

УДК 511.23

**АЛГОРИТМ ВЫЧИСЛЕНИЯ ИДЕАЛА ШТИКЕЛЬБЕРГЕРА  
ДЛЯ МУЛЬТИКВАДРАТИЧНЫХ ПОЛЕЙ<sup>1</sup>**

Е. А. Киршанова, Е. С. Малыгина, С. А. Новоселов, Д. О. Олефиренко

*Балтийский федеральный университет им. И. Канта, г. Калининград, Россия*

Представлен алгоритм вычисления идеала Штикельбергера для мультикватратичного поля  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , где  $d_i \equiv 1 \pmod{4}$ ,  $i \in \{1, \dots, n\}$ , или некоторый  $d_j \equiv \pm 2 \pmod{8}$ ,  $j \in \{1, \dots, n\}$ , все  $d_i$  – целые, попарно взаимно простые и свободные от квадратов. В основу работы положена статья Р. Кучеры [J. Number Theory, no. 56, 1996]. Мы предлагаем алгоритм вычисления идеала Штикельбергера, работающий за время  $\mathcal{O}(\lg \Delta_K \cdot 2^n \cdot \text{poly}(n))$ , где  $\Delta_K$  – дискриминант поля  $K$ . В качестве приложения показана взаимосвязь идеала Штикельбергера с числом классов мультикватратичного поля.

**Ключевые слова:** мультикватратичные поля, элемент Штикельбергера, идеал Штикельбергера, группа классов мультикватратичного поля.

DOI 10.17223/20710410/50/1

**AN ALGORITHM FOR COMPUTING THE STICKELBERGER IDEAL  
FOR MULTIQUADRATIC NUMBER FIELDS**

E. A. Kirshanova, E. S. Malygina, S. A. Novoselov, D. O. Olefirenko

*Immanuel Kant Baltic Federal University, Kaliningrad, Russia*

**E-mail:** {ekirshanova,emalygina,snovoselov,dolefirenko}@kantiana.ru

We present an algorithm for computing the Stickelberger ideal for multiquadratic fields  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , where the integers  $d_i \equiv 1 \pmod{4}$  for  $i \in \{1, \dots, n\}$  or  $d_j \equiv 2 \pmod{8}$  for one  $j \in \{1, \dots, n\}$ ; all  $d_i$ 's are pairwise co-prime and square-free. Our result is based on the paper of Kučera [J. Number Theory, no. 56, 1996]. The algorithm we present works in time  $\mathcal{O}(\lg \Delta_K \cdot 2^n \cdot \text{poly}(n))$ , where  $\Delta_K$  is the discriminant of  $K$ . As an interesting application, we show a connection between Stickelberger ideal and the class number of a multiquadratic field.

**Keywords:** multiquadratic number field, Stickelberger element, Stickelberger ideal, class group of multiquadratic field.

**Введение**

Идеал Штикельбергера  $I$  числового поля  $K$  – это идеал групповой алгебры  $\mathbb{Z}[G_K]$ , где  $G_K = \text{Gal}(K/\mathbb{Q})$  – группа Галуа поля  $K$ . Ключевое свойство идеала Штикельбергера, известное как теорема Штикельбергера [1] (современное изложение см. в [2, § 6.2]), заключается в том, что элементы этого идеала аннигилируют группу классов  $K$ , то есть для любого  $\sigma \in I$  и любого дробного идеала  $J$  кольца целых поля  $K$  идеал  $J^\sigma$  является главным.

<sup>1</sup>Работа Киршановой Е. А. выполнена при частичной финансовой поддержке конкурса «Молодая математика России» 2020 и Программы мобильности 5-100.

Получение идеала Штикельбергера в явном виде, то есть вычисление его образующих, является важной алгоритмической задачей в алгебраической теории чисел [3] и, с недавних пор, в криптоанализе [4].

Так, например, явный вид идеала Штикельбергера для кругового поля  $K = \mathbb{Q}(\zeta_r)$  ( $r > 0, r \in \mathbb{Z}$ ), описанный в [2], позволил получить алгоритм [4] нахождения короткого вектора в идеалах кольца целых кругового поля; в современном криптоанализе нахождение короткого вектора в решётках является основополагающей задачей.

В этой работе рассматриваются другие поля, а именно, мультикватратичные поля  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , где  $d_i \equiv 1 \pmod{4}$  свободны от квадратов и попарно взаимно просты. Предлагается алгоритм вычисления идеала Штикельбергера поля  $K$ . Такой алгоритм интересен, в первую очередь, с точки зрения вычислений группы классов поля  $K$  (см. п. 4). В криптографии эта задача возникает в конструкциях проверяемых функций задержки (VDF) [5, 6] и в гомоморфном шифровании [7].

Алгоритм, описанный в п. 3, имеет сложность  $\mathcal{O}(\lg \Delta_K \cdot 2^n \cdot \text{poly}(n))$ , где  $\Delta_K$  — дискриминант  $K$ . Таким образом, он является полиномиальным от степени расширения  $[K : \mathbb{Q}] = 2^n$  и имеет логарифмическую зависимость от дискриминанта поля. В основе работы лежат результаты [8], где представлены основные ингредиенты алгоритма.

### Результатами работы являются:

- Алгоритм вычисления образующих идеала Штикельбергера для мультикватратичных полей вида  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , где  $d_i \equiv 1 \pmod{4}$  свободны от квадратов и попарно взаимно просты. Наш алгоритм, во-первых, систематизирует идеи, описанные в [8]. Во-вторых, мы расширяем область действия алгоритма на поля с образующими  $d_i \equiv \pm 2 \pmod{8}$ .
- Эффективная реализация предлагаемого алгоритма.<sup>2</sup>

В п. 1 приведены определения, связанные с идеалом Штикельбергера, и описано, как с помощью гауссовых сумм мультикватратичное поле вкладывается в круговое. Пункты 2 и 3 посвящены алгоритму вычисления образующих идеала Штикельбергера и анализу его сложности. В п. 4 изучается связь идеала Штикельбергера с числом классов поля  $K$ .

Предварительные результаты данной работы были представлены на конференции SIBECRYPT'20 [9].

## 1. Предварительные сведения

### 1.1. Определение идеала Штикельбергера

Будем рассматривать мультикватратичные поля  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , где  $d_1, \dots, d_n \in \mathbb{Z}$  попарно взаимно просты и свободны от квадратов. Через  $\Delta_K$  обозначим дискриминант  $K$ . Для  $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$ , заданного взаимно простыми и свободными от квадратов образующими  $d_i$ , известно [10, Satz 2.1], что  $\Delta_K = (2^a \prod_i d_i)^{2^{n-1}}$ , где  $a \in \{0, 2, 3\}$ .

Рассмотрим башню числовых полей  $\mathbb{Q} \subseteq K \subseteq L$  и обозначим их группы Галуа  $G_L = \text{Gal}(L/\mathbb{Q})$  и  $G_K = \text{Gal}(K/\mathbb{Q})$ . Группу, конечно порождённую элементами из  $G_L$  над  $\mathbb{Q}$  (соответственно элементами  $G_K$  над  $\mathbb{Q}$ ), будем обозначать  $\mathbb{Q}[G_L] = \{\sum a_i \cdot \sigma_i : a_i \in \mathbb{Q}, \sigma_i \in G_L\}$  ( $\mathbb{Q}[G_K] = \{\sum a_j \cdot \sigma_j : a_j \in \mathbb{Q}, \sigma_j \in G_K\}$ ). Важными понятиями при вычислении элементов Штикельбергера являются отображения  $\text{res}$  и  $\text{cor}$ .

<sup>2</sup><https://gitlab.com/Denis01/stickelberger-ideal>

Определим их согласно [8, с. 157] для расширения числовых полей  $L/K$ :

$$\begin{aligned} \text{res}_{L/K} : \mathbb{Q}[G_L] &\rightarrow \mathbb{Q}[G_K], & \text{res}_{L/K} \left( \sum_{\sigma \in G_L} a_\sigma \sigma \right) &= \sum_{\sigma \in G_L} a_\sigma (\sigma|_K), \\ \text{cor}_{L/K} : \mathbb{Q}[G_K] &\rightarrow \mathbb{Q}[G_L], & \text{cor}_{L/K} \left( \sum_{\sigma \in G_K} a_\sigma \sigma \right) &= \sum_{\sigma \in G_L} a_{\sigma|_K} \sigma, \end{aligned}$$

где  $\sigma|_K$  — сужение автоморфизма  $\sigma \in G_L$  на поле  $K$ ;  $a_\sigma, a_{\sigma|_K}$  — коэффициенты, соответствующие автоморфизмам  $\sigma, \sigma|_K$ .

Дробную часть числа обозначим  $\langle \cdot \rangle$ ,  $0 \leq \langle \cdot \rangle < 1$ ; наибольший общий делитель двух элементов  $a, b \in \mathbb{Z}$  обозначим  $(a, b)$ ; символ Кронекера-Якоби для  $a, b$  (для нечетного  $b > 1$  — символ Якоби, для простого нечетного  $b$  — символ Лежандра) обозначим  $\left(\frac{a}{b}\right)$ ; для произвольного множества  $A$  его мощность будем обозначать  $\#A$ .

Дадим классические определения элемента и идеала Штикельберга [11, с. 189].

**Определение 1.** Для любого положительного целого  $r$ , любого  $\alpha \in \mathbb{Z}$  и кругового поля  $\mathbb{Q}(\zeta_r)$  определим

$$\theta_r(\alpha) = \sum_{(a,r)=1} \left\langle -\frac{\alpha a}{r} \right\rangle \sigma_a^{-1} \in \mathbb{Q}[G_{\mathbb{Q}(\zeta_r)}],$$

где  $0 < a \leq r$  и  $\sigma_a \in G_{\mathbb{Q}(\zeta_r)} = \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ .

**Определение 2.** Для любого положительного целого  $r$  и произвольного  $\alpha \in \mathbb{Z}$  элементом Штикельберга  $\theta'_r(\alpha)$  называется элемент вида

$$\theta'_r(\alpha) = (\text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_r)/K \cap \mathbb{Q}(\zeta_r)}) (\theta_r(\alpha)) \in \mathbb{Q}[G_K],$$

где  $K$  и  $\mathbb{Q}(\zeta_r)$  — абелево числовое поле и круговое поле соответственно.

**Определение 3.** Идеалом Штикельберга поля  $K$  называется идеал вида  $I = I' \cap \mathbb{Z}[G_K]$ , где

$$I' = \{\theta'_r(\alpha) : \alpha, r \in \mathbb{Z}, r \geq 1\}.$$

## 1.2. Квадратичные гауссовы суммы

Дадим определение квадратичных гауссовых сумм, а также покажем, как они связаны с автоморфизмами круговых полей, поскольку эта взаимосвязь поможет вычислить действие отображения  $\text{res}$ , и как следствие, элемент Штикельберга соответствующего числового поля.

**Определение 4.** Пусть  $m, k \in \mathbb{Z}$ ,  $k > 0$ . Квадратичная гауссова сумма определяется как  $g(m, k) = \sum_{b=0}^{k-1} e^{2\pi i m b^2 / k}$ .

Следующая теорема позволяет выражать квадратные корни, которые можно рассматривать как элементы мультикватратичного поля, через квадратичные гауссовы суммы.

**Теорема 1** [12, 1.5.2, с. 26]. Пусть  $(m, k) = 1$ ,  $k > 0$  и  $k$  — нечетное. Тогда

$$g(m, k) = \left(\frac{m}{k}\right) g(1, k) = \begin{cases} \left(\frac{m}{k}\right) \sqrt{k}, & k \equiv 1 \pmod{4}, \\ \left(\frac{m}{k}\right) i\sqrt{k}, & k \equiv 3 \pmod{4}. \end{cases}$$

Заметим, что если  $-k \equiv 1 \pmod{4}$ , то  $k \equiv 3 \pmod{4}$ . Отсюда следует, что в этом случае  $\sqrt{-k} = g(1, k)$  по теореме 1.

Рассмотрим действие автоморфизмов кругового поля  $\mathbb{Q}(\zeta_k)$  на корни  $\sqrt{k}$ , которое необходимо для вычисления отображения  $\text{res}$ . Всякий автоморфизм поля  $\mathbb{Q}(\zeta_k)$  имеет вид  $\sigma_a(e^{2\pi i/k}) = e^{2\pi i a/k}$ . В случае, когда  $k = p$  — нечётное простое и  $p \nmid a$ , согласно [12, (1.5.3), с. 26] имеем:

$$\sigma_a(g(1, p)) = \left(\frac{a}{p}\right) g(1, p) = \begin{cases} \left(\frac{a}{p}\right) \sqrt{p}, & p \equiv 1 \pmod{4}, \\ \left(\frac{a}{p}\right) \sqrt{-p}, & -p \equiv 1 \pmod{4}. \end{cases}$$

Отсюда следует, что  $\sigma_a(\sqrt{p}) = \left(\frac{a}{p}\right) \sqrt{p}$ , если  $p \equiv 1 \pmod{4}$ , и  $\sigma_a(\sqrt{-p}) = \left(\frac{a}{p}\right) \sqrt{-p}$ , если  $p \equiv 3 \pmod{4}$ .

