charac

1. Характери і ґаусові суми

У цьому розділі G позначає *скінченну абелеву групу* порядку $g = \#(G)$. $\mathbb{C}^\times$ — мультиплікативна група ненульових комплексних чисел.

ch1 **Означення 1.1.** *Характером* групи G зветься гомоморфізм $G \to \mathbb{C}^\times$. *Добутком* характерів χ nf η зветься характер $\chi\eta$, для якого $(\chi\eta)(a) = \chi(a)\eta(a)$. Позначимо через $\hat{G}$ множину всіх характерів групи G, а через χ_0 — *тривіальний характер*, для якого $\chi(a) = 1$ для всіх inG.

ch2 **Теорема 1.2.** (1) *$\hat{G}$ є групою відносно множення характерів, причому χ_0 є нейтральним елементом цієї групи, а $\chi^{-1}(a) = \chi(a^{-1}) = \bar{\chi}(a)$*

(2) $\#(\hat{G}) = \#(G)$.

(3) *Для довільних характерів $\chi, \eta \in \hat{G}$*

$$\sum_{a\in G} \chi(a)\bar{\eta}(a) = \begin{cases} g, & \text{якщо } \chi = \eta, \\ 0, & \text{якщо } \chi \neq \eta. \end{cases}$$

(4) *Для довільних елементів $a, b \in G$*

$$\sum_{\chi\in \hat{G}} \chi(a)\bar{\chi}(b) = \begin{cases} g, & \text{якщо } a = b, \\ 0, & \text{якщо } a \neq b. \end{cases}$$

Доведення. (1) Те, що $\hat{G}$ є групою, очевидно. Крім того, $a^g = 1$ для кожного $a \in G$, тому й $\chi(a)^g = 1$, звідки $|\chi(a)| = 1$. Отже, $\chi(a)\bar{\chi}(a) = |\chi(a)|^2 = 1$, тобто $\chi(a)^{-1} = \bar{\chi}(a)$.

(3) Якщо $\chi = \eta$, ця сума дорівнює $\sum_{a\in G} |chi(a)|^2 = g$. Якщо $\chi \neq \eta$, виберемо елемент $b \in G$, для якого $\chi(b) \neq \eta(b)$, або, що те саме, $\chi(b)\bar{\eta}(b) \neq 1$. Тоді

$$\sum_{a\in G} \chi(a)\bar{\eta}(a) = \sum_{a\in G} \chi(ab)\bar{\eta}(ab) = \chi(a)\bar{\eta}(b) \sum_{a\in G} \chi(a)\bar{\eta}(a).$$

Оскільки $\chi(b)\bar{\eta}(b) \neq 1$, звідси $\sum_{a\in G} \chi(a)\bar{\eta}(a) = 0$.

Доведення тверджень (2) і (4) ґрунтується на такій лемі.

ch3 **Лема 1.3.** *Для кожного неодиничного елемента $a \in G$ існує характер η, для якого $\eta(a) \neq 1$.*

Доведення. Розкладемо G у прямий добуток циклічних підгруп: $G = C_1 \times C_2 \times \ldots \times C_m$, де C_j породжена елементом c_j порядку n_j. Тоді кожен елемент a групи G однозначно розкладається у добуток $a = c_1^{k_1} c_2^{k_2} \ldots c_m^{k_m}$, де $0 \leqslant k_j < n_j$, причому якщо $a \neq 1$, то знайдеться номер j, для якого $k_j \neq 0$. Нехай ε_j — первісний корінь з одиниці степеня n_j. Тоді функція η, задана правилом $\eta(a) = \varepsilon_j^{k_j}$ є характером групи G і $\eta(a) \neq 1$, якщо $k_j \neq 0$. $\square$

