *у мультиплікативній групі лишків за модулем* m*, співпервинних з* m*).*

Доведення. *1)* Оскільки $\delta\alpha \in \mathbb{Z}[\varepsilon]$, елемент α є многочленом від ε з раціональними коефіцієнтами зі спільним знаменником δ. Знайдемо ціле c, для якого $c\delta \equiv 1 \,(\mathrm{mod}\, p)$. Тоді $\alpha \equiv c\delta\alpha \,(\mathrm{mod}\, p)$, причому $\beta = c\delta\alpha \in \mathbb{Z}[\varepsilon]$.

2) Тепер можна вважати, що $\alpha = g(\varepsilon)$ для деякого многочлена $g(x)$ з цілими коефіцієнтами. Але факторкільце $\mathsf{A}/p\mathsf{A}$ має характеристику p, тому піднесення до ступеня p є в ньому гомоморфізмом. Крім того, $a^p \equiv a \,(\mathrm{mod}\, p)$ для довільного цілого a. Отже, $g(\varepsilon)^{p^f} \equiv g(\varepsilon^{p^f}) \,(\mathrm{mod}\, p)$, звідки, очевидно, і випливає необхідне порівняння. □

Наслідок III.5.2. *Первинні натуральні числа* p*, які не ділять* $m\delta$*, є нерозгалуженими в* K*.*

Зважаючи на теорему I.7.8, це твердження можна переформулювати в наступний спосіб:

первинні дільники дискримінанта D *поля* K *є первинними дільниками добутку* $m\delta$*.*

Доведення. Дійсно, припустимо що таке первинне число p є розгалуженим, тобто ділиться на квадрат деякого первинного ідеалу $\mathfrak{p}$. Тоді $\alpha^{p^f} \equiv \alpha \,(\mathrm{mod}\, \mathfrak{p}^2)$ для довільного $\alpha \in \mathsf{A}$. Виберемо $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$. Тоді $\alpha \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$, звідки $\alpha^p \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^2)$. Отже, $\alpha \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^2)$, що суперечить вибору α, □

Звідси виводиться *закон розкладу* первинних чисел у полі K.

Теорема III.5.3. *Первинне число* p*, яке не ділить* $m\delta$*, розкладається у полі* K *в добуток* k/f *різних первинних ідеалів, кожен з яких має ступінь інерції* f*, де* f *– найменший показник, для якого* $p^f \equiv 1 \,(\mathrm{mod}\, m)$.

Доведення. Дійсно, ми вже знаємо, що число p є нерозгалуженим. Нехай $\mathfrak{p}$ – якийсь первинний ідеал, що ділить p, а g – його ступінь інерції. Тоді $\mathsf{L} = \mathsf{A}/\mathfrak{p}$ – поле з p^g елементів, тому $\alpha^{p^g} \equiv \alpha \,(\mathrm{mod}\, \mathfrak{p})$ для довільного $\alpha \in \mathsf{A}$, причому g – найменший показник, який має цю властивість. Ўз твердження III.5.1 випливає, що $g \le f$. Припустимо, що $g < f$. Тоді $p^g \not\equiv 1 \,(\mathrm{mod}\, m)$, а тому $\varepsilon^{p^g} \ne \varepsilon$, але $\varepsilon^{p^g} \equiv \varepsilon \,(\mathrm{mod}\, \mathfrak{p})$. Звдіси випливає, що многочлен $x^m - 1 = \prod_{k=0}^{m-1}(x - \varepsilon^k)$ має в полі L кратний корінь ε, що неможливо, бо він є співпервинним зі своєю похідною mx^{m-1} (адже m не ділиться на p). Отже, $g = f$. Оскільки це вірно для всіх первинних ідеалів, які ділять p, твердження про їх кількість тепер безпосередньо випливає з наслідку I.7.2. □

Зокрема, первинні ідеали першого ступеня в полі K, крім скінченної кількості дільників $m\delta$ – це первинні дільники таких натуральних

первинних чисел p, що $p \equiv 1 \,(\mathrm{mod}\, m)$, причому кожне таке первинне число розкладаЄться в полі K у добуток k первинних ідеалів. Тому наслідок III.4.3 в цьому випадку перетворюЄться на таку формулу:

$$k \sum_{p \equiv 1 \,(\mathrm{mod}\, m)} \frac{1}{p^s} \;=\; \ln \frac{1}{s-1} + O(1)\,. \tag{15}$$

Наслідок III.5.4. *ІснуЄ безліч первинних чисел p, таких що $p \equiv 1 \,(\mathrm{mod}\, m)$.*

Це – частковий випадок *теореми Діріхле про первинні числа в арифметичній прогресії*. Доведення ціЄї теореми в повному обсязі потребує деяких додаткових міркувань і буде проведене в наступному розділі. З тих же міркувань ми одержимо точну рівність $k = \varphi(m)$ для розмірності поля поділу кола.