Если  $k$  не является простым, для нахождения действия автоморфизма  $\sigma_a$  можно применить китайскую теорему об остатках [12, с. 43]. Пусть  $k = k_1 \cdot \dots \cdot k_s$ , где  $k_i$  — различные простые числа,  $M_i = k/k_i$ . Тогда

$$g(a, k) = g(aM_1, k_1) \cdot \dots \cdot g(aM_s, k_s).$$

По теореме 1 имеем

$$g(a, k) = \left(\frac{aM_1}{k_1}\right) \cdot \dots \cdot \left(\frac{aM_s}{k_s}\right) g(1, k_1) \cdot \dots \cdot g(1, k_s).$$

Таким образом, так как  $\sigma_a(g(1, k)) = g(a, k)$ , нахождение действия автоморфизма  $\sigma_a$  на  $g(1, k)$  в случае, когда  $k$  — не простое свободное от квадратов (хотя утверждение верно и в случае, если  $k_i$  — взаимно просты), сводится к определению его действия на все  $g(1, k_1), \dots, g(1, k_s)$ . Отсюда для  $(a, k) = 1$  следует:  $\sigma_a(\sqrt{k}) = \left(\frac{a}{k}\right) \sqrt{k}$ , если  $k \equiv 1 \pmod{4}$ , и  $\sigma_a(\sqrt{-k}) = \left(\frac{a}{k}\right) \sqrt{-k}$ , если  $k \equiv 3 \pmod{4}$ .

Рассмотрим поле  $K = \mathbb{Q}(\sqrt{d})$ , где  $d \equiv 2 \pmod{8}$  и  $d = 2p$ ,  $p$  — простое. Тогда  $g(1, d)$  имеет следующий вид:

$$g(1, d) = g(1, 8) g(1, p) = \sqrt{2} \cdot \sqrt{p} = \sqrt{2p} = \sqrt{d}.$$

### 1.3. Вложения числовых полей в круговые

По теореме Кронекера-Вебера [2, Chapter 14] любое абелево расширение  $K$  поля  $\mathbb{Q}$  вкладывается в  $\mathbb{Q}(\zeta_f)$  для некоторого  $f \in \mathbb{Z}$ ,  $f > 1$ . Кондуктором  $K$  называется минимальное такое  $f$  (мы используем определение из [13, с. 75]). Тогда, если  $f$  — кондуктор абелева числового поля  $K$ , то для положительного целого  $r$  справедливо:  $K \cap \mathbb{Q}(\zeta_r) = K \cap \mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_r) = K \cap \mathbb{Q}(\zeta_{(f,r)})$ .

Мультикватратичное поле является абелевым расширением поля рациональных чисел. Рассмотрим, как определяется кондуктор для мультикватратичного поля  $K$  в соответствии с [14, с. 159], [8, с. 140] и [15, с. 112]. Обозначим

$$d'_i = \begin{cases} |d_i|, & d_i \equiv 1 \pmod{4}, \\ 4|d_i|, & d_i \equiv 2, 3 \pmod{4}. \end{cases} \quad (1)$$

Тогда  $\mathbb{Q}(\sqrt{d_1}) \subset \mathbb{Q}(\zeta_{d'_1})$ ,  $\mathbb{Q}(\sqrt{d_2}) \subset \mathbb{Q}(\zeta_{d'_2})$ ,  $\dots$ ,  $\mathbb{Q}(\sqrt{d_n}) \subset \mathbb{Q}(\zeta_{d'_n})$ . Таким образом,  $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n}) \subset \mathbb{Q}(\zeta_{d'_1}) \dots \mathbb{Q}(\zeta_{d'_n}) = \mathbb{Q}(\zeta_{d'_1 \dots d'_n}) = \mathbb{Q}(\zeta_{\text{НОК}(d'_1, \dots, d'_n)})$  и соответственно кондуктор  $K$  равен  $\text{НОК}(d'_1, \dots, d'_n)$ .

Рассмотрим теперь отображение  $\text{res}_{\mathbb{Q}(\zeta_r)/K \cap \mathbb{Q}(\zeta_r)}$ . Возникают два вопроса: каким образом происходит сужение автоморфизмов кругового поля  $\mathbb{Q}(\zeta_r)$  на поле  $K \cap \mathbb{Q}(\zeta_r)$  и что есть пересечение  $K \cap \mathbb{Q}(\zeta_r)$ ?

Ответим на первый вопрос, определив сужение автоморфизмов кругового поля  $\mathbb{Q}(\zeta_r)$  сначала на круговые подполя, а затем с помощью гауссовых сумм – на мультикватратичные числовые поля. Рассмотрим случай, когда  $r = p \cdot q$ , где  $p, q > 0$  – взаимно простые. Произвольным образом выберем  $a$ , взаимно простое с  $p$  и  $q$ . Тогда автоморфизм  $\sigma_a : \zeta_{pq} \mapsto \zeta_{pq}^a$  поля  $\mathbb{Q}(\zeta_{pq})$  можно связать с действием автоморфизмов полей  $\mathbb{Q}(\zeta_p)$  и  $\mathbb{Q}(\zeta_q)$  на элементы  $\sqrt{\pm p}$  и  $\sqrt{\pm q}$  следующим образом:

$$\sigma_a(g(1, pq)) = g(a, pq) = \left(\frac{aq}{p}\right) g(1, p) \left(\frac{ap}{q}\right) g(1, q) = \begin{cases} \sigma_{aq}(\sqrt{p}) \sigma_{ap}(\sqrt{q}), & p, q \equiv 1, 1 \pmod{4}, \\ \sigma_{aq}(\sqrt{p}) \sigma_{ap}(\sqrt{-q}), & p, q \equiv 1, 3 \pmod{4}, \\ \sigma_{aq}(\sqrt{-p}) \sigma_{ap}(\sqrt{q}), & p, q \equiv 3, 1 \pmod{4}, \\ \sigma_{aq}(\sqrt{-p}) \sigma_{ap}(\sqrt{-q}), & p, q \equiv 3, 3 \pmod{4}. \end{cases}$$

Здесь индекс  $aq$  в случае  $\sigma_{aq}(\sqrt{\pm p})$  рассматривается по модулю  $p$ , а индекс  $ap$  в случае  $\sigma_{ap}(\sqrt{\pm q})$  рассматривается по модулю  $q$ .

Ответ на второй вопрос даёт следующая лемма.

**Лемма 1.** Пусть  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$  – мультикватратичное поле такое, что  $d_1, \dots, d_n$  попарно взаимно просты и свободны от квадратов,  $(i_1, \dots, i_\ell) \in \{1, \dots, n\}^\ell$  – набор из  $\ell$  индексов и  $d'_{i_1}, \dots, d'_{i_\ell}$  определены по формуле (1). Тогда

$$K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}}) = \mathbb{Q}(\sqrt{d_{i_1}}, \sqrt{d_{i_2}}, \dots, \sqrt{d_{i_\ell}}).$$

**Доказательство.** Заметим, что  $K_0 = \mathbb{Q}(\sqrt{d_{i_1}}, \sqrt{d_{i_2}}, \dots, \sqrt{d_{i_\ell}})$  – подполе  $K$ , имеющее кондуктор  $\text{НОК}(d'_{i_1}, \dots, d'_{i_\ell})$ . Поэтому оно содержится в  $\mathbb{Q}(\zeta_{\text{НОК}(d'_{i_1}, \dots, d'_{i_\ell})}) = \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}})$ , т.е. имеем включение  $K_0 \subset K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}})$ .

Обратное включение докажем от противного.

Положим, найдется  $\alpha \in K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}})$  такое, что  $\alpha \notin K_0$ . Любое  $\alpha \in K$  имеет вид  $\alpha = \sum_{j_1, \dots, j_n} a_{j_1, \dots, j_n} \sqrt{d_1}^{j_1} \cdot \dots \cdot \sqrt{d_n}^{j_n}$ . Из условия  $\alpha \notin K_0$  следует, что в сумме найдется слагаемое  $a_{j_1, \dots, j_n} \sqrt{d_1}^{j_1} \cdot \dots \cdot \sqrt{d_n}^{j_n}$ , содержащее  $\sqrt{d_k}$ ,  $k \notin \{i_1, \dots, i_\ell\}$ ,  $j_k \equiv 1 \pmod{2}$  и  $a_{j_1, \dots, j_k, \dots, j_n} \neq 0$ . При этом  $\sqrt{d_k} \in \mathbb{Q}(\zeta_{d'_k})$ . Так как все  $d_1, \dots, d_n$  попарно взаимно просты, имеем  $d'_k \nmid d'_{i_1} \cdot \dots \cdot d'_{i_\ell}$ , поэтому  $\mathbb{Q}(\zeta_{d'_k}) \not\subset \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}})$ . Из чего следует, что  $\alpha \notin \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}})$ . Получили противоречие, из которого следует, что  $K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}}) \subset K_0$ . ■

**Лемма 2.** Пусть  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$  – мультикватратичное поле такое, что  $d_1, \dots, d_n$  попарно взаимно просты и свободны от квадратов,  $f = d'_1 \cdot \dots \cdot d'_n$  – кондуктор поля  $K$ , где  $d'_i$  заданы в (1), и пусть  $r$  – целое положительное число такое, что  $r \mid f$ . Тогда  $r$  можно представить в виде  $r = t \cdot d'_{i_1} \cdot \dots \cdot d'_{i_\ell}$ , где  $\{i_1, \dots, i_\ell\}$  – множество всех индексов  $i$  таких, что  $d'_i \mid r$  и  $t$  – положительное целое. Кроме того,

$$K \cap \mathbb{Q}(\zeta_r) = \mathbb{Q}(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}}).$$

**Доказательство.** Так как  $d_1, \dots, d_n$  – взаимно просты, то  $f = \text{НОК}(d'_1, \dots, d'_n) = d'_1 \cdot \dots \cdot d'_n$ . Из чего следует представление  $r$ .

Пусть  $K_0 = \mathbb{Q}(\sqrt{d_{j_1}}, \dots, \sqrt{d_{j_{n-\ell}}})$ , где  $j_1, \dots, j_{n-\ell} \in \{1, \dots, n\} \setminus \{i_1, \dots, i_\ell\}$ , и  $K_1 = \mathbb{Q}(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}})$ . Тогда  $K = K_0 K_1 = K_0(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}}) = K_1(\sqrt{d_{j_1}}, \dots, \sqrt{d_{j_{n-\ell}}})$  – композит полей  $K_0$  и  $K_1$ .

Покажем, что  $K_0 \cap \mathbb{Q}(\zeta_r) = \mathbb{Q}$ . Если  $i \notin \{i_1, \dots, i_\ell\}$ , то  $\sqrt{d_i} \notin \mathbb{Q}(\zeta_r)$ , так как кондуктор  $d'_i$  поля  $\mathbb{Q}(\sqrt{d_i})$  не делит  $r$  и, соответственно,  $\mathbb{Q}(\sqrt{d_i}) \subseteq \mathbb{Q}(\zeta_{d'_i}) \not\subseteq \mathbb{Q}(\zeta_r)$ . Кроме того, кондукторы полей, образованных произведениями элементов  $\sqrt{d_i}$ , также не делят  $r$ , поэтому все такие произведения не лежат в  $\mathbb{Q}(\zeta_r)$ . Так как всевозможные произведения различных  $\sqrt{d_i}$  порождают поле  $K_0$  как  $\mathbb{Q}$ -векторное пространство [27, Th. 2.1], получаем  $K_0 \cap \mathbb{Q}(\zeta_r) = \mathbb{Q}$ .

Аналогичным образом можно показать, что  $\mathbb{Q}(\sqrt{d_i}) \subseteq \mathbb{Q}(\zeta_r)$  для  $i \in \{i_1, \dots, i_\ell\}$  и, как следствие,  $K_1 \subseteq K \cap \mathbb{Q}(\zeta_r)$ .

Таким образом пересечение  $K \cap \mathbb{Q}(\zeta_r)$  содержит поле  $K_1$  с кондуктором  $d'_{i_1} \dots d'_{i_\ell}$  и не содержит поле  $K_0$ . Так как кондукторы всех подполей  $\mathbb{Q}(\zeta_r)$  должны делить  $r$ , остаётся рассмотреть только поля с кондуктором-делителем  $t$ .

