Алгоритм вычисления элемента Штикельбергера для мнимых мультиквадратичных полей

Денис Олефиренко, Елена Киршанова, Екатерина Малыгина, Семён Новосёлов

Аннотация

В нашей статье мы представляем алгоритм вычисления идеала Штикельбергера для мультиквадратичного поля $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 \pmod 4$ и d_i попарно взаимно просты. В основу работы положена статья Кучеры [Journal of number theory 56, 1996]. Мы алгоритмизируем идеи, описанные в этой статье, доказываем корректность полученных алгоритмов и анализируем их сложность. Интересно, что для $2^n = [K : \mathbb{Q}]$, наш алгоритм работает за время $\widetilde{\mathcal{O}}(2^n)$. Мы полагаем, что полученный результат будет полезен для решения криптоаналитических задач поиска короткого вектора в идеалах мультиквадратичных полей.

In this paper we present an algorithm for computing the Stickelberger ideal for multiquadratic fields $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, where $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 \pmod 4$ and d_i pair-wise co-prime. Our result is based on the work of Kucera [Journal of number theory 56, 1996]. We systematize the ideas of this work, present them in the shape of algorithms, prove correctness of the obtained algorithms and analyze their complexity. Interestingly, for $2^n = [K : \mathbb{Q}]$ our algorithm works in time $\widetilde{\mathcal{O}}(2^n)$. We hope that the obtained results will serve are the first step towards solving the shortest vector problem for ideals of multiquadratic fields, which is the core problem in lattice-based cryptography.

Keywords:
мультиквадратичные поля, идеал Штикельбергера, элемент Штикельбергер, азадача поиска короткого вектора

Keywords:
multiquadratic number field, Stickelberger ideal, Stickelberger element, the shortest vector problem

1 Введение

Получение идеала Штикельбергера в явном виде является важной алгоритмической задачей в вычислительной теории чисел, в теории групп классов и, с недавних пор, в криптоанализе. Для числового поля K идеал Штикельбергера I – идеал групповой алгебры $\mathbb{Z}[G_K]$, где $G_K = \mathrm{Gal}(K/\mathbb{Q})$ – группа Галуа поля K. Полезное свойство I заключается в том, что под действием элементов I на Cl_K – группу классов идеалов K – любой класс становится тривиальным классом (иначе говоря, J^σ – главный идеал для любого $\sigma \in I$ и любого идеала J кольца целых $\mathcal{O}_K$ числового поля K).

Для кругового поля $K = \mathbb{Q}(\zeta_n)$ идеал Штикельберегра, рассматриваемый как решётка в $\mathbb{Z}^n$ с помощью вложения $\mathbb{Z}[G_K] \hookrightarrow \mathbb{Z}^n$, обладает "хорошим" базисом. Явный вид этого базиса описан, например, в [CDW17]. Это свойство идеала Штикельбергера в сочетании с 1) "обнуляющим" действием элементов идеала на целые идеалы $\mathbb{Z}[\zeta_n]$, 2) существованием (относительно) быстрого алгоритма нахождения короткого вектора в главных идеалах $\mathbb{Z}[\zeta_n]$, позволило Кармеру-Люка-Весоловски в [CDW17] получить алгоритм нахождения короткого вектора в идеалах кольца целых круговых полей. А в современном криптоанализе нахождение короткого вектора в решетках является основополагающей задачей.

Именно приложение идеала Штикельбергера в криптоанализе является нашей главной мотивацией для его изучения. Ввиду большой группы Галуа интересными полями являются мультиквадратичные. Недавние работы по эффективному вычислению короткого вектора в мультиквадраичных полях [BBdV$^+$17] и по вычислению группы классов [BV19] подводят к вопросу нахождения коротких векторов в произвольных идеалах. Следуя примеру круговых полей, для получения результатов в произвольных идеалах необходимо рассмотреть структуру идеала Штикельбергера для мультиквадратичных расширений.

В нашей статье мы предлагаем алгоритм вычисления идеала Штикельбергера для мультиквадратичного поля $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 \pmod 4$ и d_i попарно взаимно просты. Наш алгоритм имеет сложность $\widetilde{\mathcal{O}}(2^n)$, а так как $[K : \mathbb{Q}] = 2^n$, то даже для криптографически значимых степеней, наш алгоритм будет эффективным. В основе алгоритма лежит работа Кучеры [R.96].

2 Предварительные сведения

Обозначим за $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$ – мультиквадратичное поле, где $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 (\mathrm{mod}\, 4)$ и все d_i – попарно взаимно просты для $i = 1, \ldots, n$. Исходя из условий, наложенных на d_i, произвдение примитивных элементов поля K, а именно, $\sqrt{d_1} \cdot \sqrt{d_2} \cdot \ldots \cdot \sqrt{d_n}$, очевидно, лежит в круговом поле $\mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n})$, где $\zeta_{d_1 \cdot \ldots \cdot d_n}$ – примитивный корень степени $d_1 \cdot \ldots \cdot d_n$ из единицы. Тем самым, справедливо вложение $K \hookrightarrow \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n})$. Следует отметить, что указанный выбор примитивных элементов поля K обеспечивает условие $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$, где $\ell \leq n$. Это равенство будет доказано позже в лемме 1.