Вправи III.1. (1) (a) Доведіть, що первинні дільники числа δ, означеного вище в цьому розділі, Є також дільниками числа m. Отже, розгалуженими в полі K можуть бути лише первинні дільники m.

(b) Припустимо, що m Є первинним числом. Доведіть, що воно Є розгалуженим у полі поділу кола на m частин.

(c) Виведіть звідси, що і в загальному випадку всі первинні дільники числа m Є розгалуженими в полі поділу кола на m частин. (Скористайтеся, наприклад, результатом вправи I.7.7).

(2) Припустимо, що $m = l^d$, де l – первинне число.

(a) Доведіть, що всі числа $1 - \varepsilon^j$, де j не ділиться на l, Є асоційованими в кільці A.

(b) Перевірте, що $\Phi_m(1) = l$. Виведіть звідси, що $l\mathsf{A} = \pi^{\varphi(m)}\mathsf{A}$, де $\pi = 1 - \varepsilon$.

(c) Доведіть, що число $a_0 + a_1\pi + \cdots + a_{\varphi(m)-1}\pi^{\varphi(m)-1}$, де a_j – цілі числа, ділиться на l в кільці A тоді й лише тоді, коли всі коефіцієнти a_j діляться на l. Виведіть звідси, що $\mathsf{A} = \mathbb{Z}[\varepsilon]$.

III.6. Первинні числа в арифметичних прогресіях

Для доведення теореми Діріхле нам потрібні будуть властивості так званих *характерів абелевих груп*. Хоч їх можна знайти, наприклад, у книзі [**K**, гл. 8], ми дамо короткий виклад цих властивостей. У цьому розділі всі групи вважаються комутативними.

Означення III.6.1. (1) *Характером групи G* зветься довільний її гомоморфізм у мультиплікативну групу $\mathbb{C}^*$ поля комплексних чисел. Множина всіх характерів групи G позначається $\hat{G}$.

(2) *Головним характером* групи G зветься відображення $\chi_0 : G \to \mathbb{C}^*$, таке що $\chi_0(g) = 1$ для всіх $g \in G$.

Теорема III.6.2. *Нехай G – абелева група порядку n. Тоді:*

(1) *G має рівно n різних характерів.*

(2) *$\chi(g^{-1}) = \overline{\chi(g)}$ для кожного характера $\chi \in G$ і кожного елемента $g \in G$.*

(3) *Для довільних характерів $\chi, \psi \in \hat{G}$ має місце рівність:*

$$\sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 0 & \text{при } \chi \neq \psi \\ n & \text{при } \chi = \psi \end{cases}$$

(4) *Для довільних елементів $g, h \in G$ має місце рівність:*

$$\sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{при } g \neq h \\ n & \text{при } g = h \end{cases}$$

Доведення. *1.* Розкладемо групу G у прямий добуток циклічних, або, що те саме, задамо її твірними і співвідношеннями вигляду:

$$G = \langle\, g_1, g_2, \ldots, g_k \,|\, g_j^{m_j} = 1 \,\rangle$$

(звичайно, ми не записуємо тут співвідношень комутативності). Тоді кожен гомоморфізм $\chi : G \to \mathbb{C}^*$ визначається значеннями $\chi(g_j)$, причому єдина вимога до цих значень полягає у рівностях $\chi(g_j)^{m_j} = 1$ для всіх j. Отже, для кожного номера j маємо m_j можливостей для вибору значення $\chi(g_j)$, що разом дає $m_1 m_2 \ldots m_k = n$ різних характерів.

Твердження *2* одразу випливає з того, що $\chi(g)^n = 1$, отже $|\chi(g)|^2 = \chi(g)\overline{\chi(g)} = 1$, а тоді $\overline{\chi(g)} = \chi(g)^{-1} = \chi(g^{-1})$.