Нехай $g' = \#(\hat{G})$. Тоді $\sum_{\chi\in\hat{G}} \chi(a)\bar{\chi}(a) = g'$. Якщо $a \neq b$, виберемо характер η, для якого $\eta(a)\bar{\eta}(b) = \eta(ab^{-1}) \neq 1$. Тоді

$$\sum_{\chi\in\hat{G}} \chi(a)\bar{\chi}(b) = \sum_{\chi\in\hat{G}} (\chi\eta)(a)(\bar{\chi}\bar{\eta})(b) = \eta(a)\bar{\eta}(b) \sum_{\chi\in\hat{G}} \chi(a)\bar{\chi}(b),$$

звідки $\sum_{\chi\in\hat{G}} \chi(a)\bar{\chi}(b) = 0$. Отже, ми довели «властивість $(4')$», яка відрізняється від (4) лише заміною g на g'.

Занумеруємо елементи групи G: $G = \{ a_1, a_2, \dots, a_g \}$, та її характери: $\hat{G} = \{ \chi_1, \chi_2, \dots, \chi_{g'} \}$. Розглянемо матрицю $X = (x_{ij})$ розміру $g' \times g$, де $x_{ij} = \chi_i(a_j)$. Тоді властивість (3) перепишеться у вигляді $X\bar{X}^\top = gE_{g'}$, а «властивість $(4')$» — у вигляді $X^\top\bar{X} = g'E_g$, де E_m позначає одиничну матрицю розміру $m\times m$. Звідси легко випливає, що $g = g'$. Це й завершує доведення тверджень (2) і (4). $\square$

ch4 **Означення 1.4.** Позначимо через Z_m кільце лишків за модулем m, а через Φ_m — мультиплікативну групу його оборотних елементів (тобто тих класів лишків, елементи яких співпервинні з m).

(1) Характери групи Φ_m звуться *характерами за модулем m*. Кожен такий характер χ розповсюдимо на всі цілі числа, вважаючи, що $\chi(a) = \chi(a + m\mathbb{Z})$, якщо нсд$\,(a, m) = 1$, і $\chi(a) = 0$, якщо нсд$\,(a, m) > 1$.

(2) Характер χ за модулем m зветься *парним*, якщо $\chi(-1) = 1$ (тоді $\chi(-a) = \chi(a)$ для всіх a), і *непарним*, якщо $\chi(-1) = -1$ (тоді $\chi(-a) = -\chi(a)$ для всіх a).
Зауважимо, що $\chi(-1)^2 = \chi(1) = 1$, тому кожен характер є або парним, або непарним.

(3) Характер χ за модулем m зветься *примітивним*, якщо для кожного власного дільника d числа m існує число $a \equiv 1$ *pmdd*, для якого $\chi(a) \neq 1$.

ch5 **Означення 1.5.** Нехай χ — характер за модулем m. *Ґаусовою сумою* для характеру χ зветься число $\tau_k(\chi) = \sum_{a\in\Phi_m} \chi(a)\varepsilon^{-ka}$, де $\varepsilon = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. Позначимо $\tau(\chi) = \tau_1(\chi)$.

ch6 **Твердження 1.6.** *Якщо χ — примітивний характер за модулем m, то*

$$\tau_k(\chi) = \begin{cases} 0, & \text{якщо нсд}\,(k, m) > 1, \\ \bar{\chi}(k)\tau(\chi), & \text{якщо нсд}\,(k, m) = 1. \end{cases}$$

Доведення. Нехай нсд $(k,m)=d>1$, $c=\frac{m}{d}$. Тоді ε^k є первинним коренем степеня c з 1, тому $\varepsilon^a b=\varepsilon^a$, якщо $b\equiv 1$
pmdc. Оскільки χ примітивний, знайдеться число $b\equiv 1$
pmdc, для якого $\chi(b)\neq 1$. Тоді

$$\tau_k(\chi)=\sum_{a\in\Phi_m}\chi(ab)\varepsilon^{abk}=\chi(b)\sum_{a\in\Phi_m}\varepsilon^{ak}=\chi(b)\tau_k(\chi),$$

звідки $\tau_k(\chi)=0$. Якщо ж нсд $(k,m)=1$, то

$$\tau_k(a)=\chi(k)^{-1}\sum_{a\in\Phi_m}\chi(ka)\varepsilon^{ka}=\bar{\chi}(k)\sum_{a\in\Phi_m}\chi(a)\varepsilon^{a}=\bar{\chi}(k)\tau(\chi).$$

□

ch5 **Вправа 1.7.** (1) Довести, що для довільного характеру χ за модулем m має місце рівність

$$\chi(a)=\frac{1}{m}\sum_{k=0}^{m-1}\tau_k(\chi)\varepsilon^{-ka},$$

.