Рассмотрим мультикватратичные поля с кондуктором  $t_0$  – делителем  $t$ . Отметим, что число  $t$  делит кондуктор  $d'_{j_1} \dots d'_{j_{n-\ell}}$  поля  $K_0$ , причём  $d'_{j_k} \nmid t$ . Все мультикватратичные поля с кондуктором  $t_0 \mid t$  содержатся в  $\mathbb{Q}(\zeta_t) \subseteq \mathbb{Q}(\zeta_r)$ . Из условия  $K_0 \cap \mathbb{Q}(\zeta_r) = \mathbb{Q}$  следует, что  $K_0 \cap \mathbb{Q}(\zeta_t) = \mathbb{Q}$ . Из того, что  $\gcd(t, d'_{i_1} \dots d'_{i_\ell}) = 1$ , имеем  $K_1 \cap \mathbb{Q}(\zeta_t) = \mathbb{Q}$ .

Так как  $K$  – композит полей  $K_0$  и  $K_1$ , получаем  $K \cap \mathbb{Q}(\zeta_r) = K_1$ . ■

#### 1.4. Расширенное определение идеала Штикельбергера

Прежде чем приступить к детальному описанию вычисления элементов Штикельбергера, дадим альтернативные определения элементу и идеалу Штикельбергера, которые, во-первых, упростят вычисления, а во-вторых, позволят доказать их корректность.

**Определение 5.** Согласно [8], идеалом Штикельбергера поля  $K$  с кондуктором  $f$ , называется идеал вида  $I = I' \cap \mathbb{Z}[G_K]$ , где

$$I' = \{\theta'_r(\alpha) : r \mid f, \alpha \in \mathbb{Z}, \alpha < 0\} \cup \left\{ \frac{1}{2} N_K \right\}.$$

Пусть  $a \in \mathbb{Z}$ ,  $a \geq 1$  и  $(a, fr) = 1$ , где  $f$  – кондуктор числового поля  $K$ . Как и прежде, обозначим через  $\sigma_a \in G_{\mathbb{Q}(\zeta_{fr})}$  автоморфизм, ставящий в соответствие корню из единицы его  $a$ -ю степень. Тогда по определению

$$\theta'_r(a\alpha) = (\text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_r)/K \cap \mathbb{Q}(\zeta_r)}) (\theta_r(a\alpha)).$$

С другой стороны, исходя из определений отображений  $\text{res}$  и  $\sigma_a$ , можно записать  $\theta_r(a\alpha)$  следующим образом:

$$\theta_r(a\alpha) = \text{res}_{\mathbb{Q}(\zeta_{rf})/\mathbb{Q}(\zeta_r)} \sigma_a(\theta_r(\alpha)).$$

Окончательно имеем

$$\begin{aligned} \theta'_r(a\alpha) &= (\text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_r)/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_{rf})/\mathbb{Q}(\zeta_r)} \sigma_a) (\theta_r(\alpha)) = \\ &= (\text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_{rf})/K \cap \mathbb{Q}(\zeta_r)} \sigma_a) (\theta_r(\alpha)) = \\ &= (\text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_{rf})/K \cap \mathbb{Q}(\zeta_r)}) (\sigma_a) (\text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \circ \text{res}_{\mathbb{Q}(\zeta_{rf})/K \cap \mathbb{Q}(\zeta_r)}) (\theta_r(\alpha)) = \\ &= \sigma \theta'_r(\alpha), \end{aligned}$$

где  $\sigma$  – автоморфизм поля  $K$  согласно определениям  $\text{res}$  и  $\text{cor}$ . Полагая  $\alpha = -1$ , получаем, что элемент Штикельбергера имеет вид  $\theta'_r(-a) = \sigma \theta'_r(-1)$ , где  $\sigma \in G_K$ . Соответственно, можно переписать определение идеала Штикельбергера:

**Определение 6.** Идеалом Штикельбергера числового поля  $K$  с кондуктором  $f$ , называется идеал вида  $I = I' \cap \mathbb{Z}[G_K]$ , где

$$I' = \left\{ \sigma \cdot \theta'_r(-1) : r|f, \sigma \in G_K \right\} \cup \left\{ \frac{1}{2}N_K \right\}.$$

В случае мультикватратичного поля  $K$  и некоторых дополнительных ограничениях, определение можно упростить, как показано в следующей лемме.

**Лемма 3.** Пусть  $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$  – мультикватратичное поле такое, что  $d_i$  – свободны от квадратов и попарно взаимно просты. Тогда идеал Штикельбергера поля  $K$  имеет вид  $I = I' \cap \mathbb{Z}[G_K]$ , где

$$I' = \left\{ \sigma \cdot \theta'_r(-1) : r = d'_{i_1} \cdot \dots \cdot d'_{i_\ell}, (i_1, \dots, i_\ell) \subseteq \{1, \dots, n\}, \sigma \in G_K \right\} \cup \left\{ \frac{1}{2}N_K \right\}.$$

*Доказательство.* Согласно Определению 6 идеал  $I'$  состоит из элементов Штикельбергера, соответствующих всем делителям  $r$  кондуктора  $f$ . Пусть  $r = td_{i_1} \cdot \dots \cdot d_{i_\ell}$  как в Лемме 2, тогда нам достаточно показать, что  $\theta'_r(-1) = c\theta'_{\frac{r}{t}}(-1)$  для некоторого  $c \in \mathbb{Q}$ . В конце доказательства мы получим  $c = \phi(t)$ . Имеем

$$\theta'_r(-1) = \text{cor}_{K/K \cap \mathbb{Q}(\zeta_r)} \text{res}_{\mathbb{Q}(\zeta_r)/K \cap \mathbb{Q}(\zeta_r)}(\theta_r(-1))$$

и

$$\theta'_{\frac{r}{t}}(-1) = \text{cor}_{K/K \cap \mathbb{Q}(\zeta_{\frac{r}{t}})} \text{res}_{\mathbb{Q}(\zeta_{\frac{r}{t}})/K \cap \mathbb{Q}(\zeta_{\frac{r}{t}})}(\theta_{\frac{r}{t}}(-1)).$$

Применяя Лемму 2, получаем:

$$\theta'_r(-1) = \text{cor}_{K/\mathbb{Q}(\sqrt{d_{i_1}, \dots, d_{i_\ell}})} \text{res}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}(\sqrt{d_{i_1}, \dots, d_{i_\ell}})}(\theta_r(-1))$$

и

$$\theta'_{\frac{r}{t}}(-1) = \text{cor}_{K/\mathbb{Q}(\sqrt{d_{i_1}, \dots, d_{i_\ell}})} \text{res}_{\mathbb{Q}(\zeta_{\frac{r}{t}})/\mathbb{Q}(\sqrt{d_{i_1}, \dots, d_{i_\ell}})}(\theta_{\frac{r}{t}}(-1)).$$

Рассмотрим элемент

$$\theta_r(-1) = \sum_{(a,r)=1} \left\langle \frac{a}{r} \right\rangle \sigma_a^{-1} \in \mathbb{Q}[G_{\mathbb{Q}(\zeta_r)}]. \quad (2)$$

Группа Галуа  $G_{\mathbb{Q}(\zeta_r)}$  изоморфна  $(\mathbb{Z}/r\mathbb{Z})^\times$ , где  $a \bmod r$  соответствует автоморфизму  $\sigma_a : \zeta_r \mapsto \zeta_r^a$  [2, Th. 2.5]. Так как  $\gcd(t, \frac{r}{t}) = 1$ , то по китайской теореме об остатках имеем изморфизм  $(\mathbb{Z}/r\mathbb{Z})^\times \simeq (\mathbb{Z}/t\mathbb{Z})^\times \oplus (\mathbb{Z}/\frac{r}{t}\mathbb{Z})^\times$ . Поэтому

$$G_{\mathbb{Q}(\zeta_r)} \simeq \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}(\zeta_{\frac{r}{t}})) \oplus \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}(\zeta_t)), \quad (3)$$

и любой автоморфизм  $\sigma \in G_{\mathbb{Q}(\zeta_r)}$  можно единственным образом представить в виде  $\sigma = \rho \circ \tau$ , где  $\rho \in \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}(\zeta_{\frac{r}{t}}))$  и  $\tau \in \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}(\zeta_t))$ .

В явном виде изморфизм записывается следующим образом. По китайской теореме об остатках имеем  $a = b' \frac{r}{t} \left( \left( \frac{r}{t} \right)^{-1} \bmod t \right) + c' t \left( t^{-1} \bmod \frac{r}{t} \right)$  для некоторых  $b', c'$  таких, что  $(b', t) = 1, b' \in (\mathbb{Z}/t\mathbb{Z})^\times$  и  $(c', \frac{r}{t}) = 1, c' \in (\mathbb{Z}/\frac{r}{t}\mathbb{Z})^\times$ . Тогда

$$\sigma_a : \zeta_r \mapsto \zeta_r^a = \zeta_t^{b' \left( \left( \frac{r}{t} \right)^{-1} \bmod t \right)} \zeta_{\frac{r}{t}}^{c' \left( t^{-1} \bmod \frac{r}{t} \right)},$$

где мы используем равенства  $\zeta_r^{\frac{r}{t}} = \zeta_t$  и  $\zeta_r^t = \zeta_{\frac{r}{t}}$ . Заметим, что поля  $\mathbb{Q}(\zeta_t^{((\frac{r}{t})^{-1} \bmod t)})$  и  $\mathbb{Q}(\zeta_{\frac{r}{t}}^{(t^{-1} \bmod \frac{r}{t})})$  изоморфны полям  $\mathbb{Q}(\zeta_t)$  и  $\mathbb{Q}(\zeta_{\frac{r}{t}})$ , где изоморфизмы задаются отображениями  $\zeta_t \mapsto \zeta_t^{\frac{r}{t}}$  и  $\zeta_{\frac{r}{t}} \mapsto \zeta_{\frac{r}{t}}^t$ . Поэтому для каждой пары  $b', c'$  всегда существуют единственные  $b \in (\mathbb{Z}/t\mathbb{Z})^\times$ ,  $c \in (\mathbb{Z}/\frac{r}{t}\mathbb{Z})^\times$  такие, что  $b' = b \frac{r}{t} \bmod r$ ,  $\gcd(b, t) = 1$  и  $c' = ct \bmod r$ ,  $\gcd(c, \frac{r}{t}) = 1$ . Тогда мы можем записать  $\sigma_a$  в виде

$$\sigma_a : \zeta_r \mapsto \zeta_r^a = \zeta_r^{b(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t) + ct^2(t^{-1} \bmod \frac{r}{t})} = \zeta_t^{b\frac{r}{t}((\frac{r}{t})^{-1} \bmod t)} \zeta_{\frac{r}{t}}^{ct(t^{-1} \bmod \frac{r}{t})} = \zeta_t^b \zeta_{\frac{r}{t}}^c = \rho_b \circ \tau_c,$$

где  $\rho_b \in \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}(\zeta_{\frac{r}{t}}))$  и  $\tau_c \in \text{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}(\zeta_t))$  задаются следующим образом:

$$\rho_b : \zeta_r \mapsto \zeta_r^{b(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t) + t^2(t^{-1} \bmod \frac{r}{t})} = \zeta_r^{b(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t)} \zeta_r^{t^2(t^{-1} \bmod \frac{r}{t})} = \zeta_t^b \zeta_{\frac{r}{t}},$$

$$\tau_c : \zeta_r \mapsto \zeta_r^{(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t) + ct^2(t^{-1} \bmod \frac{r}{t})} = \zeta_r^{(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t)} \zeta_r^{ct^2(t^{-1} \bmod \frac{r}{t})} = \zeta_t \zeta_{\frac{r}{t}}^c.$$

Теперь, получив автоморфизмы в явном виде, выразим через них элемент  $\theta_r(-1)$ . Имеем

$$\theta_r(-1) = \sum_{(a,r)=1} \left\langle \frac{a}{r} \right\rangle \sigma_a^{-1} = \sum_{(c,\frac{r}{t})=1} \left( \sum_{(b,t)=1} \left\langle \frac{b(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t) + ct^2(t^{-1} \bmod \frac{r}{t})}{r} \right\rangle \rho_b^{-1} \right) \tau_c^{-1}.$$

Так как ограничение автоморфизма  $\rho_b^{-1}$  на поле  $K_1 = \mathbb{Q}(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}})$  равно  $id$ , получаем:

$$\text{res}_{\mathbb{Q}(\zeta_r)/K_1}(\theta_r(-1)) = \sum_{(c,\frac{r}{t})=1} \left( \sum_{(b,t)=1} \left\langle \frac{b(\frac{r}{t})^2((\frac{r}{t})^{-1} \bmod t) + ct^2(t^{-1} \bmod \frac{r}{t})}{r} \right\rangle \right) \tau_c^{-1}.$$