Рассмотрим башню числовых полей $\mathbb{Q} \subseteq K \subseteq L$ и обозначим их соответствующие группы Галуа за $G_L = \mathrm{Gal}(L/\mathbb{Q})$ и $G_K = \mathrm{Gal}(K/\mathbb{Q})$. Обозначим за $\mathbb{Q}[G_L] = \{\sum a_i \cdot \sigma_i | a_i \in \mathbb{Q}, \sigma_i \in G_L\}$ ($\mathbb{Q}[G_K] = \{\sum a_i \cdot \sigma_i | a_i \in \mathbb{Q}, \sigma_i \in G_K\}$) группу, конечно порожденную элементами G_L над $\mathbb{Q}$ (соответственно, группу, конечно порожденную элементами G_K над $\mathbb{Q}$). Важными понятиями при вычислении элементов Штикельбергера являются, так называемые, отображения res и cor. Определим эти отображения согласно [R.96] для расширения числовых полей L/K:

$$\mathsf{res}_{L/K} : \mathbb{Q}[G_L] \to \mathbb{Q}[G_K], \quad \mathsf{res}_{L/K}(\sum_{\sigma \in G_L} a_\sigma \sigma) = \sum_{\sigma \in G_L} a_\sigma (\sigma|_K),$$

$$\mathsf{cor}_{L/K} : \mathbb{Q}[G_K] \to \mathbb{Q}[G_L] \quad \mathsf{cor}_{L/K}(\sum_{\sigma \in G_K} a_\sigma \sigma) = \sum_{\sigma \in G_K} a_{\sigma|_K} \sigma,$$

где $\sigma|_K$ означает сужение автоморфизма $\sigma \in G_L$ на поле K, а a_σ, $a_{\sigma|_K}$ – коэффициенты, соответствующие автоморфизмам σ, $\sigma|_K$.

Также введем ряд следующих обозначений. Дробную часть числа обозначим как $\langle \cdot \rangle$, т.е. $0 < \langle \cdot \rangle < 1$. Наибольший общий делитель двух элементов $a, b \in \mathbb{Z}$ обозначим через (a, b). Символ Лежандра этих же элементов – через $\left(\frac{a}{b}\right)$. Для произвольного множества A его мощность будем обозначать как $\#A$.

Дадим классические определения элементу и идеалу Штикельбергера согласно [Sin81, с.189]:

Определение 2.1. Для любых положительного целого n и $\alpha \in \mathbb{Z}$ и кругового поля $\mathbb{Q}(\zeta_n)$ определим

$$\theta_n(\alpha) = \sum_{(a,n)=1} \left\langle -\frac{\alpha a}{n} \right\rangle \sigma_a^{-1},$$

где $0 < a \leq n$ и $\sigma_a \in G_{\mathbb{Q}(\zeta_n)} = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Определение 2.2. Для любого положительного целого n и произвольного $\alpha \in \mathbb{Z}$ элементом Штикельбергера $\theta_n^{'}(\alpha)$ называется элемент вида

$$\theta_n^{'}(\alpha) = \left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)} \circ \mathsf{res}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}\right)(\theta_n(\alpha)),$$

где K и $\mathbb{Q}(\zeta_n)$ соответственно числовое и круговое поля.

Определение 2.3. Идеалом Штикельбергера поля K называется идеал вида $I = I' \cap \mathbb{Z}[G_K]$, где

$$I' = \{\theta_n^{'}(\alpha) | \alpha, n \in \mathbb{Z}, n \geq 1\}.$$

Теперь дадим определение квадратичным гауссовым суммам, а также покажем как они взаимосвязаны с автоморфизмами круговых полей, поскольку эта взаимосвязь поможет вычислить действие отображения res, и как следствие, элемент Штикельбергера соответствующего числового поля.

Определение 2.4. Пусть $m, k \in \mathbb{Z}, k > 0$. Квадратичная гауссова сумма определяется как $g(m,k) = \sum\limits_{b=0}^{k-1} e^{\frac{2\pi i m b^2}{k}}$.

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

Теорема 1. *[BEW98, 1.5.2, с. 26]. Пусть $(m,k) = 1$, $k > 0$ и k – нечётное. Тогда*

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

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

Рассмотрим теперь действие автоморфизмов кругового поля $\mathbb{Q}(\zeta_k)$ на корни $\sqrt{k}$. Всякий такой автоморфизм имеет вид: $\sigma_a(e^{\frac{2\pi i}{k}}) = e^{\frac{2\pi i a}{k}}$. В случае, когда $k = p$ – нечетное простое, согласно [BEW98, (1.5.3), с. 26] имеем:

$$\sigma_a(\zeta_p) = \sigma_a(\sqrt{p}) = \sigma_a(g(1,p)) = \left(\frac{a}{p}\right) g(1,p) = \left(\frac{a}{p}\right)\sqrt{p}, \quad p \equiv 1 \pmod 4$$

и

$$\sigma_a(\zeta_p) = \sigma_a(\sqrt{-p}) = \left(\frac{a}{p}\right)\sqrt{-p}, \quad -p \equiv 1 \pmod 4.$$

В случае, если k – не простое, для нахождения действия автоморфизма σ_a мы можем применить китайскую теорему об остатках [BEW98, с. 43]. Пусть $k = k_1 \cdot ... \cdot k_n$, где k_i – простые числа, $(k_i, k_j) = 1$, $M_i = \frac{k}{k_i}$. Тогда

$$g(a,k) = g(aM_1, k_1) \cdot ... \cdot g(aM_n, k_n).$$

По теореме 1 имеем

$$g(a,k) = \left(\frac{aM_1}{k_1}\right) \cdot ... \cdot \left(\frac{aM_n}{k_n}\right) g(1,k_1) \cdot ... \cdot g(1,k_n).$$

Таким образом, нахождение действия автоморфизма σ_a на $g(a,k)$ в случае, когда k – не простое, сводится к определению его действия на все $g(1,k_1), ..., g(1,k_n)$.