(2) З попереднього твердження та того, що $\sum_{a\in Z_m}\chi(a)\bar{\chi}(a)=\phi(m)$, вивести, що $|\tau(\chi)|=\sqrt{m}$ для кожного примітивного характеру за модулем m.

2. L-ряди примітивних характерів

lr

У цьому розділі ми фіксуємо натуральне число $m>1$ і позначаємо через χ деякий *примітивний* характер за модулем m. Оскільки $\chi\neq\chi_0$, то з теореми 1.2 (3) випливає, що $\sum_{a\in Z_m}\chi(a)=0$. Тому модуль суми $F(x)=\sum_{n\leqslant x}\chi(n)$ не перевищує $\phi(m)$. Отже, для довільного $c>0$

$$\lim_{x\to\infty}\frac{F(x)}{x^c}=0.$$

Тому ряд Діріхле $L(\chi,s)$ збігається при всіх $s>0$ і визначає для таких s аналітичну функцію. Зокрема, визначене значення $L(\chi,1)$. Наша мета полягає у обчисленні цього значення. Нехай $\varepsilon=\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$. Враховуючи, що

$$\sum_{k=0}^{m-1}\varepsilon^{ka}=\begin{cases}0, & \text{якщо } a\equiv 0\,(\mathrm{mod}\,m),\\ m, & \text{якщо } a\not\equiv 0\,(\mathrm{mod}\,m),\end{cases}$$

ряд Діріхле $L(\chi, s)$ можна перетворити в такий спосіб:

$$\begin{aligned} L(\chi, s) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{a\in\Phi_m} \chi(a) \sum_{n\equiv a \pmod m} \frac{1}{n^s} = \\ &= \frac{1}{m} \sum_{a\in\Phi_m} \chi_a \sum_{n=1}^{\infty} \Big(\sum_{k=0}^{m-1} \varepsilon^{k(a-n)} \Big) \frac{1}{n^s} = \\ &= \frac{1}{m} \sum_{k=0}^{m-1} \Big(\sum_{a\in\Phi_m} \chi(a)\varepsilon^{ak} \Big) \sum_{n=1}^{\infty} \frac{\varepsilon^{-kn}}{n^s} = \\ &= \frac{1}{m} \sum_{k=0}^{m} \tau_k(\chi) \sum_{n=1} \frac{\varepsilon^{-kn}}{n^s} = \frac{\tau(\chi)}{m} \sum_{k\in\Phi_m} \bar{\chi}(k) \sum_{n=1} \frac{\varepsilon^{-kn}}{n^s}. \end{aligned}$$

Зокрема,

eq1

$$\begin{aligned} L(\chi, 1) &= \frac{\tau(\chi)}{m} \sum_{k\in\Phi_m} \bar{\chi}(k) \sum_{n=1} \frac{\varepsilon^{-kn}}{n} = \\ &= -\frac{\tau(\chi)}{m} \sum_{k\in\Phi_m} \bar{\chi}(k) \ln(1-\varepsilon^{-k}). \end{aligned} \tag{1}$$

Тут $\ln z$ позначає *головне значення* логарифму комплексного числа z, тобто якщо $z = \rho(\cos\alpha + i\sin\alpha)$, де $\rho = |z|$, а $\alpha = \arg z$, причому $-\pi < \alpha \leqslant \pi$, то $\ln z = \ln\rho + i\alpha$. Саме для головного значеня логарифму має місце розклад:[1]

$$\ln(1-z) = -\sum_{n=1}^{\infty} \frac{z^n}{n}, \text{ якщо } |z| \leqslant 1 \text{ і } z \neq 1.$$