3. Випадок $\chi = \psi$ одразу випливає з твердження *2*. Припустимо, що $\chi \neq \psi$. Позначимо $S = \sum_{g \in G} \chi(g)\overline{\psi(g)}$. Знайдемо елемент $h \in G$, для якого $\chi(h) \neq \psi(h)$. Тоді

$$\chi(h)\overline{\psi(h)}\, S = \sum_{g \in G} \chi(h)\chi(g)\, \overline{\psi(h)\psi(g)} = \sum_{g \in G} \chi(hg)\, \overline{\psi(hg)} = S\,,$$

оскільки добуток hg також пробігає всі елементи групи G по одному разу. Оскільки $\chi(h)\overline{\psi(h)} \neq 1$, звідси $S = 0$.

4. Нехай $g_1, g_2, \ldots, g_n$ – всі елементи групи G, а $\chi_1, \chi_2, \ldots, \chi_n$ – всі її характери. Розглянемо квадратну матрицю X, на місці з номером (ij) в якій стоїть число $\chi_i(g_j)$. Тоді вже доведені рівності *3)* означають, що $XX^\top = nE$ (E – одинична матриця). Але тоді й $X^\top X = nE$. Розписавши останню рівність покоефіцієнтно, ми й одержимо рівності *4*. □

Нам знадобиться ще наступний наслідок з доведеної теореми.

Наслідок III.6.3. *Якщо H – підгрупа порядку k в групі $\mathfrak{G}$ порядку n, то для довільного її характеру $\psi \in \hat{H}$ існує рівно n/k характерів групи G, обмеження яких на H збігається з ψ.*

Доведення. Нехай χ і χ' – два характери групи G, для яких обмеження на H збігаються. Легко перевірити, що функція $\xi(g) = \chi(g)^{-1}\chi'(g)$ також Є характером групи G, причому його обмеження на H Є, очевидно, головним характером. Тоді ξ визначаЄ характер ξ^* факторгрупи G/H за правилом: $\xi^*(gH) = \xi(g)$. Згідно з теоремою III.6.2(1) для ξ^* існуЄ щонайбільше n/k можливостей. Але за значенням ξ^* однозначно відновлюЄться характер ξ, а знаючи χ та ξ, можна теж однозначно відновити χ'. Отже, для довільного ψ існуЄ щонайбільше n/k характерів усієї групи, які в обмеженні на H дають ψ. Оскільки G маЄ n, а H – k характерів, усі n/k можливостей повинні реалізуватися для кожного характеру ψ. □

Ми використаЄмо ці властивості у випадку, коли $G = G_m$ Є мультиплікативною групою кільця лишків за модулем m, тобто тих лишків, які Є співпервинними з m. Порядок ціЄї групи дорівнюЄ $\varphi(m)$. °ї характери, звичайно, можна розглядати як функції на множині цілих чисел, співпервиннимх з m. Нам буде зручно також покласти $\chi(a) = 0$ для кожного такого характеру і цілого a, яке не Є співпервинним з m. Перш за все, перетворимо Ойлерів добуток для дзета-функції поля K поділу кола на m. Для цього фіксуЄмо деяке первинне число p, яке не ділить $m\delta$ (ми зберігаЄмо позначення попереднього розділу). Нехай f – найменший показник, для якого $p^f \equiv 1 \pmod m$. За теоремою III.5.3 розклад числа p в полі K маЄ вигляд:

$$p\mathsf{A} = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l\,,$$

де $l = k/f$, причому $\mathrm{N}(\mathfrak{p}_j) = p^f$ для всіх $j = 1,\dots,l$. Внесок цих ідеалів в Ойлерів добуток для $\zeta_{\mathsf{K}}(s)$ становить

$$\Pi_p = \prod_{j=1}^{k} \frac{1}{1-\frac{1}{p^{fs}}}\,.$$

Розглянемо клас числа p в групі G_m. Він породжуЄ циклічну підгрупу порядку f. Ця підгрупа маЄ f характерів, які переводять p в η^j, де η – первісний корінь ступеня f з одиниці, а $j = 0,\dots,f-1$. З наслідку III.6.3 випливаЄ, що для кожного j існуЄ рівно $\varphi(m)/f$ характерів χ групи G_m, таких що $\chi(p) = \eta^j$. Зауважимо ще, що $1 - x^f = \prod_{j=0}^{f-1}(1-\eta^j x)$. Тому вираз для Π_p можна перетворити так:

$$\Pi_p = \left(\prod_{j=0}^{f-1}\frac{1}{1-\frac{\eta^j}{p^s}}\right)^{\frac{k}{f}} = \left(\prod_{\chi\in\hat{G}_m}\frac{1}{1-\frac{\chi(p)}{p^s}}\right)^{\frac{k}{\varphi(m)}}\,.$$