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

Ответим на первый вопрос, определив сужение кругового поля $\mathbb{Q}(\zeta_n)$ на некоторое числовое поле. Рассмотрим общий случай, когда $n = p \cdot q$, где $p, q > 0$ – взаимно простые. Случай, когда n – простое, – очевиден, поскольку сопоставление θ_n корню $\sqrt{n}$ описано явно выше. Произвольным образом выберем a, взаимно простое с p и q. Тогда автоморфизм σ_a поля $\mathbb{Q}(\zeta_{pq})$ можно связать с действием автоморфизмов полей $\mathbb{Q}(\zeta_p)$ и $\mathbb{Q}(\zeta_q)$ на элементы $\sqrt{-p}$ и $\sqrt{-q}$ следующим образом:

$$\sigma_a(\zeta_{pq}) = g(a,pq) = \left(\frac{aq}{p}\right) g(1,p) \left(\frac{ap}{q}\right) g(1,q) = \sigma_{aq}(\sqrt{-p}) \cdot \sigma_{ap}(\sqrt{-q}).$$

Здесь индекс aq в случае $\sigma_{aq}(\sqrt{-p})$ рассматривается по модулю p, индекс ap в случае $\sigma_{ap}(\sqrt{-q})$ рассматривается по модулю q. Более детально все вычисления будут представлены в Разделе 3.

Ответ на второй вопрос даст следующая лемма:

Лемма 1. *Пусть $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$ – мультиквадратичное поле, где $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 \pmod 4$ и все d_i – попарно взаимно просты для $i = 1 \ldots n$; $\mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$ – круговое поле, где $\zeta_{d_1 \cdot \ldots \cdot d_\ell}$ – корень степени $d_1 \cdot \ldots \cdot d_\ell$ из единицы и $\ell \leq n$. Тогда $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$.*

Доказательство. Докажем сначала включение $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell}) \subset K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$. Очевидно, что $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$ – подполе поля K. Учитывая [S09, 4.5.5, с.112], условия $d_1 \equiv d_2 \equiv \ldots \equiv d_\ell \equiv 1 \pmod 4$ и тот факт, что $d_i | d_1 \cdot \ldots \cdot d_\ell$ для $i = 1, \ldots, \ell$, получаем $\mathbb{Q}(\sqrt{d_1}) \subset \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$, $\ldots$, $\mathbb{Q}(\sqrt{d_\ell}) \subset \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$. Очевидно, что произведение любой комбинации

d_i также будет сравнимо с единицей по модулю 4. Поэтому применяя вышесказанное на различные комбинации произведений, получим, что и $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell}) \subset \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$.

Теперь докажем обратное, что $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n}) \subset \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$. Для этого воспользуемся гауссовыми суммами, которые были описаны ранее, а именно, следующим равенством

$$g(1, d_1 \cdot \ldots \cdot d_\ell) = g(1, d_1) \cdot \ldots \cdot g(1, d_\ell) = \sqrt{d_1} \cdot \ldots \cdot \sqrt{d_\ell}.$$

Это означает, что сужение кругового поля $\mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$ на некоторое числовое поле, в нашем случае это $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell})$, осуществляется путем выражения элемента $\zeta_{d_1 \cdot \ldots \cdot d_\ell}$ через элемент $\sqrt{d_1} \cdot \ldots \cdot \sqrt{d_\ell}$, который будет лежать в числовом поле, на которое мы сужаем круговое поле. Учитывая, что $\sqrt{d_1} \cdot \ldots \cdot \sqrt{d_\ell} \in \mathbb{Q}(\sqrt{d_1 \cdot \ldots \cdot d_\ell}) \subset \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell}) \subset \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n}) = K$, получаем, что наибольшим полем, через элементы которого выражается $\zeta_{d_1 \cdot \ldots \cdot d_\ell}$ при соответствующем сужении, является $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$. Таким образом, выполняется обратное включение $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n}) \subset \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_\ell})$. □

Прежде, чем приступить к детальному описанию вычисления элементов Штикельбергера, дадим альтернативные опредления элементу и идеалу Штикельбергера, которые, во-первых, упростят вычисления, а во-вторых, повзолят доказать корректность этих вычислений.

Обозначим за f – кондуктор поля K, тогда очевидно, что $K \cap \mathbb{Q}(\zeta_n) = K \cap \mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_n) = K \cap \mathbb{Q}(\zeta_{(f,n)})$ для положительного целого n. Определение кондуктора числового поля можно посмотреть в [HP08]

Ранее, когда мы рассматривали квадратичные гауссовы суммы и сопоставляли их с действием афтоморфизма σ_a кругового поля $\mathbb{Q}(\zeta_p)$, в качестве p мы выбирали нечетное простое p. Напомним, что непростой случай всегда можно свести к простому за счет мультипликативности. Рассмотрим отдельно случай $p = 2$ и вычислим для него элемент Штикельбергера

$$\theta_2'(\alpha) = \left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_2)} \circ \mathsf{res}_{\mathbb{Q}(\zeta_2)/K\cap\mathbb{Q}(\zeta_2)}\right)(\theta_2(\alpha)).$$