Зокрема, $1 - \varepsilon^{-k} = 1 - \cos\frac{2k\pi}{m} + i\sin\frac{2k\pi}{m}$, тому

$$|1-\varepsilon^{-k}|^2 = 1 - 2\cos\frac{2k\pi}{m} + \cos^2\frac{2k\pi}{m} + \sin^2\frac{2k\pi}{m} = 2\Big(1 - \cos\frac{2k\pi}{m}\Big),$$

звідки $|1-\varepsilon^{-k}| = 2\sin\frac{k\pi}{m}$. Оскільки $1 - \cos\frac{2k\pi}{m} \geqslant 0$, аргумент α числа $1-\varepsilon^{-k}$ належить проміжку $\big[-\frac{\pi}{2}, \frac{\pi}{2}\big]$. Тому з рівності

$$\sin\alpha = \frac{\sin\frac{2k\pi}{m}}{2\sin\frac{k\pi}{m}} = \cos\frac{k\pi}{m}$$

випливає, що $\alpha = \frac{\pi}{2} - \frac{k\pi}{m}$. Отже

$$\ln(1-\varepsilon^{-k}) = \ln\Big(2\sin\frac{k\pi}{m}\Big) + i\pi\Big(\frac{1}{2} - \frac{k}{m}\Big).$$

[1] Див. підручник: А. И. Маркушевич. Теория аналитических функций. Т. 1, глава 3, пп. 5.4 та 7.3.

З цих формул виводяться остаточні вирази для значення $L(\chi,1)$ в залежності від парності характеру χ.

lr1 **Теорема 2.1.** *Якщо примітивний характер* χ *за модулем* m *є парним, то*

$$L(\chi,1)=-\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\ln\sin\frac{k\pi}{m}.$$

Якщо примітивний характер χ *за модулем* m *є непарним, то*

$$L(\chi,1)=\frac{\pi i\tau(\chi)}{m^2}\sum_{k\in\Phi_m}\bar\chi(k)k.$$

Доведення. Замінимо у формулі (1) число k на $-k$. Якщо характер χ є парним, одержимо

$$L(\chi,1)=-\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\ln(1-\varepsilon^k),$$

звідки

$$\begin{aligned}2L(\chi,1)&=-\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\big(\ln(1-\varepsilon^{-k})+\ln(1-\varepsilon^k)\big)=\\&=-2\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\ln\left(2\sin\frac{k\pi}{m}\right)=\\&=-2\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\ln\sin\frac{k\pi}{m},\end{aligned}$$

оскільки $\sum_{k\in\Phi_m}\bar\chi(k)\ln 2=0$. Це доводить першу формулу. Якщо ж характер χ є непарним, аналогічно одержимо

$$\begin{aligned}2L(\chi,1)&=-\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\big(\ln(1-\varepsilon^{-k})-\ln(1-\varepsilon^k)\big)=\\&=-2\frac{\tau(\chi)}{m}\sum_{k\in\Phi_m}\bar\chi(k)\pi i\Big(\frac12-\frac{k}{m}\Big)=2\frac{\pi i\tau(\chi)}{m^2}\sum_{k\in\Phi_m}\bar\chi(k)k,\end{aligned}$$

що доводить другу формулу. □

lr2 **Вправа 2.2.** Характер χ за модулем m зветься *квадратичним*, якщо всі значення $\chi(a)$ дійсні, тобто дорівнюють ±1. Доведіть, що для квадратичного парного характера ґаусова сума $\tau(\chi)$ є дійсною, а для квадратичного непарного — чисто уявною. Зокрема, якщо квадратичний характер χ є примітивним парним, то $\tau(\chi)=\pm\sqrt{m}$, а якщо він є примітивним непарним, то $\tau(\chi)=\pm i\sqrt{m}$.

lr3 *Зауваження* 2.3. Насправді, можна довести, що для примітивного квадратичного характера χ за модулем m

$$\tau(\chi) = \begin{cases} \sqrt{m}, & \text{якщо } \chi \text{ парний,} \\ i\sqrt{m}, & \text{якщо } \chi \text{ непарний.} \end{cases}$$

З того, що характер є мультиплікативною функцією, тобто $\chi(ab) = \chi(a)\chi(b)$ випливає, що для ряду Діріхле $L(\chi, s)$ має місце *розклад Ойлера*

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

Доведення дослівно повторює відповідні міркування для дзета-функції.