Так как мы перешли в подгруппу группы Галуа  $G_{\mathbb{Q}(\zeta_r)}$ , образованную автоморфизмом  $\tau_c$ , то значение множителя перед  $\tau_c$  можно рассматривать по модулю  $\frac{r}{t}$ . Тогда:

$$\begin{aligned} \text{res}_{\mathbb{Q}(\zeta_r)/K_1}(\theta_r(-1)) &= \sum_{(c,\frac{r}{t})=1} \left( \sum_{(b,t)=1} \left\langle \frac{ct^2(t^{-1} \bmod \frac{r}{t})}{r} \right\rangle \right) \tau_c^{-1} = \sum_{(c,\frac{r}{t})=1} \left( \sum_{(b,t)=1} \frac{ct}{r} \right) \tau_c^{-1} = \\ &= \phi(t) \sum_{(c,\frac{r}{t})=1} \left( \frac{ct}{r} \right) \tau_c^{-1} = \text{res}_{\mathbb{Q}(\zeta_r)/K_1}(\theta_{\frac{r}{t}}(-1)). \end{aligned}$$

В итоге получаем,  $\theta_r'(-1) = \phi(t)\theta_{\frac{r}{t}}'(-1)$ . ■

## 2. Метод вычисления элемента Штикельбергера

1) Рассмотрим  $K = \mathbb{Q}(\sqrt{d})$ , где  $d \equiv 1 \pmod{4}$ ,  $d > 0$ ,  $d$  свободно от квадратов. Вычислим элемент Штикельбергера для действительного квадратичного поля. Отметим, что предвычисления мы проводим в круговом поле  $\mathbb{Q}(\zeta_f)$ , где  $f = d - \text{кондуктор поля } K$ , согласно (1). Тогда

$$\theta_d'(-1) = \text{cor}_{K/K \cap \mathbb{Q}(\zeta_d)} \left( \text{res}_{\mathbb{Q}(\zeta_d)/K \cap \mathbb{Q}(\zeta_d)}(\theta_d(-1)) \right),$$

где  $\theta_d(-1) = \sum_{(a,d)=1} \left\langle \frac{a}{d} \right\rangle \sigma_a^{-1}$  и  $\sigma_a^{-1} \in \text{Gal}(\mathbb{Q}(\zeta_d))$ . Запишем более подробно  $\theta_d(-1)$ :

$$\begin{aligned} \theta_d(-1) &= \sum_{(a,d)=1} \left\langle \frac{a}{d} \right\rangle \sigma_a^{-1} = \frac{1}{d} \sigma_1^{-1} + \frac{2}{d} \sigma_2^{-1} + \dots + \frac{d-2}{d} \sigma_{d-2}^{-1} + \frac{d-1}{d} \sigma_{d-1}^{-1} = \\ &= \frac{1}{d} \sigma_1 + \frac{2}{d} \sigma_{\frac{1}{2} \bmod d} + \dots + \frac{d-2}{d} \sigma_{\frac{1}{d-2} \bmod d} + \frac{d-1}{d} \sigma_{\frac{1}{d-1} \bmod d} = \end{aligned}$$

или, переобозначив, получаем

$$= \frac{1}{d}\sigma_1 + \frac{2}{d}\sigma_b + \dots + \frac{d-2}{d}\sigma_{-b \bmod d} + \frac{d-1}{d}\sigma_{-1 \bmod d}. \quad (4)$$

Важно отметить, что при дробях с противоположными по модулю  $d$  числителями фигурируют автоморфизмы с противоположными по модулю  $d$  индексами. Напомним, что вычисляя отображение  $\text{res}$ , мы, по сути, вычисляем символ Кронекера-Якоби  $\left(\frac{i}{d}\right)$ , сопоставляя автоморфизму кругового поля  $\sigma_i$  автоморфизм кватратичного поля  $id$  в случае  $\left(\frac{i}{d}\right) = 1$ , или автоморфизм  $\sigma : \sqrt{d} \mapsto -\sqrt{d}$ , если  $\left(\frac{i}{d}\right) = -1$ . Рассмотрим пары  $\frac{1}{d}\sigma_1$  и  $\frac{d-1}{d}\sigma_{-1 \bmod d}$ ,  $\frac{2}{d}\sigma_b$  и  $\frac{d-2}{d}\sigma_{-b \bmod d}$ , и т.д. из разложения (4):

$$\left(\frac{1}{d}\right) = 1 \text{ и } \left(\frac{-1}{d}\right) = 1, \text{ поскольку } d \equiv 1 \pmod{4}.$$

Это означает, что  $\sigma_1$  и  $\sigma_{-1 \bmod d}$  соответствуют одному и тому же автоморфизму поля  $K$  и  $\frac{1}{d} + \frac{d-1}{d} = 1$ . Аналогично,

$$\left(\frac{b}{d}\right) \equiv b^{(d-1)/2} \pmod{d} \text{ и } \left(\frac{-b}{d}\right) = \left(\frac{-1}{d}\right) \left(\frac{b}{d}\right) \equiv b^{(d-1)/2} \pmod{d}, \text{ поскольку } d \equiv 1 \pmod{4}.$$

Это снова означает, что  $\sigma_b$  и  $\sigma_{-b \bmod d}$  соответствуют одному и тому же автоморфизму поля  $K$  и  $\frac{2}{d} + \frac{d-2}{d} = 1$ . То же и для оставшихся пар. Тогда

$$\theta_d(-1) = \frac{1}{2} \sum_{a \bmod d} \sigma_a,$$

согласно определению  $I'$  идеала Штикельбергера числового поля  $K$  и по определению нормы получаем  $\theta_d(-1) = \frac{1}{2}N_K$ .

Отметим, что

$$\sum_{\substack{i=1 \\ i \in \mathbb{Z}_d^\times}}^{d-1} \chi(i) = 0,$$

где  $\chi(i) = \left(\frac{i}{d}\right)$  – характер Дирихле по модулю  $d$ , определяемый символом Якоби  $\left(\frac{i}{d}\right)$ . Учитывая, что число характеров по модулю  $d$  равно  $\varphi(d)$ , и значение  $\varphi(d)$  – четно, то число символов Якоби, равных  $-1$ , совпадает с числом символов Якоби, равных  $1$ , и, соответственно, равно  $\varphi(d)/2$ , где  $\varphi$  – функция Эйлера, в итоге получаем

$$\theta'_d(-1) = \frac{\varphi(d)}{4}(id + \sigma) = \frac{\varphi(d)}{4}N_{K/\mathbb{Q}}.$$

Для составного  $d = p_1 \cdot p_2$ , где  $p_1, p_2$  – простые числа, в силу мультипликативности функции Эйлера имеем  $4|(p_1 - 1) \cdot (p_2 - 1) = \varphi(p_1) \cdot \varphi(p_2) = \varphi(d)$ . Это условие распространяется и на большее число множителей  $d$ . Тогда  $\varphi(d)/4 \in \mathbb{Z}$ .

- 2) Рассмотрим теперь  $K = \mathbb{Q}(\sqrt{-d})$ , где  $d > 0$  и  $-d \equiv 1 \pmod{4}$ . Запишем элемент Штикельбергера

$$\theta_d(-1) = \sum_{(a,d)=1} \left\langle \frac{a}{d} \right\rangle \sigma_a^{-1} = \sum_{a \in (\mathbb{Z}_d)^\times} \frac{a}{d} \sigma_a^{-1} = u \cdot id + v \cdot \sigma.$$

Докажем, что  $u, v \in \mathbb{Z}$ . Согласно определению отображения  $\text{res}$ ,

$$\sigma_a^{-1}|_K = id \Leftrightarrow \left( \frac{a}{d} \right) = 1, \quad \sigma_a^{-1}|_K = \sigma \Leftrightarrow \left( \frac{a}{d} \right) = -1.$$

Тогда

$$u = \sum_{\substack{a=1 \\ \left(\frac{a}{d}\right)=1}}^d \frac{a}{d}, \quad v = \sum_{\substack{a=1 \\ \left(\frac{a}{d}\right)=-1}}^d \frac{a}{d}. \quad (5)$$

Как уже было отмечено выше, для элементов из  $(\mathbb{Z}_d)^\times$  число символов Якоби, равных  $-1$ , равно числу символов Якоби, равных  $1$ . Имеем

$$\begin{aligned} \sum_{\left(\frac{b}{d}\right)=1} b &= \sum_{\substack{k=1 \\ \left(\frac{\alpha}{d}\right)=1}}^{\varphi(d)/2} \alpha^k = \alpha^2 + \alpha^3 + \dots + \alpha^{\varphi(d)/2+1} = \\ &= \alpha^2(1 + \alpha + \dots + \alpha^{\varphi(d)/2-1}) = \alpha^2 \sum_{\left(\frac{b}{d}\right)=1} b. \end{aligned}$$

Заметим, что такой  $\alpha \in \mathbb{Z}_d^\times$  всегда будет существовать, так как для  $d = p_1 \cdot p_2 \cdot \dots \cdot p_s$  справедливо  $\mathbb{Z}_d^\times \cong \mathbb{Z}_{p_1}^\times \oplus \mathbb{Z}_{p_2}^\times \oplus \dots \oplus \mathbb{Z}_{p_s}^\times$  — циклическая в силу взаимной попарной простоты  $p_1, p_2, \dots, p_s$ . Следовательно, поскольку  $\alpha^2 \neq 1$ , то

$$\sum_{\left(\frac{b}{d}\right)=1} b \equiv 0 \pmod{d}.$$

Соответственно,  $u = \sum_{\left(\frac{a}{d}\right)=1} \frac{a}{d} \in \mathbb{Z}$ .

Отсюда следует, что

$$d(u + v) = \sum_{\substack{a=1 \\ (a,d)=1}}^d a = \frac{\varphi(d)}{2} d,$$

откуда, учитывая, что  $\varphi(d)/2$  — целое в силу разложения  $d = p_1 \cdot \dots \cdot p_n$ , где  $p_i$  — различные простые, получаем

$$v = \varphi(d)/2 - u \in \mathbb{Z}.$$

Отметим также, что применение отображения  $\text{cor}$  не изменяет целостность коэффициентов при автоморфизмах.

Теперь рассмотрим случай, когда  $d$  — простое. Покажем, что тогда вычисление значений в (5) можно значительно ускорить.

При  $d \equiv 1 \pmod{4}$  значения  $u$  и  $v$  легко получить, не вычисляя суммы уравнений (5). Запишем  $d = 4k + 1$ ,  $k \in \mathbb{Z}$ . Если  $a \in \mathbb{Z}_d^\times$  — квадратичный вычет, то  $-a$  также является квадратичным вычетом в  $\mathbb{Z}_d^\times$ , и существует всего  $(d-1)/2$  квадратичных вычетов. Получаем  $(d-1)/4$  пар вычетов, сумма элементов каждой пары равна  $d$ .

Отсюда сумма всех квадратичных вычетов равна  $d(d-1)/4 = d \cdot k$ , а значит,  $u = k$ . Следовательно,  $v = \varphi(d)/2 - u = \varphi(d)/2 - k$ .

Очевидно, эти рассуждения не переносятся на случай  $d = 4k + 3$ ,  $k \in \mathbb{Z}$ . Однако и здесь можно ускорить вычисления по формулам (5), используя результат [16]: если  $d \equiv 3 \pmod{8}$ , то  $v = dv'$ , где  $v'$  — сумма всех квадратичных невычетов по модулю  $d$ , меньших  $d/2$ , а если  $d \equiv 7 \pmod{8}$ , то  $v = \frac{1}{3} \left( dv' + \binom{d}{2} \right)$ . Таким образом, вычисления  $v$  ускоряются в два раза.