Отметим, что в данном случае $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ и, соответственно, $K \cap \mathbb{Q}(\zeta_2) = \mathbb{Q}$. Кроме того, согласно определению $\theta_n(\alpha)$, получаем $\theta_2(1) = \frac{1}{2}\sigma_1^{-1}$. Здесь, очевидно, σ_1 – единственный автоморфизм поля $\mathbb{Q}(\zeta_2)$, а потому рассматриваем его как тождественный автоморфизм id поля $\mathbb{Q}$. Тогда элемент Штикельбергера примет вид

$$\theta_2'(1) = \left(\mathsf{cor}_{K/\mathbb{Q}} \circ \mathsf{res}_{\mathbb{Q}/\mathbb{Q}}\right)(\theta_2(1)) = \mathsf{cor}_{K/\mathbb{Q}}\left(\frac{1}{2}\mathsf{id}\right).$$

Применяя отображение cor к id, мы получим $\sum\limits_{\sigma\in G_K}\sigma$, обозначим эту сумму за N_K. Тогда окончательно получаем

$$\theta_2^{'}(1)=\frac{1}{2}\sum_{\sigma\in G_K}\sigma=\frac{1}{2}N_K.$$

Кроме того, следует отметить, что в случае действительного поля K согласно [Was82, с.94] $\sigma_a=\mathsf{id}$, где $\sigma_a\in G_{\mathbb{Q}(\zeta_n)}$. Тогда элемент Штикельбергера $\theta_n^{'}(\alpha)=\frac{1}{2}\sum\limits_{\sigma\in G_K}\sigma=\frac{1}{2}N_K$ не зависит от α. Для действительных полей принято рассматривать $\alpha>0$, а поскольку, зависимость при вычислении элемента Штикельбергера от α отсутствует, то полагают $\alpha=1$.

Исходя из вышесказанного, мы можем переписать определение идеала Штикельбергера следующим образом:

Определение 2.5. Идеалом Штикельбергера поля K с кондуктором f называется идеал вида $I=I'\cap\mathbb{Z}[G_K]$, где

$$I'=\{\theta_n^{'}(\alpha)|n|f,\alpha\in\mathbb{Z},\alpha<0\}\cup\left\{\frac{1}{2}N_K\right\}.$$

Положим $a\geq 1$ – целое и $(a,fn)=1$, где f – кондуктор поля K, и, как и прежде, обозначим за $\sigma_a\in G_{\mathbb{Q}(\zeta_{fn})}$ – автоморфизм, ставящий в соответствие корню из единицы его a-ю степень. Тогда по определению

$$\theta_n^{'}(a\alpha)=\left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)}\circ\mathsf{res}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}\right)(\theta_n(a\alpha)).$$

С другой стороны, исходя из опредлений отображений res и σ_a, мы можем записать $\theta_n(a\alpha)$ следующим образом:

$$\theta_n(a\alpha)=\mathsf{res}_{\mathbb{Q}(\zeta_{nf})/\mathbb{Q}(\zeta_n)}\sigma_a(\theta_n(\alpha)).$$

Окончательно имеем

$$\begin{aligned}\theta_n^{'}(a\alpha)&=\left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)}\circ\mathsf{res}_{\mathbb{Q}(\zeta_n)/K\cap\mathbb{Q}(\zeta_n)}\circ\mathsf{res}_{\mathbb{Q}(\zeta_{nf})/\mathbb{Q}(\zeta_n)}\sigma_a\right)(\theta_n(\alpha))\\&=\left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)}\circ\mathsf{res}_{\mathbb{Q}(\zeta_{nf})/K\cap\mathbb{Q}(\zeta_n)}\sigma_a\right)(\theta_n(\alpha))\\&=\left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)}\circ\mathsf{res}_{\mathbb{Q}(\zeta_{nf})/K\cap\mathbb{Q}(\zeta_n)}\right)(\sigma_a)\cdot\left(\mathsf{cor}_{K/K\cap\mathbb{Q}(\zeta_n)}\circ\mathsf{res}_{\mathbb{Q}(\zeta_{nf})/K\cap\mathbb{Q}(\zeta_n)}\right)(\theta_n(\alpha))\\&=\sigma\theta_n^{'}(\alpha),\end{aligned}$$

где σ – автоморфизм поля K согласно опредлениям res и cor. Полагая $\alpha=-1$, получаем, что элемент Штикельбергера для мнимых числовых полей имеет вид $\theta_n^{'}(-a)=\sigma\theta_n^{'}(-1)$, где $\sigma\in G_K$. Соответственно, мы можем переписать определение идеала Штикельбергера:

Определение 2.6. Идеалом Штикельбергера поля K с кондуктором f называется идеал вида $I = I' \cap \mathbb{Z}[G_K]$, где

$$I' = \{\sigma \cdot \theta_n^{'}(-1)|n|f, \sigma \in G_K\} \cup \left\{\frac{1}{2}N_K\right\}.$$

3 Алгоритм

В этой главе подробно рассмотрим алгоритм вычисления идеала Штикельбергера для мнимых мультиквадратичных полей в соответствии с описанной в предыдущей главе теорией.