3. Характер квадратичного поля

qua З кожним квадратичним полем $\mathbf{K} = \mathbb{Q}(\sqrt{d})$, де $d \neq 1$ — ціле число, вільне від квадратів, D — дискримінант поля K і $\mathbf{A}$ — кільце цілих чисел поля $\mathbf{K}$. Нехай $d = b_0 b_1 \dots b_k$ де $b_1, b_2, \dots, b_k$ — різні первинні числа, а $b_0 = \operatorname{sgn} d = \pm 1$. Для кожного цілого числа a,
p1 співпервинного з D, визначимо $\chi_d(a)$ правилом

$$\chi_d(a) = \prod_{i=1}^{k} \left(\frac{a}{b_i}\right), \text{ якщо } d \equiv 1 \pmod 4;$$

$$\chi_d(a) = (-1)^{\frac{a-1}{2}\cdot\frac{d-2}{4}+\frac{a^2-1}{8}} \prod_{i=1}^{k-1} \left(\frac{a}{b_i}\right) \prod_{i=1}^{k-1} \left(\frac{a}{b_i}\right), \text{якщо } d \equiv 2 \pmod 4, b_k = 2;$$

$$\chi_d(a) = (-1)^{\frac{a-1}{2}} \prod_{i=1}^{k} \left(\frac{a}{b_i}\right), \text{ якщо } d \equiv 3 \pmod 4.$$

Зауважимо, що в другому й третьому випадках число a обов'язково є непарним.

qua1 **Твердження 3.1.** *Значення $\chi_d(a)$ залежить лише від залишку числа a за модулем $|D|$, причому $\chi_d(aa') = \chi_d(a)\chi_d(a')$.*

Доведення. Це очевидно випливає з таких фактів:

- $D = d$, якщо $d \equiv 1 \pmod 4$, і $D = 4d$ в інших випадках.
- $\left(\frac{a}{b_i}\right)$ залежить лише від залишку a за модулем b_i, причому $\left(\frac{ab}{b_i}\right) = \left(\frac{a}{b_i}\right)\left(\frac{b}{b_i}\right)$.
- Парність числа $\frac{a-1}{2}$ залежить лише від залишку a за модулем 4, причому $aa' - 1 \equiv (a-1) + (a'-1) \pmod 4$ для довільних непарних a, a'.

- Парність числа $\frac{a^2-1}{8}$ залежить лише від залишку a за модулем 8, причому $(aa')^2 - 1 \equiv (a^2-1) + (a'^2-1) \pmod{16}$ для довільних непарних a, a'.

$\square$

qua2 **Вправа 3.2.** Доведіть, що $\chi_d(|D|-1) = \operatorname{sgn} d$.

Розповсюдимо χ_d на всі цілі числа, вважаючи, що $\chi_d(a) = 0$, якщо нсд$(a, D) > 1$, і $\chi_d(-a) = \chi_d(a) \operatorname{sgn} d$ $(a > 0)$. З твердження 3.1 та вправи 3.2 випливає, що в такий спосіб функція χ_d перетворюється на характер за модулем $|D|$, який є парним, якщо $d > 0$, і непарним, якщо $d < 0$. Він зветься *характером квадратичного поля* $\mathbf{K} = \mathbb{Q}(\sqrt{d})$. Виявляється, що цей характер «відповідає» за розклад первинних чисел у кільці $\mathbf{A}$.