- 3) Рассмотрим  $K = \mathbb{Q}(\sqrt{d})$ , где  $d \equiv \pm 2 \pmod{8}$ , и  $d$  может быть как положительным, так и отрицательным, но свободным от квадратов. В зависимости от знака мы получаем вид элемента Штикельбергера, соответствующий одному из предыдущих случаев. Очевидно, что  $|d|$  имеет вид  $|2p|$ , где  $p$  — нечётное. Кроме того,  $\sqrt{2}$  соответствует  $\zeta_8$ , а  $\sqrt{p}$  соответствует  $\zeta_p$ . Согласно теории круговых полей, композит  $\mathbb{Q}(\zeta_8)\mathbb{Q}(\zeta_p)$  есть  $\mathbb{Q}(\zeta_{\text{НОК}(8,p)}) = \mathbb{Q}(\zeta_{8p}) = \mathbb{Q}(\zeta_{4d})$ , откуда кондуктор поля равен  $4|d| = 8|p|$ . Тогда

$$\theta_{4|d|}(-1) = \frac{1}{4|d|} \sum_{k=1}^{4|d|-1} k \cdot \sigma_k^{-1}(\zeta_{4|d|}),$$

где  $(k, 4|d|) = 1$ . При этом

$$\sigma_k^{-1}(\zeta_{4|d|}) = \sigma_{k \frac{4|d|}{8} \pmod{8}}(\zeta_8) \sigma_{k \cdot 8 \pmod{\frac{4|d|}{8}}} \left( \zeta_{\frac{4|d|}{8}} \right).$$

Если  $\left( \frac{8}{k \frac{4|d|}{8} \pmod{8}} \right) \left( \frac{k \cdot 8 \pmod{\frac{4|d|}{8}}}{\frac{4|d|}{8}} \right) = 1$ , то действие автоморфизма  $\sigma_k^{-1}$  кругового поля  $\mathbb{Q}(\zeta_{4|d|})$  на  $\zeta_{4|d|}$  соответствует действию автоморфизма  $id$  числового

поля  $K$  на элемент  $\sqrt{d}$ . Если  $\left( \frac{8}{k \frac{4|d|}{8} \pmod{8}} \right) \left( \frac{k \cdot 8 \pmod{\frac{4|d|}{8}}}{\frac{4|d|}{8}} \right) = -1$ , то действие

автоморфизма  $\sigma_k^{-1}$  кругового поля  $\mathbb{Q}(\zeta_{4|d|})$  на  $\zeta_{4|d|}$  соответствует действию автоморфизма  $\sigma$  числового поля  $K$  на элемент  $\sqrt{d}$ .

Обобщение на мультикватратичный случай аналогично предыдущим случаям, поскольку  $d_i \equiv \pm 2 \pmod{8}$  в записи  $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$  фигурирует лишь в одной позиции.

**Замечание 1.** Рассмотрим поле  $K = \mathbb{Q}(\sqrt{2})$ . Из рассуждений в п. 3 следует, что кондуктор данного поля равен 8. Тогда

$$\begin{aligned} \theta_8(-1) &= \frac{1}{8} \sum_{k=1}^7 k \sigma_k^{-1}(\zeta_8) = \frac{1}{8} (\sigma_1^{-1}(\zeta_8) + 3 \sigma_3^{-1}(\zeta_8) + 5 \sigma_5^{-1}(\zeta_8) + 7 \sigma_7^{-1}(\zeta_8)) = \\ &= \frac{1}{8} (\sigma_1(\zeta_8) + 3 \sigma_3(\zeta_8) + 5 \sigma_5(\zeta_8) + 7 \sigma_7(\zeta_8)). \end{aligned}$$

Вычислим символы Кронекера-Якоби. Поскольку  $\left( \frac{8}{1} \right) = 1$ , действие автоморфизма  $\sigma_1^{-1}$  на  $\zeta_8$  соответствует действию автоморфизма  $id$  на элемент  $\sqrt{2}$ ;  $\left( \frac{8}{3} \right) = -1$ , поэтому действие автоморфизма  $\sigma_3^{-1}$  на  $\zeta_8$  соответствует действию автоморфизма  $\sigma$  на элемент  $\sqrt{2}$ . Аналогично рассуждаем для  $\left( \frac{8}{5} \right) = -1$ ,  $\left( \frac{8}{7} \right) = 1$ . Таким образом,

получаем

$$\theta_8(-1) = \frac{1}{8} (id + 3\sigma + 5\sigma + 7id) = id + \sigma.$$

- 4) Обобщим рассмотренные случаи на произвольное биквадратичное поле. Пусть  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ , где  $d_1 \equiv 2 \pmod{8}$  и  $d_1 < 0$ , а  $d_2 \equiv 1 \pmod{4}$  и  $d_2 > 0$ ,  $d_1, d_2$  свободны от квадратов. В соответствии с п. 1 и 3, кондуктор числового поля  $K$  равен  $4|d_1|d_2$ . Тогда

$$\theta'_{4|d_1|d_2}(-1) = \text{cor}_{K/K \cap \mathbb{Q}(\zeta_{4|d_1|d_2})} \left( \text{res}_{\mathbb{Q}(\zeta_{4|d_1|d_2})/K \cap \mathbb{Q}(\zeta_{4|d_1|d_2})} (\theta_{4|d_1|d_2}(-1)) \right),$$

где

$$\theta_{4|d_1|d_2}(-1) = \frac{1}{4|d_1|d_2} \sum_{k=1}^{4|d_1|d_2-1} k \sigma_k^{-1}(\zeta_{4|d_1|d_2}), \quad (k, 4|d_1|d_2) = 1.$$

Рассмотрим отдельно  $\sigma_k^{-1}(\zeta_{4|d_1|d_2})$ :

$$\begin{aligned} \sigma_k^{-1}(\zeta_{4|d_1|d_2}) &= \sigma_{k \cdot d_2 \pmod{4|d_1|}}^{-1}(\zeta_{4|d_1|}) \sigma_{k \cdot 4|d_1| \pmod{d_2}}^{-1}(\zeta_{d_2}) = \\ &= \sigma_{(k \cdot d_2 \pmod{4|d_1|}) \frac{4|d_1|}{8} \pmod{8}}(\zeta_8) \sigma_{(k \cdot d_2 \pmod{4|d_1|}) 8 \pmod{\frac{4|d_1|}{8}}}(\zeta_{\frac{4|d_1|}{8}}) \sigma_{(1/(k \cdot 4|d_1| \pmod{d_2})) \pmod{d_2}}(\zeta_{d_2}). \end{aligned}$$

Далее действуем в соответствии с п. 1 и 3. Рассмотрим

$$\sigma_{(k \cdot d_2 \pmod{4|d_1|}) \frac{4|d_1|}{8} \pmod{8}}(\zeta_8) \sigma_{(k \cdot d_2 \pmod{4|d_1|}) 8 \pmod{\frac{4|d_1|}{8}}}(\zeta_{\frac{4|d_1|}{8}}).$$

Если  $\left( \frac{8}{(k \cdot d_2 \pmod{4|d_1|}) \frac{4|d_1|}{8} \pmod{8}} \right) \left( \frac{(k \cdot d_2 \pmod{4|d_1|}) 8 \pmod{\frac{4|d_1|}{8}}}{\frac{4|d_1|}{8}} \right) = 1$ , то действие автоморфизма  $\sigma_{k \cdot d_2 \pmod{4|d_1|}}^{-1}$  на  $\zeta_{4|d_1|}$  соответствует действию автоморфизма  $id_1$  на элемент  $\sqrt{d_1}$ . Если  $\left( \frac{8}{(k \cdot d_2 \pmod{4|d_1|}) \frac{4|d_1|}{8} \pmod{8}} \right) \left( \frac{(k \cdot d_2 \pmod{4|d_1|}) 8 \pmod{\frac{4|d_1|}{8}}}{\frac{4|d_1|}{8}} \right) = -1$ , то действие автоморфизма  $\sigma_{k \cdot d_2 \pmod{4|d_1|}}^{-1}$  на  $\zeta_{4|d_1|}$  соответствует действию автоморфизма  $\sigma_1$  на  $\sqrt{d_1}$ .

Рассмотрим  $\sigma_{(1/(k \cdot 4|d_1| \pmod{d_2})) \pmod{d_2}}(\zeta_{d_2})$ . Вычислим символ Кронекера-Якоби  $\left( \frac{(1/(k \cdot 4|d_1| \pmod{d_2})) \pmod{d_2}}{d_2} \right)$ . Если он равен 1, то действие автоморфизма  $\sigma_{k \cdot 4|d_1| \pmod{d_2}}^{-1}$  на  $\zeta_{d_2}$  соответствует действию автоморфизма  $id_2$  на элемент  $\sqrt{d_2}$ . Если он равен  $-1$ , то действие автоморфизма  $\sigma_{k \cdot 4|d_1| \pmod{d_2}}^{-1}$  на  $\zeta_{d_2}$  соответствует действию автоморфизма  $\sigma_2$  на элемент  $\sqrt{d_2}$ . В итоге получим комбинации произведений автоморфизмов  $id_1, id_2, \sigma_1, \sigma_2$ , где каждая соответствует одному из автоморфизмов  $\tau_i$  поля  $K$ . Аналогичным образом вычисляются  $\theta_f(-1)$  для мультикватратичных полей.

### 3. Алгоритм

Рассмотрим подробно алгоритм вычисления идеала Штикельбергера для мультикватратичных полей в соответствии с описанной теорией. Заметим, что согласно Лемме 3 при взаимно простых  $d_i$  для нахождения идеала Штикельбергера, достаточно ограничиться делителями кондуктора, составленными из произведений  $d_i'$ .

#### 3.1. Вычисление действий отображений $\text{res}$ и $\text{cor}$

**I. Вычисление  $\text{res}$ .** Рассмотрим алгоритм для вычисления  $\text{res}_{\mathbb{Q}(\zeta_f)/K \cap \mathbb{Q}(\zeta_f)}(\theta_f(-1))$ , где  $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$  и  $f$  – кондуктор  $K$ . Значения  $\text{res}_{\mathbb{Q}(\zeta_r)/K \cap \mathbb{Q}(\zeta_r)}(\theta_r(-1))$  для  $r \mid f$

можно найти по тому же алгоритму положив  $f = r$ ,  $n = \ell$  и  $d_1 = d_{i_1}, \dots, d_\ell = d_{i_\ell}$ , для  $\ell, i_1, \dots, i_\ell$  как в Лемме 2.

Если одно из  $d_i \equiv \pm 2 \pmod{8}$ , то алгоритм вычисляет

$$\text{res}_{\mathbb{Q}(\zeta_{4d'_1 \dots |d_i| \dots d'_n})/K \cap \mathbb{Q}(\zeta_{4d'_1 \dots |d_i| \dots d'_n})}(\theta_{4d'_1 \dots |d_i| \dots d'_n}(-1)),$$

где

$$\theta_{4d'_1 \dots |d_i| \dots d'_n}(-1) = \frac{1}{4d'_1 \cdot \dots \cdot |d_i| \cdot \dots \cdot d'_n} \sum_{k=1}^{4d'_1 \dots |d_i| \dots d'_n - 1} k \cdot \sigma_k^{-1}(\zeta_{4d'_1 \dots |d_i| \dots d'_n})$$

и  $(k, 4d'_1 \cdot \dots \cdot |d_i| \cdot \dots \cdot d'_n) = 1$ .

В противном случае, алгоритм вычисляет

$$\text{res}_{\mathbb{Q}(\zeta_{d'_1 \dots d'_n})/K \cap \mathbb{Q}(\zeta_{d'_1 \dots d'_n})} \theta_{d'_1 \dots d'_n}(-1),$$

где

$$\theta_{d'_1 \dots d'_n}(-1) = \sum_{(a, d'_1 \dots d'_n) = 1} \left\langle \frac{a}{d'_1 \cdot \dots \cdot d'_n} \right\rangle \sigma_a^{-1}.$$

Результатами вычисления  $\theta_{4d'_1 \dots |d_i| \dots d'_n}(-1)$  или  $\theta_{d'_1 \dots d'_n}(-1)$  будут комбинации автоморфизмов, которые обозначим

$$\begin{aligned} id_1 \cdot id_2 \cdot \dots \cdot id_n &= id : \sqrt{d_1} + \dots + \sqrt{d_n} \rightarrow \sqrt{d_1} + \sqrt{d_2} + \dots + \sqrt{d_n}, \\ &\dots \\ \sigma_1 \cdot \dots \cdot \sigma_{n-1} \cdot \sigma_n &= \tau_m : \sqrt{d_1} + \dots + \sqrt{d_{n-1}} + \sqrt{d_n} \rightarrow -\sqrt{d_1} - \dots - \sqrt{d_n}. \end{aligned} \tag{6}$$

Псевдокод процедуры вычисления  $\text{res}$  представлен в Алгоритме 1.

**Алгоритм 1.** Вычисление  $\text{res}_{\mathbb{Q}(\zeta_f)/K \cap \mathbb{Q}(\zeta_f)}(\theta_f(-1))$ 

**Вход:**  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , где  $d_i \equiv 1 \pmod{4}$  для всех  $i \in \{1, \dots, n\}$ , или  $d_j \equiv \pm 2 \pmod{8}$  для некоторого  $j \in \{1, \dots, n\}$ ;  $d_i$  свободны от квадратов и взаимно просты.