Вычисление действия отображения res не тривиально в общем случае, поэтому рассмотрим его более детально. Применим описанный ранее метод с использованием квадратичных гауссовых сумм для вычисления $\mathsf{res}_{\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_n})/K\cap\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_n})}\theta_{d_1\cdot\ldots\cdot d_n}(-1)$. Отдельно распишем $\theta_{d_1\cdot\ldots\cdot d_n}(-1)$:

$$\theta_{d_1\cdot\ldots\cdot d_n}(-1) = \sum_{(a,d_1\cdot\ldots\cdot d_n)=1} \left\langle \frac{a}{d_1\cdot\ldots\cdot d_n}\right\rangle \sigma_a^{-1}.$$

Здесь автоморфизмы σ_a – автоморфизмы поля $\mathbb{Q}(\zeta_{d_1\cdot\ldots\cdot d_n})$ и действуют лишь на элемент $\sqrt{d_1\cdot\ldots\cdot d_n}$. Применяя вышеописанную формулу, каждый такой автоморфизм мы сведем к произведению автоморфизмов полей $\mathbb{Q}(\zeta_{d_1})$, …, $\mathbb{Q}(\zeta_{d_n})$ соответственно. Рассмотрим каждое слагаемое, а именно, $\langle \frac{a}{d_1\cdot\ldots\cdot d_n}\rangle \sigma_a^{-1}$ более детально. Введем обозначение: $\pi_i = a\prod_{j\neq i} d_j$, тогда

$$\left\langle \frac{a}{d_1\cdot\ldots\cdot d_n}\right\rangle \sigma_a^{-1}(\zeta_{d_1\cdot\ldots\cdot d_n}) = \sigma_a(\sqrt{d_1\cdot\ldots\cdot d_n}) =$$
$$\sigma_{\pi_1 \bmod (d_1)}(\sqrt{d_1})\cdot\ldots\cdot\sigma_{\pi_n \bmod (d_n)}(\sqrt{d_n}) =$$
$$\left\langle \frac{a}{d_1\cdot\ldots\cdot d_n}\right\rangle \sigma^{-1}_{\pi_1 \bmod (d_1)}(\zeta(d_1))\cdot\ldots\cdot\sigma^{-1}_{\pi_n \bmod (d_n)}(\zeta(d_n)) =$$
$$\left\langle \frac{a}{d_1\cdot\ldots\cdot d_n}\right\rangle \sigma_{\frac{1}{\pi_1 \bmod (d_1)} \bmod (d_1)}(\zeta(d_1))\cdot\ldots\cdot\sigma_{\frac{1}{\pi_n \bmod (d_n)} \bmod (d_n)}(\zeta(d_n))$$

Далее рассуждаем следующим образом. Если $\frac{1}{\pi_1 \bmod (d_1)} \bmod (d_1)$ – квадратичный вычет по модулю d_1, то заменяем $\sigma_{\frac{1}{\pi_1 \bmod (d_1)} \bmod (d_1)}(\zeta(d_1))$ на id_1, где $id_1 : \sqrt{d_1} \to \sqrt{d_1}$; в противном случае, заменяем на σ_1, где $\sigma_1 : \sqrt{d_1} \to -\sqrt{d_1}$. Аналогичные рассуждения применяем для остальных множителей.

Полученные композиции автоморфизмов переобозначим следующим образом:

$$\begin{aligned}
id_1 \cdot id_2 \cdot \ldots \cdot id_n &= id : \sqrt{d_1} + \ldots + \sqrt{d_n} \to \sqrt{d_1} + \sqrt{d_2} + \ldots + \sqrt{d_n} \\
id_1 \cdot id_2 \cdot \ldots \cdot \sigma_n &= \tau_1 : \sqrt{d_1} + \ldots + \sqrt{d_n} \to \sqrt{d_1} + \sqrt{d_2} + \ldots - \sqrt{d_n} \\
&\vdots \qquad (1) \\
\sigma_1 \cdot \ldots \cdot \sigma_{n-1} \cdot id_n &= \tau_{m-1} : \sqrt{d_1} + \ldots + \sqrt{d_{n-1}} + \sqrt{d_n} \to -\sqrt{d_1} - \ldots + \sqrt{d_n} \\
\sigma_1 \cdot \ldots \cdot \sigma_{n-1} \cdot \sigma_n &= \tau_m : \sqrt{d_1} + \ldots + \sqrt{d_{n-1}} + \sqrt{d_n} \to -\sqrt{d_1} - \ldots - \sqrt{d_n}
\end{aligned}$$

Очевидно, что общее количество получившихся композиций автоморфизмов равно 2^n. Таким образом, поскольку первый автоморфизм мы обозначили за id, то $m = 2^n - 1$. Псевдокод процедуры вычисления res представлен в Алгоритме 3.1.

Алгоритм 3.1 Вычисление $\mathsf{res}(\theta_n(-1))$

Вход: $K = \mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})$
Выход: $\mathsf{res}(\theta_n(-1))$

$f \leftarrow \prod_{j=1}^{k} d'_j$ ▷ f–кондуктор K
for $a \in \mathbb{Z}_f^*$ **do**
  for $j \leftarrow 1$ to k **do**
    $t \leftarrow \frac{a \cdot d'_1 \cdot \ldots \cdot d'_k}{d'_j} \bmod d'_j$
    $index \leftarrow \frac{1}{t} \bmod d'_j$
    if $legendre(index, d'_j) = 1$ **then**
      $\sigma_a^{-1} = \sigma_a^{-1} \cdot id_j$ ▷ id_j–тождественный в $\mathbb{Q}(\sqrt{d'_j})$
    else if $legendre(index, d'_j) = -1$ **then**
      $\sigma_a^{-1} = \sigma_a^{-1} \cdot \sigma_j$ ▷ σ_j–сопряжение в $\mathbb{Q}(\sqrt{d'_j})$
  $\sigma_a^{-1} = \frac{a}{f} \cdot \sigma_a^{-1}$
$\theta \leftarrow \sum_{a \in \mathbb{Z}_f^*} \sigma_a^{-1}$
res ← заменить получившиеся комбинации автоморфизмов в каждом слагаемом θ на соответствующие τ_i в соответствии с формулами 1
return res