qua3 **Теорема 3.3.** *Нехай p — первинне натуральне число. У кільці* $\mathbf{A}$ *ідеал $p\mathbf{A}$ є*

- *квадратом первинного ідеала, якщо $\chi_d(p) = 0$;*
- *добутком двох різних первинних ідеалів, якщо $\chi_d(p) = 1$;*
- *первинним ідеалом, якщо $\chi_d = -1$.*

Доведення. Розглянемо випадок, коли $d \equiv 1 \pmod 4$, тобто $D = d$; інші випадки перевіряються аналогічно. Нагадаємо, що p є розгалуженим в полі $\mathbf{K}$ тоді й лише тоді, коли $p \mid D$. Оскільки $(\mathbf{K} : \mathbb{Q}) = 2$, тоді $p\mathbf{A} = \mathfrak{p}^2$ для деякого первинного $\mathfrak{p}$. Нехай $p \nmid D$. Якщо p непарне, то ідеал $p\mathbf{A}$ залишається первинним, якщо $\left(\frac{d}{p}\right) = -1$ і розкладається в добуток двох первинних, якщо $\left(\frac{d}{p}\right) = 1$. Але

$$\left(\frac{d}{p}\right) = \prod_{i=0}^{k} \left(\frac{b_i}{p}\right) = \prod_{i=0}^{k} (-1)^{\frac{p-1}{2} \cdot \frac{b_i-1}{2}} \prod_{i=1}^{k} \left(\frac{p}{b_i}\right) =$$
$$= (-1)^{\frac{p-1}{2} \sum_{i=0}^{k} \frac{b_i-1}{2}} \prod_{i=1}^{k} \left(\frac{p}{b_i}\right) =$$
$$= (-1)^{\frac{p-1}{2} \cdot \frac{d-1}{2}} \prod_{i=1}^{k} \left(\frac{p}{b_i}\right) = \prod_{i=1}^{k} \left(\frac{p}{b_i}\right) = \chi_d(p).$$

Якщо ж $p = 2$, то

$$\chi_d(2) = \prod_{i=1}^{k} \left(\frac{2}{b_i}\right) = (-1)^{\sum_{i=0}^{k} \frac{b_i^2-1}{8}} = (-1)^{\frac{d^2-1}{8}}.$$

Останній вираз дорівнює 1, якщо $d \equiv 1 \pmod 8$, а саме в цьому випадку ідеал $2\mathbf{A}$ розкладається в добуток двох первинних, і дорівнює -1, якщо $d \equiv 5 \pmod 8$, а саме в цьому випадку ідеал $2\mathbf{A}$ залишається первинним. $\square$

З наступної вправи випливає, що характер χ_d завжди є примітивним.

Вправа 3.4. Довести, що для довільного цілого числа $d \neq 1$, яке вільне від квадратів, і для кожного дільника $c|D$, $1 < c < d$, існує таке число $a \equiv 1 \pmod c$, що $\chi_d(a) = -1$, де χ_d — характер квадратичного поля $\mathbb{Q}(\sqrt{d})$, а D — дискримінант цього поля.

zet

4. Дзета-функція квадратичного поля

Ми зберігаємо позначення попереднього розділу. Нагадаємо, що *ζ-функцією поля* $\mathbf{K}$ зветься функція

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

де $\mathcal{I}$ — множина (ненульових) ідеалів кільця $\mathbf{A}$, а $\mathcal{P}$ — множина (ненульових) первинних ідеалів цього кільця. Перепишемо Ойлерів добуток у вигляді

$$\zeta_{\mathbf{K}}(s) = \prod_{p} g_p(s), \text{ де } g_p(s) = \prod_{\mathfrak{p} \ni p} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}},$$

а p пробігає всі первинні числа. З теореми 3.3 безпосередньо випливає такий наслідок.