Позначимо $\nu = k/\varphi(m)$. Зауважимо також, що кожен співмножник з Ойлерова добутку, взятий окремо, являЄ собою нескінченно диференційовну (навіть аналітичну) функцію при $s > 0$. Оскільки існуЄ лише скінченна кількість первинних ідеалів, які ділять $m\delta$, одержуЄмо такий результат.

Твердження III.6.4. *Для дзета-функції поля поділу кола* K *маЄ місце формула:*

$$\zeta_{\mathsf{K}}(s) = F(s) \left(\prod_{\chi \in \hat{G}_m} \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \right)^{\nu},$$

де $F(s)$ *– функція, нескінченно диференційовна при* $s > 0$.

Розглянемо тепер властивості нескінченних добутків, які входять в останню формулу для дзета-функції. Зауважимо, перш за все, що для довільного характеру $\chi \in \hat{G}_m$ можна розглянути ряд Діріхле $L(\chi, s)$. При цьому ряд $L(\chi_0, s)$, який відповідаЄ головному характеру, лише скінченною кількістю співмножників відрізняЄться від дзета-функції Рімана. Тому сконцентруЄмо увагу на рядах Діріхле, які відповідають неголовним характерам.

Теорема III.6.5. *Нехай* χ *– неголовний характер групи* G_m. *Тоді:*

(1) *Ряд Діріхле* $L(\chi, s)$ *збігаЄться при* $s > 0$ *і рівномірно збігаЄться на множині* $s \geq s_0$ *для довільного* $s > 0$.

(2) *При цих значеннях* s *маЄ місце розклад ряду* $L(\chi, s)$ *в Ойлерів добуток:*

$$L(\chi, s) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

(3) *В околі* $s = 1$

$$\ln L(\chi, s) = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Доведення. *1)* Оскільки характер χ неголовний, з Теореми III.6.2(3) виплива Є, що $\sum_{a=1}^{m} \chi(a) = 0$ (досить покласти $\psi = \chi_0$). Отже, "суматорна функція" $\sum_{a<x} \chi(a)$ Є обмеженою і можна застосувати Теорему III.1.2 при довільному показнику.

2) і *3)* доводяться практично так само, як Теореми III.3.3 і III.4.2. Ми залишаЄмо ці доведення читачеві. □

Тепер ми вже можемо встановити наступні вирішальні факти.

Теорема III.6.6. (1) $L(\chi, 1) \neq 0$.
(2) $k = \varphi(m)$.

Доведення. Скористаймося твердженням III.6.4, згідно з яким

$$\zeta_{\mathsf{K}}(s) = F(s) \left(\prod_{\chi \in \hat{G}_m} L(\chi, s) \right)^{\nu},$$

де $\nu = k/\varphi(m) \leq 1$. Зауважимо, що функції $F(s)$ і $L(\chi, s)$ при $\chi \neq \chi_0$ нескінченно диференційовні в точці 1, а $\lim_{s \to 1+0}(s-1)L(\chi_0, s)$ існуЄ і не рівний 0 (так само, як для дзета-функції Рімана). Звідси виплива Є,

що, коли б якась із функцій $L(\chi, s)$ оберталась в нуль у точці 1 або було б $\nu < 1$, ми мали б $\lim_{s\to 1+0}(s-1)\zeta_{\mathsf{K}}(s) = 0$, що протирічить наслідку III.3.2. □

Тепер формула для дзета-функції з твердження III.6.4 записуЄться так:

$$\zeta_{\mathsf{K}}(s) = F(s) \prod_{\chi\in\hat{G}_m} \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}\,. \tag{16}$$

Наслідок III.6.7. *Якщо χ – характер групи G_m, то*

$$\sum_p \frac{\chi(p)}{p^s} = \begin{cases} \ln\frac{1}{s-1} + O(1) & \text{при } \chi = \chi_0 \\ O(1) & \text{при } \chi \neq \chi_0 \end{cases}$$

З останнього наслідку вже легко виводиться теорема Діріхле про первинні числа в арифметичній прогресії у вельми сильному варіанті: первинні числа виявляються у деякому розумінні рівномірно розподіленими між класами лишків за модулем m.