Вычисление cor Автоморфизмы, полученные после вычисления res, являются автоморфизмами поля $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n})$. Вычисление же действия отображения cor представляет собой переход от этих автоморфизмов к

автоморфизмам поля K. Обозначим автоморфизмы поля K следующим образом:

$$\begin{aligned}
id &: \sqrt{d_1} + \sqrt{d_2} + \ldots + \sqrt{d_n} \to \sqrt{d_1} + \sqrt{d_2} + \ldots + \sqrt{d_n} \\
\rho_1 &: \sqrt{d_1} + \sqrt{d_2} + \ldots + \sqrt{d_n} \to \sqrt{d_1} + \sqrt{d_2} + \ldots - \sqrt{d_n} \\
&\vdots \\
\rho_{m-1} &: \sqrt{d_1} + \ldots + \sqrt{d_{n-1}} + \sqrt{d_n} \to -\sqrt{d_1} - \ldots - \sqrt{d_{n-1}} + \sqrt{d_n} \\
\rho_m &: \sqrt{d_1} + \ldots + \sqrt{d_{n-1}} + \sqrt{d_n} \to -\sqrt{d_1} - \ldots - \sqrt{d_{n-1}} - \sqrt{d_n}.
\end{aligned}$$

Очевидно, что если $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n}) = K$, то отображение cor будет действовать тождественно (полученные ранее автоморфизмы τ_i совпадают с ρ_i). Отметим, что такой случай возникает при вычислении элемента Штикельбергера $\theta'_{d_1 \cdot \ldots \cdot d_n}(-1)$. А как быть, если мы вычисляем, например, элемент Штикельбергера вида $\theta'_{d_1 \cdot \ldots \cdot d_\ell}(-1)$, где $\ell < n$? Рассмотрим случай, когда $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_n}) \neq K$. Пусть $K \cap \mathbb{Q}(\zeta_{d_1 \cdot \ldots \cdot d_\ell}) = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$. Результатом действия отображения res в этом случае будет

$$a_1 \cdot id_l + a_2 \cdot \tau_1 + \ldots + a_{2^l-1} \cdot \tau_{2^l-2} + a_{2^l} \cdot \tau_{2^l-1},$$

где id_l, τ_i – это автоморфизмы поля $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$, $i = 1, \ldots, 2^l - 1$:

$$\begin{aligned}
id_l &: \sqrt{d_1} + \ldots + \sqrt{d_l} \to \sqrt{d_1} + \sqrt{d_2} + \ldots + \sqrt{d_l} \\
\tau_1 &: \sqrt{d_1} + \ldots + \sqrt{d_l} \to \sqrt{d_1} + \sqrt{d_2} + \ldots - \sqrt{d_l} \\
&\vdots \\
\tau_{2^l-2} &: \sqrt{d_1} + \ldots + \sqrt{d_{l-1}} + \sqrt{d_l} \to -\sqrt{d_1} - \ldots + \sqrt{d_l} \\
\tau_{2^l-1} &: \sqrt{d_1} + \ldots + \sqrt{d_{l-1}} + \sqrt{d_l} \to -\sqrt{d_1} - \ldots - \sqrt{d_l}
\end{aligned}$$

Далее переходим от перечисленных автоморфизмов поля $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_\ell})$ к автоморфизмам ρ_i поля K. Переход осуществляется следующим образом: если ρ_i относительно элемента $\sqrt{d_1} + \ldots + \sqrt{d_l}$ действует как id_l, то все такие автоморфизмы ρ_i будут участвовать в записи элемента Штикельбергера с коэффициентом a_1. Аналогично, если ρ_i относительно $\sqrt{d_1} + \ldots + \sqrt{d_l}$ действует как τ_1, то все такие автоморфизмы ρ_i будут участвовать в записи элемента Штикельбергера с коэффициентом a_2. Применяя аналогичный подход для всех остальных случаев, получаем

$$\theta'_{d_1 \cdot \ldots \cdot d_\ell}(-1) = a_1 \cdot id + a_1 \cdot \rho_1 + \ldots + a_{2^l} \cdot \rho_{m-1} + a_{2^l} \cdot \rho_m.$$

Таким образом, в общем случае элемент Штикельбергера примет следующий вид:

$$\theta_n^{'}(-1) = c_0 \cdot id + c_1 \cdot \rho_1 + \ldots + c_{m-1} \cdot \rho_{m-1} + c_m \cdot \rho_m,$$

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

Очевидно, что общее количество элементов Штикельбергера в поле K равно $2^n - 1$ (по количеству всех возможных подполей). Таким образом, нам необходимо умножить 2^n автоморфизов на каждый из $2^n - 1$ элементов Штикельбергера.