zet1 **Твердження 4.1.** *Нехай $\chi = \chi_d$ — характер поля $\mathbf{K}$. Для кожного первинного числа p*

$$g_p(s) = \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

Тому

$$\zeta_{\mathbf{K}}(s) = \zeta(s) L(\chi, s).$$

Нагадаємо, що $\lim_{s \to 1+0} (s-1)\zeta(s) = 1$, а $\lim_{s \to 1+0} \zeta_{\mathbf{K}}(s) = \kappa h$, де h — кількість класів ідеалів в полі $\mathbf{K}$, а

$$\kappa = \frac{2^{r+t} \pi^t R}{w \sqrt{|D|}},$$

де R — регулятор поля $\mathbf{K}$, а w — кількість коренів з одиниці в цьому полі. У випадку квадратичного поля, якщо $d > 0$, то $r = w = 2$, $t = 0$, а $R = \ln \varepsilon$, де ε — такий твірний групи одиниць, що $\varepsilon > 1$.

Якщо $d < 0$, то $r = 0$, $t = 1$, $w = 2$, крім випадків $d = -1$, $w = 4$ та $d = -3$, $w = 6$, $R = 1$.

zet2 **Наслідок 4.2.**

eq2 (2)
$$h = \begin{cases} L(\chi, 1)\dfrac{\sqrt{D}}{2\ln\varepsilon}, & \textit{якщо } d > 0, \\ \\ L(\chi, 1)\dfrac{q\sqrt{-D}}{\pi} & \textit{якщо } d < 0, \end{cases}$$
де $q = 2$*, якщо* $d = -1$*,* $q = 3$*, якщо* $d = -3$*, і* $q = 1$ *в інших випадках.*

Останній результат можна застосувати для знаходження числа класів ідеалів, оскільки для $L(\chi, 1)$ є явні формули (теорема 2.1 і зауваження 2.3). З іншого боку, її можна застосувати для знаходження суми ріду Діріхле $L(\chi, 1)$.

zet3 **Приклад 4.3.** Якщо $d = -1$, то $h = 1$, $q = \sqrt{-D} = 2$, $\chi(n) = (-1)^{\frac{n-1}{2}}$, якщо n непарне, інакше $\chi(n) = 0$. Звідси одержуємо відомий результат Ґреґорі (який, правда, часто звуть «рядом Ляйбніца»):
$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots = \frac{\pi}{4}.$$

zet4 **Вправа 4.4.** Обчислити суму ряду
$$1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \dots$$

Формули (2) можна спростити, якщо скористатися теоремою 2.1 і зауваженням 2.3. Якщо $d > 0$, характер χ є парним, тому $\tau(\chi) = \sqrt{D}$, $\chi(D - k) = \chi(k)$, а тому
$$L(\chi, 1) = \frac{2}{\sqrt{D}} \sum_{k=1}^{[D/2]} \chi(k) \ln \sin \frac{\pi k}{D},$$
звідки
$$h = -\frac{1}{\ln\varepsilon} \sum_{k=1}^{[D/2]} \chi(k) \ln \sin \frac{\pi k}{D} = \frac{\ln \eta}{\ln \varepsilon},$$
де

eq3 (3)
$$\eta = \frac{\prod_{\substack{0<b<D/2 \\ \chi(b)=1}} \sin \frac{\pi b}{D}}{\prod_{\substack{0<a<D/2 \\ \chi(a)=1}} \sin \frac{\pi a}{D}}.$$
Останню рівність можна переписати так.

zet5 **Теорема 4.5.** *Для дійсного квадратичного поля з дискримінантом D і характером χ число η, яке визначене формулою (3) є одиницею цього поля, причому $\eta = \varepsilon^h$, де $\varepsilon > 1$ — основна одиниця цього поля. Зокрема $\eta > 1$.*

Цей наслідок (навіть те, що $\eta > 1$) досі не вдалося довести елементарними методами, незважаючи на численні спроби.