Теорема III.6.8. *Якщо натуральні числа a і m співпервинні, то при $s \to 1+0$*

$$\sum_{p\equiv a\,(\mathrm{mod}\,m)} \frac{1}{p^s} = \frac{1}{\varphi(m)}\,\ln\frac{1}{s-1} + O(1)$$

(p пробігаЄ первинні числа). Зокрема, існуЄ безліч первинних чисел p, таких що $p \equiv a\,(\mathrm{mod}\,m)$.

Доведення. За теоремою III.6.2 одержуЄмо:

$$\begin{aligned} \sum_{\chi\in\hat{G}_m} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} &= \sum_{\chi\in\hat{G}_m}\sum_p \frac{\chi(p)\overline{\chi(a)}}{p^s} = \\ \sum_p \frac{1}{p^s} \sum_{\chi\in\hat{G}_m} \chi(p)\overline{\chi(a)} &= \varphi(m) \sum_{p\equiv a\,(\mathrm{mod}\,m)} \frac{1}{p^s}\,. \end{aligned}$$

Але з наслідку III.6.7 виплива Є, що

$$\sum_{\chi\in\hat{G}_m} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} = \ln\frac{1}{s-1} + O(1)\,.$$

□

Вправи III.2. (1) Нехай $\mathsf{K} = \mathbb{Q}(\sqrt{d})$, де d – натуральне число, яке не ділиться на квадрати первинних чисел, $D = |D(\mathsf{K})|$.

(а) Доведіть, що існує Єдиний характер χ_d групи G_D, для якого $\chi_d(p) = \left(\frac{d}{p}\right)$ для довільного непарного первинного p, яке не ділить d.

(b) Використовуючи результати вправи I.7 (3), доведіть, що дзета-функція поля K розкладається у добуток $\zeta_{\mathsf{K}}(s) = F(s)\mathsf{L}(\chi_0, s)\mathsf{L}(\chi_d, s)$, де χ_0 – головний характер групи G_D, а $F(s)$ – функція, нескінченно диференційовна при $s > 0$.

(c) Виведіть звідси, що

$$\lim_{s\to 1}\prod_p \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} = \frac{2\tau}{\sqrt{D}}\mathrm{h}\,,$$

(добуток береться за всіма непарними первинними p, які не ділять d). Тут h – число класів ідеалів поля K, а $\tau = \ln\eta$, де η – така основна одиниця цього поля, що $\eta > 1$, якщо $d > 0$, і $\tau = 1/w$, якщо $d < 0$, де $w = 6$ при $d = -3$, $w = 4$ при $d = -1$ і $w = 2$ в інших випадках.

(2) (a) Нехай d – ціле число, яке не є повним квадратом. Доведіть, що ряд $\sum_p \left(\frac{d}{p}\right)p^{-s}$ збігається при $s = 1$ (сума береться за всіма непарними первинними, які не ділять d). Зокрема, існує безліч первинних p, для яких $\left(\frac{d}{p}\right) = -1$.

(b) Уточнити останній результат, довівши, що

$$\sum_{\left(\frac{d}{p}\right)=\delta}\frac{1}{p^s} = \frac{1}{2}\ln\frac{1}{s-1} + O(1)$$

при $i \to 1+0$, де $\delta = \pm 1$. Інакше кажучи, існує "асимптотично однакова" кількість первинних p, таких що d є квадратичним лишком за модулем p і таких що d не є квадратичним лишком за модулем p.