**Выход:**  $\text{res}(\theta_f(-1))$ .

- 1:  $f := \prod_{j=1}^n d'_j$ . //  $f$  — кондуктор  $K$
- 2: **Для**  $a \in \mathbb{Z}_f^\times$ :
- 3:  $\sigma_a := 1$ .
- 4: **Для**  $j = 1, \dots, n$ :
- 5:   **Если**  $d_j = 2 \pmod{8}$ , **то**
- 6:      $i_1 := a(4 \cdot |d_j|/8) \pmod{8}$ ;
- 7:      $i_2 := a \cdot 8 \pmod{4 \cdot |d_j|/8}$ .
- 8:   **Если**  $\binom{8}{i_1} \binom{i_2}{\frac{4 \cdot |d_j|}{8}} = 1$ , **то**
- 9:      $\sigma_a^{-1} := \sigma_a^{-1} \cdot id_j$ , //  $id_j$  — тождественный в  $\mathbb{Q}(\sqrt{d_j})$
- 10:   **иначе**
- 11:      $\sigma_a^{-1} := \sigma_a^{-1} \cdot \sigma_j$ , //  $\sigma_j$  — сопряжение в  $\mathbb{Q}(\sqrt{d_j})$
- 12:   **иначе**
- 13:      $t := \frac{a \cdot d'_1 \cdot \dots \cdot d'_n}{d'_j} \pmod{d'_j}$ ,  $i := \frac{1}{t} \pmod{d'_j}$ .
- 14:   **Если**  $\binom{i}{d'_j} = 1$ , **то**
- 15:      $\sigma_a^{-1} := \sigma_a^{-1} \cdot id_j$ , //  $id_j$  — тождественный в  $\mathbb{Q}(\sqrt{d_j})$
- 16:   **иначе**
- 17:      $\sigma_a^{-1} := \sigma_a^{-1} \cdot \sigma_j$ . //  $\sigma_j$  — сопряжение в  $\mathbb{Q}(\sqrt{d_j})$
- 18:    $\sigma_a^{-1} := \frac{a}{f} \cdot \sigma_a^{-1}$ .
- 19:  $\theta := \sum_{a \in \mathbb{Z}_f^*} \sigma_a^{-1}$ .
- 20: **res** := (заменить получившиеся комбинации автоморфизмов в каждом слагаемом  $\theta$  на соответствующие  $\tau_i$  согласно формулам (6)).
- 21: **Вернуть** **res**.

**II. Вычисление  $\text{cor}$ .** Автоморфизмы, полученные после вычисления **res**, являются автоморфизмами поля  $K \cap \mathbb{Q}(\zeta_{d'_1 \dots d'_n})$  (или  $K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}})$  для  $r \mid f$  и  $\ell, i_1, \dots, i_\ell$  как в Лемме 2). Вычисление действия отображения **cor** представляет собой переход от этих автоморфизмов к автоморфизмам поля  $K$ . Обозначим автоморфизмы поля  $K$  следующим образом: сопоставим действие автоморфизма  $\rho_i$  с бинарным вектором из  $\mathbb{Z}_2^n$ , причём если  $j$ -я координата вектора (считая слева направо) есть 1, то  $\rho_i : \sqrt{d_j} \rightarrow -\sqrt{d_j}$  (например,  $\rho_1 : \sqrt{d_1} + \dots + \sqrt{d_n} \rightarrow \sqrt{d_1} + \dots - \sqrt{d_n}$ ).

Если  $K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}}) = K$ , то отображение **cor** действует тождественно (автоморфизмы  $\tau_i$  совпадают с  $\rho_i$ ). Отметим, что такой случай возникает при вычислении  $\theta'_{d'_1 \dots d'_n}(-1)$ . А как быть, если мы вычисляем, например, элемент Штикельбергера вида  $\theta'_{d'_{i_1} \dots d'_{i_\ell}}(-1)$ , где  $\ell < n$ ? Положим  $K \cap \mathbb{Q}(\zeta_{d'_{i_1} \dots d'_{i_\ell}}) = \mathbb{Q}(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}})$ . Результатом

действия отображения  $\text{res}$  в этом случае будет

$$a_1 \cdot id_\ell + a_2 \cdot \tau_1 + \dots + a_{2^\ell-1} \cdot \tau_{2^\ell-2} + a_{2^\ell} \cdot \tau_{2^\ell-1},$$

где  $id_\ell, \tau_i$  — автоморфизмы поля  $\mathbb{Q}(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}})$ ,  $i = 1, \dots, 2^\ell - 1$ . Нумерация автоморфизмов  $\tau_i$  аналогична нумерации автоморфизмов  $\rho_i$ .

Далее переходим от перечисленных автоморфизмов поля  $\mathbb{Q}(\sqrt{d_{i_1}}, \dots, \sqrt{d_{i_\ell}})$  к автоморфизмам  $\rho_i$  поля  $K$ . Если  $\rho_i$  относительно элемента  $\sqrt{d_{i_1}} + \dots + \sqrt{d_{i_\ell}}$  действует как  $id_\ell$ , то все такие автоморфизмы  $\rho_i$  участвуют в записи элемента Штикельбергера с коэффициентом  $a_1$ . Аналогично, если  $\rho_i$  относительно  $\sqrt{d_{i_1}} + \dots + \sqrt{d_{i_\ell}}$  действует как  $\tau_1$ , то все такие автоморфизмы  $\rho_i$  участвуют в записи элемента Штикельбергера с коэффициентом  $a_2$ . Применяя аналогичный подход для всех остальных случаев, получаем что, в общем случае элемент Штикельбергера примет следующий вид:

$$\theta'_r(-1) = c_0 \cdot id + c_1 \cdot \rho_1 + \dots + c_{m-1} \cdot \rho_{m-1} + c_m \cdot \rho_m,$$

где  $c_i \in \mathbb{Z}$  для  $i = 0, \dots, m$  и  $m = 2^n - 1$ .

Общее количество элементов Штикельбергера в поле  $K$  равно  $2^n - 1$ . Количество различных комбинаций зависит от количества разных коэффициентов в элементе Штикельбергера. Будем записывать все различные комбинации в множество  $I'$  (алгоритм 2) мощности  $\#I'$ .

---

### Алгоритм 2. Вычисление идеала Штикельбергера

---

**Вход:**  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ , где  $d_i \equiv 1 \pmod{4}$  для всех  $i \in \{1, \dots, n\}$ , или некоторый  $d_j \equiv \pm 2 \pmod{8}$ ,  $j \in \{1, \dots, n\}$ ;  $d_i$  свободны от квадратов и взаимно просты.

**Выход:** Выход:  $I = I' \cap \mathbb{Z}[\text{Gal}(K/\mathbb{Q})]$ .

- 1:  $A :=$  массив, индексирующий подполя  $K$  вида  $\mathbb{Q}(\{\sqrt{d_i}\}_{i \in J})$ , для всех непустых подмножеств  $J \subseteq \{1, \dots, n\}$ .
  - 2: Для  $i = 1, \dots, 2^n - 1$ :
  - 3:  $r := d'_{i_1} \cdot \dots \cdot d'_{i_\ell}$ , где  $i_1, \dots, i_\ell = A[i]$ .
  - 4:  $\text{res}_i := \text{res}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}(\sqrt{d_{i_1}}, \sqrt{d_{i_2}}, \dots, \sqrt{d_{i_\ell}})} \theta_r(-1)$ ; // Алгоритм 1
  - 5:  $\gamma_i \leftarrow \text{cor}_{K/\mathbb{Q}(\sqrt{d_{i_1}}, \sqrt{d_{i_2}}, \dots, \sqrt{d_{i_\ell}})} \text{res}_i$ .
  - 6:  $I' := \emptyset$ .
  - 7: Для  $i = 1, \dots, 2^n - 1$ :
  - 8: Для  $j = 0, \dots, 2^n - 1$ :
  - 9:  $t := \rho_j \cdot \gamma_i$ .
  - 10: Если  $t \notin I'$  то
  - 11:  $I' := I' \cup \{t\}$ .
  - 12: Вернуть  $I$ .
- 

### 3.2. Сложность алгоритма

**Теорема 2.** Получив на вход поле  $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$ , где  $d_i \equiv 1 \pmod{4}$  для всех  $i \in \{1, \dots, n\}$ , или некоторый  $d_j \equiv \pm 2 \pmod{8}$ ,  $j \in \{1, \dots, n\}$ ;  $d_i$  свободны от квадратов и взаимно просты, Алгоритм 2, возвращает образующие идеала Штикельбергера поля  $K$  за время

$$T = \mathcal{O}(\lg \Delta_K \cdot 2^n \cdot \text{poly}(n)).$$

В частности, если  $d_i$  — первые  $n$  простых чисел, сложность Алгоритма 2 равна

$$T = \mathcal{O}(e^{n \log(n)} \cdot 2^{2n} \cdot n^4 \cdot \text{poly} \log(n)).$$

**Доказательство.** Поскольку Алгоритм 1 является частью Алгоритма 2, рассмотрим сначала его вычислительную сложность. На вход Алгоритма 1 подаётся  $\ell$ -квадратичное поле  $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_\ell})$  ( $d_1 = d_{i_1}, \dots, d_\ell = d_{i_\ell}$  во входных данных алгоритма) и на шаге 1 вычисляется произведение всех  $d'_j$ ,  $j \leq \ell$ . Для взаимно простых  $d'_i$  имеем  $\prod_i d'_i = \mathcal{O}(\lg \Delta_K / 2^n)$ . В случае, когда  $d'_i$  — первые из  $\ell$  простых чисел ( $\ell$ -е простое оценивается  $\approx \ell \log(\ell)$ ), получаем  $f = \prod d'_i = e^{\ell \log(\ell)}$ . В доказательстве дальше рассматриваем именно этот случай.

Рассмотрим цикл на шаге 2. Он повторяется  $\varphi(f)$  раз, это значит, что его оценка  $\mathcal{O}(f) = \mathcal{O}(e^{\ell \log(\ell)})$ . В теле цикла выполняются шаги 4–10 либо 11–17. Рассмотрим сначала шаги 4–10. Оценка шага 5 не влияет на максимальную сложность. На шаге 6 производятся вычисления по модулю  $d_j$ . В худшем случае наибольшая образующая сравнима с  $2 \pmod 8$ , тогда  $d = \max_j d'_j$ . Таким образом, сложность шага 6 равна  $\mathcal{O}(\log^3(d))$ . Аналогично для шагов 7 и 9, где также производятся вычисления по модулю  $d'_j$ . Далее выполняется либо шаг 7, либо шаг 9, а оценки шагов 8 и 10 не влияют на максимальную сложность. Таким образом, сложность одной итерации внутреннего цикла для случая  $d_j \equiv 2 \pmod 8$  равна  $\mathcal{O}(\log^3(d))$ . Аналогично рассуждаем для шагов 11–17. Шаги 12, 13, 14 и 16 представляют собой вычисления по модулю  $d'_j$ . Оценка каждого из них равна  $\mathcal{O}(\log^3(d))$ . В цикле выполняется либо шаг 14, либо шаг 16, а шаги 15 и 17 имеют сложность  $\mathcal{O}(1)$ . Таким образом, сложность одной итерации внутреннего цикла для всех остальных случаев равна  $\mathcal{O}(\log^3(d))$ . Во внешнем цикле также выполняется шаг 18, чья сложность равна  $\mathcal{O}(\log^3(f)) = \mathcal{O}(\log^3(e^{\ell \log(\ell)})) = \mathcal{O}(\ell^3 \cdot \log^3(\ell))$ . Оценка шага 19 не влияет на максимальную сложность, а замена на шаге 20 имеет сложность  $\mathcal{O}(2^\ell)$ , поскольку мы имеем  $2^\ell$  автоморфизмов. Обобщая, получаем, что общая сложность Алгоритма 1 равна

$$\mathcal{O}(e^{\ell \log(\ell)} \cdot \ell^4 \cdot \log^3(d) \cdot \log^3(\ell) + 2^\ell).$$

Поскольку функция  $e^{\ell \log(\ell)}$  возрастает быстрее, чем  $2^\ell$ , итоговая сложность Алгоритма 1 имеет вид

$$\mathcal{O}(e^{\ell \log(\ell)} \cdot \ell^4 \cdot \log^3(d) \cdot \log^3(\ell)).$$

Вернёмся к Алгоритму 2. Ему на вход мы подаём  $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ . Рассмотрим цикл на шаге 2. Он повторяется  $2^n - 1$  раз. На шаге 4 в теле цикла вычисляется результат отображения  $\text{res}$ , а значит, используется алгоритм 1. Поскольку на входе  $n$ -квадратичное поле и в худшем случае в цикл попадёт именно оно, то сложность шага 4 примет вид  $\mathcal{O}(e^{n \log(n)} \cdot n^4 \cdot \log^3(d) \cdot \log^3(n))$ . На шаге 5 осуществляется переход к автоморфизмам поля  $K$ , сложность равна  $\mathcal{O}(2^n)$  (по количеству автоморфизмов). Таким образом, общая сложность этого цикла равна  $\mathcal{O}(e^{n \log(n)} \cdot n^4 \cdot \log^3(d) \cdot \log^3(n) \cdot 2^{2n})$ . Циклы на шагах 7 и 8 повторяются  $2^n - 1$  и  $2^n$  раз соответственно, но осуществляемые в теле внутреннего цикла операции имеют сложность  $\mathcal{O}(1)$ . Таким образом, общая сложность этих циклов равна  $\mathcal{O}(2^{2n})$ .