Якщо $d < 0$, характер χ є непарним і $\tau(\chi) = i\sqrt{-D}$. Звідси

$$L(\chi, 1) = \frac{\pi}{D} \sum_{k=1}^{|D|-1} \chi(k)k$$

Вважатимемо, що $d < -3$, тоді $q = 1$, тому

$$h = \sum_{k=1}^{|D|-1} \chi(k)k.$$

Припустимо спочатку, що $d \equiv 3 \pmod 4$ або $d \equiv 2 \pmod 4$. Тоді $D = 4d$ — парне. Нехай $m = 2|d|$, тобто $|D| = 2m$. В обох випадках з означеня характеру χ_d (с. 6) безпосередньо випливає, що $\chi(m + 1) = -1$. Якщо k непарне, то $k(m + 1) \equiv m + k \pmod{2m}$, тому $\chi(m + k) = -\chi(k)$. Отже

$$\begin{aligned} h &= -\frac{1}{2m}\Big(\sum_{k=1}^{m-1} \chi(k)k + \sum_{k=1}^{m-1} \chi(m+k)(m+k)\Big) = \\ &= -\frac{1}{2m}\Big(\sum_{k=1}^{m-1} \chi(k)k - \sum_{k=1}^{m-1} \chi(k)(m+k)\Big) = \frac{1}{2}\sum_{k=1}^{m-1} \chi(k). \end{aligned}$$

Якщо $d \equiv 1 \pmod 4$, то $D = d$ — непарне. Тоді

$$\begin{aligned} h &= \frac{1}{D}\Big(\sum_{0<k<|D|/2} \chi(k)k + \sum_{0<k<|D|/2} \chi(|D|-k)(|D|-k)\Big) = \\ &= \frac{2}{D}\Big(\sum_{0<k<|D|/2} \chi(k)k - |D| \sum_{0<k<|D|/2} \chi(k)\Big). \end{aligned}$$

Зауважимо, що коли k пробігає всі лишки за модулем $|D|$, так само $2k$ пробігає всі такі лишки. Крім того, якщо $k' \neq k$, то $|D| - 2k \not\equiv$

$2k' \pmod{|D|}$. Тому

$$h = \frac{1}{D}\Big(\sum_{0<k<|D|/2}\chi(2k)2k + \sum_{0<k<|D|/2}\chi(|D|-2k)(|D|-2k)\Big) =$$

$$= \frac{\chi(2)}{D}\Big(4\sum_{0<k<|D|/2}\chi(k)k - |D|\sum_{0<k<|D|/2}\chi(k)\Big),$$

або, оскільки $\chi(2)^2 = 1$,

$$h\chi(2) = \frac{1}{D}\Big(4\sum_{0<k<|D|/2}\chi(k)k - |D|\sum_{0<k<|D|/2}\chi(k)\Big).$$

З цих двох рівностей одержуємо, що

$$h(2-\chi(2)) = \sum_{0<k<|D|/2}\chi(k).$$

Оскільки $\chi(2) = 0$ для парного D, ми одержали такий результат

zet6 **Теорема 4.6.** *Для уявного квадратичного поля з дискримінантом* $D < -4$

$$h = \frac{1}{2-\chi(2)}\sum_{0<k<|D|/2}\chi(k).$$

Цікавий наслідок отримуємо, якщо $d = -p$, де p — первинне число, причому $p \equiv 3 \pmod 4$. Тоді $|D| = p$, $\chi(k) = \left(\frac{k}{p}\right)$, а $\chi(2) = 1$, якщо $p \equiv 7 \pmod 8$, і $\chi(2) = -1$, якщо $p \equiv 3 \pmod 8$.

zet7 **Наслідок 4.7.** *Нехай A — кількість квадратичних лишків за модулем p серед чисел $0 < k < p/2$, а B — кількість квадратичних нелишків серед цих чисел. Тоді кількість класів ідеалів поля $\mathbb{Q}\sqrt{-p})$ задається формулою*

$$h = \begin{cases} A-B, & \text{якщо } p \equiv 7 \pmod 8, \\ \frac{1}{3}(A-B), & \text{якщо } p \equiv 3 \pmod 8. \end{cases}$$

Зокрема, завжди $A > B$.