(c) Нехай $d_1, d_2, \ldots, d_m$ – такі цілі числа, що добуток $d_1^{k_1}d_2^{k_2}\cdot\ldots d_m^{k_m}$ є повним квадратом тоді й лише тоді, коли всі показники k_j парні. Фіксуємо довільні значеня $\delta_j = \pm 1$ $(j = 1, \ldots m)$ і позначимо $\mathcal{P}_\delta$ множину тих первинних чисел p, для яких $\left(\frac{d_j}{p}\right) = \delta_j$ для всіх номерів j. Доведіть, що

$$\sum_{p\in\mathcal{P}_\delta}\frac{1}{p^s} = \frac{1}{2^t}\ln\frac{1}{s-1} + O(1)\,.$$

(Розгляньте ряд Діріхле:

$$\sum_p \left(1+\delta_1\left(\frac{d_1}{p}\right)\right)\ldots\left(1+\delta_m\left(\frac{d_m}{p}\right)\right)\frac{1}{p^s} \quad).$$

Покажчик

Алгебричне розширення 11
Асоційовані числа 62
База ґратки 47
База ідеалу 14
Базовий об'єм 47
Базовий паралелепіпед 47
Відносна норма ідеалу 31
Геометричне зображення елемента 42
Головний дробовий ідеал 22
Головний характер 72
Група (дробових) ідеалів 22
Група класів ідеалів 22
Група одиниць 53
Ґратка 47
Двоїста база 14
Дедекіндове кільце 18
Дзета-функція поля 65
Дзета-функція Рімана 59
Дискримінант бази 34
Дискримінант (дробового) ідеалу 34
Дискримінант повної ґратки 43
Дискримінант поля 34, 40
Диферента поля 39, 40
Дійсні занурення 42
Добуток ідеалів 18
Дробовий ідеал 21
Зведений елемент 62
Індекс підмодуля 31
Індекс розгалуження 33, 40
Канонічний розклад 23
Квадратичне поле 15
Кільце ґауссових чисел 5
Константа Мінковського 52
Корозмірність ідеалу 32
Локалізація кільця 30
Логарифмічне зображення 54
Максимальний ідеал 18
Мінімальний многочлен 11, 16
Многочлен поділу кола 69
Множина твірних ідеалу 18
Модуль без скруту 24
Незвідний елемент 6
Нерозгалужене первинне число 33
Нерозгалужений первинний ідеал 33, 40
Нетерове кільце 18
Норма елемента 12, 16
Норма ідеалу 25
Обертовний дробовий ідеал 23
Ойлерів добуток 66
Опукла множина 47
Основні одиниці 57
Первинний (простий) ідеал 18
Первинний ідеал першого ступеня 33
Періодична частина модуля 24
Повна ґратка 47
Подільність ідеалів 20
Показник дробового ідеалу 23
Показник елемента 23
Поле поділу кола 69
Поля алгебричних функцій 16
Примарний модуль 30
Проективний модуль 24
Просте розширення 37
Регулятор 57

Розгалужений первинний
ідеал 33, 40
Розгалужене первинне
число 33
Ряд Діріхле 59
Скінченне розширення 12
Слід елемента 12, 16
Скінченно-породжений модуль 21
Співпервинні ідеали 25
Спряжені занурення 42
Ступінь інерції 33, 40
Ступінь розширення 12
Твірні модуля 21
Теорема Ерміта 53
Уявні занурення 42
Форма сліду 13
Фундаментальна база 14, 17
Функція Ойлера 69
Характер групи 72
Характеристичний многочлен
елемента 12, 16
Центрально-симетррична
множина 48
Ціла алгебрична функція 16
Ціла залежність 9
Цілий алгебричний елемент 9
Цілком розкладне первинне
число 34
Цілком розкладний первинний
ідеал 40
Цілозамкнене підкільце 10

Бібліоґрафія

[КФ] Алгебраическая теория чисел / Под ред. Касселса Дж., Фрёлиха А. – М., 1969.

[БШ] Боревич З. И., И. Р. Шафаревич. Теория чисел. – М., 1985.

[ВВ] Ван дер Варден Б. Л. . Алгебра. – М., 1976.

[АВ] Вейль А. Основы теории чисел. – М., 1972.

[ГВ] Вейль Г. Алгебраическая теория чисел. – М., 1947.

[ИВ] Виноградов И.М. Основы теории чисел. – М., 1972.

[Г] Гекке Э. Лекции по теории алгебраических чисел. – М.;Л., 1940.

[К] Кострикин А.И. Введение в алгебру. – М., 1977.

[Л1] Ленг С. Алгебра. – М., 1968.

[Л2] Ленг С. Алгебраические числа. – М., 1966.

[Ф] Фаддеев Д.К. Лекции по алгебре. – М., 1980.