Окончательно общая сложность Алгоритма 2 равна

$$\mathcal{O}(e^{n \log(n)} \cdot n^4 \cdot \log^3(d) \cdot \log^3(n) \cdot 2^{2n} + 2^{2n}).$$

Упростив, получим  $\mathcal{O}(e^{n \log(n)} \cdot n^4 \cdot \log^3(d) \cdot \log^3(n) \cdot 2^{2n})$ . ■

### 3.3. Пример

Проиллюстрируем вычисление элемента и идеала Штикельбергера в случае трикватричного поля  $K = \mathbb{Q}(\sqrt{-7}, \sqrt{10}, \sqrt{13})$ . Имеем:  $-7 \equiv 1 \pmod 4$ ,  $10 \equiv 2 \pmod 8$ ,

$13 \equiv 1 \pmod{4}$ . Выпишем все подполя исходного поля  $K$ :

$$\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{13}), \mathbb{Q}(\sqrt{-7}, \sqrt{10}), \mathbb{Q}(\sqrt{-7}, \sqrt{13}), \mathbb{Q}(\sqrt{10}, \sqrt{13}), \mathbb{Q}(\sqrt{-7}, \sqrt{10}, \sqrt{13}).$$

Вычислим элементы Штикельбергера, соответствующие каждому из подполей:

$$\begin{aligned} \theta'_7(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_7)} \left( \text{res}_{\mathbb{Q}(\zeta_7)/K\cap\mathbb{Q}(\zeta_7)}(\theta_7(-1)) \right) = \\ &= id + \rho_1 + \rho_2 + \rho_3 + 2\rho_4 + 2\rho_5 + 2\rho_6 + 2\rho_7, \\ \theta'_{40}(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_{40})} \left( \text{res}_{\mathbb{Q}(\zeta_{40})/K\cap\mathbb{Q}(\zeta_{40})}(\theta_{40}(-1)) \right) = \\ &= 4id + 4\rho_1 + 4\rho_2 + 4\rho_3 + 4\rho_4 + 4\rho_5 + 4\rho_6 + 4\rho_7, \\ \theta'_{13}(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_{13})} \left( \text{res}_{\mathbb{Q}(\zeta_{13})/K\cap\mathbb{Q}(\zeta_{13})}(\theta_{13}(-1)) \right) = \\ &= 3id + 3\rho_1 + 3\rho_2 + 3\rho_3 + 3\rho_4 + 3\rho_5 + 3\rho_6 + 3\rho_7, \\ \theta'_{91}(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_{91})} \left( \text{res}_{\mathbb{Q}(\zeta_{91})/K\cap\mathbb{Q}(\zeta_{91})}(\theta_{91}(-1)) \right) = \\ &= 9id + 10\rho_1 + 9\rho_2 + 10\rho_3 + 9\rho_4 + 8\rho_5 + 9\rho_6 + 8\rho_7, \\ \theta'_{280}(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_{280})} \left( \text{res}_{\mathbb{Q}(\zeta_{280})/K\cap\mathbb{Q}(\zeta_{280})}(\theta_{280}(-1)) \right) = \\ &= 11id + 11\rho_1 + 13\rho_2 + 13\rho_3 + 13\rho_4 + 13\rho_5 + 11\rho_6 + 11\rho_7, \\ \theta'_{520}(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_{520})} \left( \text{res}_{\mathbb{Q}(\zeta_{520})/K\cap\mathbb{Q}(\zeta_{520})}(\theta_{520}(-1)) \right) = \\ &= 24id + 24\rho_1 + 24\rho_2 + 24\rho_3 + 24\rho_4 + 24\rho_5 + 24\rho_6 + 24\rho_7, \\ \theta'_{3640}(-1) &= \text{cor}_{K/K\cap\mathbb{Q}(\zeta_{3640})} \left( \text{res}_{\mathbb{Q}(\zeta_{3640})/K\cap\mathbb{Q}(\zeta_{3640})}(\theta_{3640}(-1)) \right) = \\ &= 71id + 75\rho_1 + 73\rho_2 + 69\rho_3 + 73\rho_4 + 69\rho_5 + 71\rho_6 + 75\rho_7, \end{aligned}$$

где  $\rho_i$  — автоморфизмы поля  $K$ . Идеал Штикельбергера в соответствии с определением 6 примет вид (полагаем, что столбцы матрицы соответствуют автоморфизмам  $G_K$ , а строки — образующим идеала):

$$I = \begin{pmatrix} 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 11 & 11 & 13 & 13 & 13 & 13 & 11 & 11 \\ 13 & 13 & 11 & 11 & 11 & 11 & 13 & 13 \\ 9 & 10 & 9 & 10 & 9 & 8 & 9 & 8 \\ 10 & 9 & 10 & 9 & 8 & 9 & 8 & 9 \\ 9 & 8 & 9 & 8 & 9 & 10 & 9 & 10 \\ 8 & 9 & 8 & 9 & 10 & 9 & 10 & 9 \\ 24 & 24 & 24 & 24 & 24 & 24 & 24 & 24 \\ 71 & 75 & 73 & 69 & 73 & 69 & 71 & 75 \\ 75 & 71 & 69 & 73 & 69 & 73 & 75 & 71 \\ 73 & 69 & 71 & 75 & 71 & 75 & 73 & 69 \\ 69 & 73 & 75 & 71 & 75 & 71 & 69 & 73 \end{pmatrix}.$$

#### 4. Вычисление группы классов мультикватратичных полей

В заключение покажем, как идеал Штикельбергера связан с числом группы классов мультикватратичного поля. Через  $Cl_K$  будем обозначать группу классов числового поля  $K$  с кольцом целых  $O_K$ , то есть фактор-группу  $\mathcal{I}/\mathcal{P}$ , где  $\mathcal{I}$  — мультипликативная группа дробных идеалов  $O_K$ ;  $\mathcal{P}$  — группа главных идеалов  $O_K$ . Группа классов  $Cl_K$  конечна, её размер называется числом классов и обозначается  $h_K$ . Вычисление  $Cl_K$  или

её размера  $h_K$  — одна из фундаментальных задач алгоритмической теории чисел [17]. Из теоремы Брауера — Зигеля [18, 19] известно, что асимптотически  $h_K \sim \frac{1}{2} \sqrt{|\Delta_K|}$ , где  $\Delta_K$  — дискриминант  $K$ .

Наиболее быстрые из известных алгоритмов вычисления  $Cl_K$  для произвольного поля  $K$  основаны на методе исчисления индексов [20, 21] и работают за время, субэкспоненциальное от  $\Delta_K$ . Для некоторых полей существуют специальные алгоритмы, в частности, для мультикватратичных предложен метод [22], значительно ускоряющий вычисление  $Cl_K$ .

Задача вычисления  $Cl_K$  и  $h_K$  более интересна в случае мнимых полей. Для действительных полей гипотеза Коэна — Ленстры [23] утверждает, что большая часть действительных квадратичных полей является областью главных идеалов (то есть  $Cl_K$  тривиальна). В [24] гипотеза расширена на поля больших степеней. Кроме того, для действительных полей идеал Штикельбергера тривиален [2, с. 94], поэтому сосредоточимся на мнимых полях.

**Мнимое квадратичное поле.** Рассмотрим  $K = \mathbb{Q}(\sqrt{d})$ ,  $d < 0$ ,  $d$  свободно от квадратов. Для произвольного  $d$  алгоритм Хафнера — МакКёрли [20] вычисляет  $Cl_K$  за время  $e^{\mathcal{O}(\sqrt{\ln|d| \cdot \ln \ln |d|})}$ .

П. Шмид в [25, док-во теоремы 2] показал, что  $h_K = 2v - \varphi(d)/2$ , где  $v$  — сумма квадратичных невычетов в  $(\mathbb{Z}_d)^\times$ . Таким образом, зная  $\theta_d(-1)$ , мы знаем  $h_K$ . Для произвольного  $d$  вычисление значений  $u, v$  по формулам (5) займут  $\mathcal{O}(d)$  времени, что уступает в асимптотике алгоритму Хафнера — МакКёрли. Однако, как показано в п. 2, для простого  $d$ , такого, что  $|d| \equiv 1 \pmod{4}$ , значения  $u, v$ , а значит, и  $h_K$ , можно вычислить за время  $\text{poly} \log(d)$ .

Совсем недавно мнимые квадратичные поля были предложены для эффективных конструкций так называемых *проверяемых функций задержки* (verifiable delay functions) [5, 6], которые, например, активно использует блокчейн Chia<sup>3</sup>. Для обеспечения должного уровня безопасности при генерации большого  $d$  алгоритм должен проверять, выполняется ли  $|d| \equiv 1 \pmod{4}$ . Для  $|d| \equiv 3 \pmod{4}$  остаётся открытым вопрос, для каких значений  $d$  алгоритм Хафнера — МакКёрли работает быстрее на практике, чем непосредственное вычисление  $u, v$  по формулам (5). Отметим, что вычисления сумм в (5) тривиально распараллеливаются, что даёт значительное практическое преимущество этому наивному методу относительно алгоритма Хафнера — МакКёрли.

**Мнимые бикватратичное и мультикватратичные поля.** Положим теперь  $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ ,  $d_i < 0$ ,  $d_i$  свободны от квадратов и взаимно просты. Поле  $K$  содержит 3 квадратичных подполя: два мнимых  $k_1 = \mathbb{Q}(\sqrt{d_1})$ ,  $k_2 = \mathbb{Q}(\sqrt{d_2})$  и одно действительное  $k_3 = \mathbb{Q}(\sqrt{d_1 d_2})$ . Т. Кубота в [26, Satz 5] доказал, что  $h_K = \frac{q(K/\mathbb{Q})}{2} h_{k_1} h_{k_2} h_{k_3}$ , где  $q(K/\mathbb{Q}) = [U_K : U_{k_1} U_{k_2} U_{k_3}]$  — индекс единиц поля  $K$  (то есть степень расширения  $U_K$  — группы единиц поля  $K$  — над группой  $U_{k_1} U_{k_2} U_{k_3}$ , порождённой образующими групп единиц подполей  $k_i$ ). Этот индекс для мультикватратичных полей можно получить за время  $\text{poly} \log(\Delta_K)$  с помощью алгоритма Бауха и др. [27]. Исходя из рассуждений выше, можно посчитать число классов мнимых подполей  $h_{k_1}, h_{k_2}$ , получив тем самым  $h_K$  с точностью до множителя  $h_{k_3}$ . Вычислению  $h_{k_3}$  — числа группы классов действительных квадратичных полей — посвящены работы [28, 29]. В продолжение эвристики Коэна — Ленстры в [30] показано, что  $h_{k_3}$  с большой вероятностью не делит-

<sup>3</sup><https://www.chia.net/>

ся на малые простые, а в [31, 32] приведены случаи, когда  $h_{k_3} \in \{1, 2\}$ . Отметим, что идеал Штикельбергера для действительных квадратичных полей (см. случай 3 в п. 2) не даёт информации о числе группы классов.

Формула Куботы обобщается до мультикватратичного случая. Из [33, 34] известно, что для  $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$  справедлива формула  $h_K = \frac{1}{2^\nu} q(K/\mathbb{Q}) \prod_i h(k_i)$ , где  $\nu = (n-1)(2^{n-2}-1) + 2^{n-1} - 1$ , а произведение по  $k_i$  пробегает все  $2^{n-1}$  квадратичных подполя  $K$ . В работе [35] классифицированы всевозможные значения  $q(K/\mathbb{Q})$ . Таким образом, при вычислении  $h_K$  для мультикватратичного поля ключевое значение играет алгоритм, вычисляющий группу классов квадратичного поля, а эта задача алгоритмически эквивалентна вычислению идеала Штикельбергера для мнимых полей. Классификация мультикватратичных полей с числом классов 1 представлена в [36].

**Открытые вопросы.** Было бы интересно расширить полученные результаты в следующих (прямо противоположных друг другу) направлениях: 1) ускорения алгоритма вычисления идеала Штикельбергера; 2) приложение мультикватратичных полей к конструкциям функций с задержкой с эффективной верификацией, как полей, число группы классов которых трудно вычислить на практике.

#### ЛИТЕРАТУРА

1. *Stickelberger L.* Über eine Verallgemeinerung der Kreistheilung // *Math. Ann.* 1890. vol. 37, no. 3, pp. 312–367.
2. *Washington L. C.* Introduction to cyclotomic fields. Springer, 1997.
3. *Denomme R.* A History of Stickelberger’s Theorem, <https://core.ac.uk/download/pdf/159568254.pdf> — The Ohio State University. 2009.
4. *Cramer R., Ducas L., Wesolowski B.* Short Stickelberger Class Relations and Application to Ideal-SVP // *Advances in Cryptology – EUROCRYPT 2017*, pp. 324–348.
5. *Wesolowski B.* Efficient verifiable delay functions // *Advances in Cryptology – EUROCRYPT 2019*, Springer, pp. 379–407.
6. *Pietrzak K.* Simple verifiable delay functions // *Innovations in Theoretical Computer Science Conference, ITCS, 2019*. pp. 1–60.
7. *Pedrouzo-Ulloa A., Troncoso-Pastoriza J. R., Gama N., Georgieva M., Pérez-González F.* Revisiting Multivariate Ring Learning with Errors and its Applications on Lattice-based Cryptography // *IACR Cryptol. ePrint Arch.* 2019/1109.
8. *Kučera R.* On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields // *Journal of number theory.* 1996. vol. 56. no. 1. pp. 139–166.
9. *Олефиренко Д., Куршанова Е., Малыгина Е., Новоселов С.*, Алгоритм вычисления элемента Штикельбергера для мнимых мультикватратичных полей // *Прикладная дискретная математика. Приложение.* № 13, 2020.
10. *Schmal B.* Diskriminanten,  $\mathbb{Z}$ -anzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern // *Archiv der Mathematik.* 1989. vol. 52, no. 3, pp. 245–257.
11. *Sinnott W.* On the Stickelberger Ideal and the Circular Units of an Abelian Field // *Inventiones Mathematicae.* 1980. vol. 62. pp. 181–234.
12. *Berndt B. C., Evans R. J., Williams K. S.* Gauss and Jacobi sums. // New York: Wiley, 1998.
13. *Lang S.* Cyclotomic Fields I and II. New York: Springer, 1990.
14. *Milne J.* Class field theory (v4.03). 2020. [www.jmilne.org/math/](http://www.jmilne.org/math/)
15. *Weintraub S.* Galois Theory. Second Edition. Springer, 2009.
16. *Aebi C., Cairns G.* Sums of quadratic residues and nonresidues // arXiv:1512.00896. 2015.
17. *Cohen H.* A Course in Computational Algebraic Number Theory. Springer-Verlag, 1995.

18. *Brauer R.* On the Zeta-Function of Algebraic Number Fields // American Journal of Mathematics. 1947. vol. 69, no. 2. pp. 243–250.
19. *Siegel C. L.* Über die Classenzahl quadratischer Zahlkörper // Acta Arithmetica. 1935. vol. 1, no. 1. pp. 83–86.
20. *Hafner J. L., McCurley K. S.* A rigorous subexponential algorithm for computation of class groups // J. Amer. Math. Soc. 1989. vol. 2, no 4, pp. 837–850.
21. *Buchmann J.* A subexponential algorithm for the determination of class groups and regulators of algebraic number fields // Séminaire de Théorie des Nombres (Paris 1988/1989), Progr. Math., no. 91, Birkhäuser, Boston, 1990, pp. 27–41.
22. *Biasse J.-F., Van Vredendaal C.* Fast multiquadratic S-unit computation and application to the calculation of class groups // ANTS XIII, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, 2019, pp. 103–118.
23. *Cohen H., Lenstra H. W.* Heuristics on class groups of number fields // Number Theory Noordwijkerhout. Lecture Notes in Mathematics. 1983, vol. 1068, pp. 33–62.
24. *Cohen H., Martinet J.* Class groups of number fields: numerical heuristics // Math. Comp. 1987. vol. 48, no. 177, pp. 123–137.
25. *Schmid P.* The Stickelberger element of an imaginary quadratic field // Acta Arithmetica. 1999, vol. 91. no. 2. pp. 165–169.
26. *Kubota T.* Über den bizyklischen biquadratischen Zahlkörper // Nagoya Math. J. 1956. no. 10, pp. 65–85.
27. *Bauch J., Bernstein D. J., de Valence H., Lange T., van Vredendaal C.* Short Generators Without Quantum Computers: The Case of Multiquadratics // Advances in Cryptology – EUROCRYPT 2017, pp. 27–59.
28. *Bhand A., Ram Murty M.* Class numbers of quadratic fields // Hardy-Ramanujan Journal. 2019, vol. 42. pp. 1–9.
29. *Sato H.* On class number formula for the real quadratic fields // Proc. Japan Acad. Ser. A Math. Sci. 2004. vol. 80, no. 7, pp. 129–130.
30. *Ono K.* Indivisibility of Class Numbers of Real Quadratic Fields // Compositio Mathematica. 1999. vol. 119, pp. 1–11.
31. *Mollin R., Williams H.* On a determination of real quadratic fields of class number one and related continues fraction period length less than 25 // Proc. Japan Acad. Ser. A Math. Sci. 1991. vol. 67. pp. 20–25.
32. *Mollin R., Williams H.* On Real Quadratic Fields of Class Number Two // Mathematics of Computation. 1992. vol. 59, no. 200, pp. 625–632.
33. *Kuroda H.* Über die Klassenzahlen algebraischer Zahlkörper // Nagoya Math. J. 1950. vol. 1, pp. 1–10.
34. *Herglotz G.* Über einen Dirichletschen Satz // Mathematische Zeitschrift. 1922. vol. 12, no. 1, pp. 255–261.
35. *Benjamin E., Lemmermeyer F., Snyder C.* On the unit group of some multiquadratic number fields // Pacific Journal of Mathematics. 2007. vol. 230. pp. 27–40.
36. *Feaver A.* Imaginary multiquadratic fields of class number 1 // Journal of Number Theory. 2017. vol. 174, pp. 93–117.

#### REFERENCES

1. *Stickelberger L.* Über eine Verallgemeinerung der Kreistheilung // Math. Ann. 1890. vol. 37, no. 3, pp. 312–367.
2. *Washington L. C.* Introduction to cyclotomic fields. Springer, 1997.

3. *Denomme R.* A History of Stickelberger's Theorem, <https://core.ac.uk/download/pdf/159568254.pdf> — The Ohio State University. 2009.
4. *Cramer R., Ducas L., Wesolowski B.* Short Stickelberger Class Relations and Application to Ideal-SVP // *Advances in Cryptology – EUROCRYPT 2017*, pp. 324–348.
5. *Wesolowski B.* Efficient verifiable delay functions // *Advances in Cryptology – EUROCRYPT 2019*, Springer, pp. 379–407.
6. *Pietrzak K.* Simple verifiable delay functions // *Innovations in Theoretical Computer Science Conference, ITCS, 2019*. pp. 1–60.
7. *Pedrouzo-Ulloa A., Troncoso-Pastoriza J. R., Gama N., Georgieva M., Pérez-González F.* Revisiting Multivariate Ring Learning with Errors and its Applications on Lattice-based Cryptography // *IACR Cryptol. ePrint Arch.* 2019/1109.
8. *Kučera R.* On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields // *Journal of number theory.* 1996. vol. 56. no. 1. pp. 139–166.
9. *Olefirenko D., O., Kirshanova E. A., Malygina E. S., Novoselov S. A.,* An algorithm for computing the Stickelberger elements for imaginary multiquadratic fields // *Applied Discrete Mathematics. Supplement.* 2020. no. 13, pp. 12–17.
10. *Schmal B.* Diskriminanten,  $\mathbb{Z}$ -anzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern // *Archiv der Mathematik.* 1989. vol. 52, no. 3, pp. 245–257.
11. *Sinnott W.* On the Stickelberger Ideal and the Circular Units of an Abelian Field // *Inventiones Mathematicae.* 1980. vol. 62. pp. 181–234.
12. *Berndt B. C., Evans R. J., Williams K. S.* Gauss and Jacobi sums. // New York: Wiley, 1998.
13. *Lang S.* Cyclotomic Fields I and II. New York: Springer, 1990.
14. *Milne J.* Class field theory (v4.03). 2020. [www.jmilne.org/math/](http://www.jmilne.org/math/)
15. *Weintraub S.* Galois Theory. Second Edition. Springer, 2009.
16. *Aebi C., Cairns G.* Sums of quadratic residues and nonresidues // arXiv:1512.00896. 2015.
17. *Cohen H.* A Course in Computational Algebraic Number Theory. Springer-Verlag, 1995.
18. *Brauer R.* On the Zeta-Function of Algebraic Number Fields // *American Journal of Mathematics.* 1947. vol. 69, no. 2. pp. 243–250.
19. *Siegel C. L.* Über die Classenzahl quadratischer Zahlkörper // *Acta Arithmetica.* 1935. vol. 1, no. 1. pp. 83–86.
20. *Hafner J. L., McCurley K. S.* A rigorous subexponential algorithm for computation of class groups // *J. Amer. Math. Soc.* 1989. vol. 2, no 4, pp. 837–850.
21. *Buchmann J.* A subexponential algorithm for the determination of class groups and regulators of algebraic number fields // *Séminaire de Théorie des Nombres (Paris 1988/1989)*, Progr. Math., no. 91, Birkhäuser, Boston, 1990, pp. 27–41.
22. *Biasse J.-F., Van Vredendaal C.* Fast multiquadratic S-unit computation and application to the calculation of class groups // *ANTS XIII, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, 2019*, pp. 103–118.
23. *Cohen H., Lenstra H. W.* Heuristics on class groups of number fields // *Number Theory Noordwijkerhout. Lecture Notes in Mathematics.* 1983, vol. 1068, pp. 33–62.
24. *Cohen H., Martinet J.* Class groups of number fields: numerical heuristics // *Math. Comp.* 1987. vol. 48, no. 177, pp. 123–137.
25. *Schmid P.* The Stickelberger element of an imaginary quadratic field // *Acta Arithmetica.* 1999, vol. 91. no. 2. pp. 165–169.
26. *Kubota T.* Über den bzyklischen biquadratischen Zahlkörper // *Nagoya Math. J.* 1956. no. 10, pp. 65–85.

27. *Bauch J., Bernstein D. J., de Valence H., Lange T., van Vredendaal C.* Short Generators Without Quantum Computers: The Case of Multiquadratics // Advances in Cryptology – EUROCRYPT 2017, pp. 27–59.
28. *Bhand A., Ram Murty M.* Class numbers of quadratic fields // Hardy-Ramanujan Journal. vol. 42, 2019, pp. 1–9.
29. *Sato H.* On class number formula for the real quadratic fields // Proc. Japan Acad. Ser. A Math. Sci. 2004. vol. 80, no. 7, pp. 129–130.
30. *Ono K.* Indivisibility of Class Numbers of Real Quadratic Fields // Compositio Mathematica. 1999. vol. 119, pp. 1–11.
31. *Mollin R., Williams H.* On a determination of real quadratic fields of class number one and related continued fraction period length less than 25 // Proc. Japan Acad. Ser. A Math. Sci. 1991. vol. 67. pp. 20–25.
32. *Mollin R., Williams H.* On Real Quadratic Fields of Class Number Two // Mathematics of Computation. 1992. vol. 59, no. 200, pp. 625–632.
33. *Kuroda H.* Über die Klassenzahlen algebraischer Zahlkörper // Nagoya Math. J. 1950. vol. 1, pp. 1–10.
34. *Herglotz G.* Über einen Dirichletschen Satz // Mathematische Zeitschrift. 1922. vol. 12, no. 1, pp. 255–261.
35. *Benjamin E., Lemmermeyer F., Snyder C.* On the unit group of some multiquadratic number fields // Pacific Journal of Mathematics. 2007. vol. 230. pp. 27–40.
36. *Feaver A.* Imaginary multiquadratic fields of class number 1 // Journal of Number Theory. 2017. vol. 174, pp. 93–117.

**КИРШАНОВА Елена Алексеевна** — PhD, доцент ИФМНиИТ, и. о. зав. лаборатории “Мат. методы защиты и обработки информации”, БФУ им. И.Канта, Калининград. E-mail: [ekirshanova@kantiana.ru](mailto:ekirshanova@kantiana.ru)

**МАЛЫГИНА Екатерина Сергеевна** — кандидат физ.-мат. наук, доцент ИФМНиИТ, м.н.с. лаборатории “Мат. методы защиты и обработки информации”, БФУ им. И.Канта, Калининград. E-mail: [emalygina@kantiana.ru](mailto:emalygina@kantiana.ru)

**НОВОСЕЛОВ Семен Александрович** — старший преподаватель ИФМНиИТ, м.н.с. лаборатории “Мат. методы защиты и обработки информации”, БФУ им. И.Канта, Калининград. E-mail: [snovoselov@kantiana.ru](mailto:snovoselov@kantiana.ru)

**ОЛЕФИРЕНКО Денис Олегович** — аспирант ИФМНиИТ БФУ им. И.Канта, Калининград. E-mail: [dolefrenko@kantiana.ru](mailto:dolefrenko@kantiana.ru)