Рассмотрим результат этого умножения подробнее. Пусть $n = 2$, т.е. исходное поле является биквадратичным $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ и выпишем все его подполя: $\mathbb{Q}(\sqrt{d_1})$, $\mathbb{Q}(\sqrt{d_2})$, $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Элементы Штикельбергера соответствующих подполей будут иметь вид:

$$\begin{aligned}
\theta_{d_1}^{'}(-1) &= a_1 \cdot id + a_1 \cdot \rho_1 + b_1 \cdot \rho_2 + b_1 \cdot \rho_3, \\
\theta_{d_1}^{'}(-1) &= a_2 \cdot id + b_2 \cdot \rho_1 + a_2 \cdot \rho_2 + b_2 \cdot \rho_3, \\
\theta_{d_1 \cdot d_2}^{'}(-1) &= a_3 \cdot id + b_3 \cdot \rho_1 + c_3 \cdot \rho_2 + d_3 \cdot \rho_3.
\end{aligned}$$

После умножения первых двух элементов на автоморфизмы $\{id, \rho_1, \rho_2\, \rho_3\}$ мы получим только две различные комбинации, потому что автоморфизмы будут переставлять два коэффициента a_1, b_1 и a_2, b_2 соответственно. В свою очередь, последний элемент, имеющий 4 различных коэффициента, даст 4 различные комбинации. Отсюда мы можем сделать вывод, что количество различных комбинаций зависит от количества различных коэффициентов в элементе Штикельбергера. Будем записывать все различные комбинации в множество I'. Таким образом, общее количество различных элементов для мультиквадратичного поля будет равно $\#I'$.

В результате, применяя вышеописанный метод для произвольного числового поля, мы получим следующий результат:

$$I = s_1 \cdot \theta_1 + \ldots + s_{\#I'} \cdot \theta_{\#I'} = \sum_{i=1}^{\#I'} s_i \cdot \theta_i, s_i \in \mathbb{Z}.$$

3.1 Сложность Алгоритма 3.2

Лемма 2. *Вычислительная сложность Алгоритма 3.2 равна*

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

Алгоритм 3.2 Идеал Штикельбергера

Вход: $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$
Выход: $I = I' \cap \mathbb{Z}[Gal(K/\mathbb{Q})]$

1: $A \leftarrow$ массив, состоящий из всех подполей K
2: **for** $i \leftarrow 1$ to $2^n - 1$ **do**
3: $\quad \mathsf{res}_i \leftarrow \mathsf{res}_{\mathbb{Q}(\zeta_{d'_1 \cdot \ldots \cdot d'_k})/\mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})} \theta_i$ (Алгоритм 3.1, Вход: $A[i]$)
4: $\quad \theta'_i \leftarrow \mathsf{cor}_{K/\mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})} \mathsf{res}_i$
5: $I' \leftarrow \{\}$
6: **for** $i \leftarrow 1$ to $2^n - 1$ **do**
7: $\quad$ **for** $j \leftarrow 1$ to 2^n **do**
8: $\quad\quad t \leftarrow \rho_j \cdot \theta'_i$
9: $\quad\quad I' \leftarrow A \cup t$
10: $I \leftarrow \prod_{i=1}^{\#I'} s_i \cdot I'_i$
11: **return** I

где $d = \max_i d_i$.

Доказательство. Поскольку Алгоритм 3.1 является частью Алгоритма 3.2 рассмотрим сначала его вычислительную сложность. На вход Алгоритма 3.1 подается k–квадратичное поле $\mathbb{Q}(\sqrt{d'_1}, \sqrt{d'_2}, \ldots, \sqrt{d'_k})$ и на Шаге 1 мы вычисляем произведение всех $d'_j, j \leq k$. Оценка этого произведения совпадает с оценкой сложности прайморориала, этот факт вытекает из оценки n-ого простого числа, которая в нашем случае равна $|d_i| \approx k \cdot log(k)$. Таким образом, мы получаем $f = \prod d'_i = e^{k \cdot \log(k)}$. Теперь рассмотрим циклы, расположенные на Шагах 2 и 3. Первый цикл повторяется $\phi(f)$ раз, это значит, что его оценка будет $\mathcal{O}(f) = \mathcal{O}(e^{k \cdot \log(k)})$. Второй же цикл повторяется k раз. Теперь рассмотрим тело второго цикла. Вычисления на Шагах 4, 5, 6 и 8 представляют собой вычисления по модулю d'_j. В худшем случае, образующая будет наибольшей, т.е. $d = \max_j d'_j$. Поэтому оценка каждого из шагов 4, 5, 6 и 8 представляет собой $\mathcal{O}(\log^3(d))$. В цикле мы выполняем либо Шаг 6, либо Шаг 8, а Шаги 7 и 9 имеют сложность $\mathcal{O}(1)$. Таким образом, сложность одной итерации внутреннего цикла равна $\mathcal{O}(\log^3(d))$. Во внешнем цикле у нас также производится вычисление Шага 10, чья сложность есть $\mathcal{O}(\log^3(f)) = \mathcal{O}(\log^3(e^{k \cdot \log(k)})) = \mathcal{O}(k^3 \cdot \log^3(k))$. Сложность Шага 11 равна $\mathcal{O}(1)$, а замена, осуществляющаяся на Шаге 11, имеет сложность $\mathcal{O}(2^k)$, поскольку мы имеем 2^k автоморфизмов. Обобщая все вышесказанное,

мы получаем, что общая сложность Алгоритма 3.1 есть

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

Поскольку функция $e^{k\cdot\log(k)}$ возрастает быстрее, чем 2^k, итоговая сложность Алгоритма 3.1 имеет вид:

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

Вернемся теперь к Алгоритму 3.2. Ему на вход мы подаем $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\ldots,\sqrt{d_n})$. Рассмотрим цикл на Шаге 2. Он повторяется 2^n-1 раз. На Шаге 3, в теле этого цикла, мы вычисляем результат отображения res, а значит, используем Алгоритм 3.1. Поскольку на вход мы получили n–квадратичное поле, и в худшем случае в этот цикл попадет именно оно, то сложность Шага 3 примет вид: $\mathcal{O}(e^{n\cdot\log(n)}\cdot n^4\cdot\log^3(d)\cdot\log^3(n))$. На Шаге 4 мы осуществляем переход к автоморфизмам поля K, чья сложность есть $\mathcal{O}(2^n)$, по количеству автоморфизмов. Таким образом, общая сложность этого цикла равна $\mathcal{O}(e^{n\cdot\log(n)}\cdot n^4\cdot\log^3(d)\cdot\log^3(n)\cdot 2^{2n})$. Циклы на Шагах 6 и 7 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 есть $\mathcal{O}(2^{2n})$.

Теперь рассмотрим Шаг 10 и произведем оценку верхней границы $\#I'$. Для этого рассмотрим несколько частных случаев. Пусть $K=\mathbb{Q}(\sqrt{d_1})$, тогда количество различных элементов, которое может дать квадратичное поле равно 2 (поскольку имеем два различных коэффициента в элементе Штикельбергера, и после умножения на автоморфизмы они поменяются местами). В поле $K=\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$ мы получим 8 различных элементов (по 2 – от квадратичных подполей и 4 – от биквадратичного, т.к. в худшем случае у него может быть 4 различных коэффициента). Рассуждая далее по аналогии, получим, что в триквадратичном поле - 26 различных элементов, в худшем случае, а в 4-квадратичном – 80, и так далее. Таким образом, полученная последовательность будет иметь длину 3^n-1. А значит, сложность Шага 10 есть $\mathcal{O}(3^n)$.

Окончательно общая сложность Алгоритма 3.2 будет равна:

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

Упростив, получим:

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

□

3.2 Пример

Проиллюстрируем вычисление элемента и идеала Штикельбергера в случае триквадратичного поля $K = \mathbb{Q}(\sqrt{-19}, \sqrt{-31}, \sqrt{-43})$. Отметим, что $-19 \equiv -31 \equiv -43 \equiv 1 \,(\mathrm{mod} 4)$. Выпишем все подполя исходного поля K:

$$\mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-31}), \mathbb{Q}(\sqrt{-43}),$$
$$\mathbb{Q}(\sqrt{-19}, \sqrt{-31}), \mathbb{Q}(\sqrt{-19}, \sqrt{-43}), \mathbb{Q}(\sqrt{-31}, \sqrt{-43}),$$
$$\mathbb{Q}(\sqrt{-19}, \sqrt{-31}, \sqrt{-43}).$$

Вычислим действие отображения res, соответствующее каждому из указанных подполей, а также элементу $\theta_{d_i}(-1)$, где d_i – соответствующий делитель кондуктора $f = 25327$ поля K согласно определению. Т.е. $d_i \in \{19, 31, 43, 589, 817, 1333, 25327\}$.

Рассмотрим $\mathbb{Q}(\sqrt{-19})$. Нам необходимо вычислить

$$\mathsf{res}_{\mathbb{Q}(\zeta_{19})/\mathbb{Q}(\sqrt{-19},\sqrt{-31},\sqrt{-43})\cap\mathbb{Q}(\zeta_{19})}\theta_{19}(-1) = \mathsf{res}_{\mathbb{Q}(\zeta_{19})/\mathbb{Q}(\sqrt{-19})}\theta_{19}(-1).$$

Первоначально вычислим элемент $\theta_{19}(-1)$:

$$\theta_{19}(-1) = \sum_{(a,19)=1} \langle \frac{a}{19} \rangle \sigma_a^{-1} = 4 \cdot id_1 + 5 \cdot \sigma_1,$$

где $id_1 : \sqrt{-19} \to \sqrt{-19}, \sigma_1 : \sqrt{-19} \to -\sqrt{-19}$. Таким образом,

$$\mathsf{res}_{\mathbb{Q}(\zeta_{19})/\mathbb{Q}(\sqrt{-19})}\theta_{19}(-1) = 4 \cdot id_1 + 5 \cdot \sigma_1.$$

Аналогично, для других квадратичных подполей получаем:

$$\mathsf{res}_{\mathbb{Q}(\zeta_{31})/\mathbb{Q}(\sqrt{-31})}\theta_{31}(-1) = 6 \cdot id_2 + 9 \cdot \sigma_2,$$
$$\mathsf{res}_{\mathbb{Q}(\zeta_{43})/\mathbb{Q}(\sqrt{-43})}\theta_{43}(-1) = 10 \cdot id_3 + 11 \cdot \sigma_3,$$

где $id_2 : \sqrt{-31} \to \sqrt{-31}$, $\sigma_2 : \sqrt{-31} \to -\sqrt{-31}$, $id_3 : \sqrt{-43} \to \sqrt{-43}$, $\sigma_3 : \sqrt{-43} \to -\sqrt{-43}$.

Рассмотрим теперь подполе $\mathbb{Q}(\sqrt{-19}, \sqrt{-31})$. Вычислим действие отображения res:

$$\mathsf{res}_{\mathbb{Q}(\zeta_{589})/\mathbb{Q}(\sqrt{-19},\sqrt{-31},\sqrt{-43})\cap\mathbb{Q}(\zeta_{589})}\theta_{589}(-1) = \mathsf{res}_{\mathbb{Q}(\zeta_{589})/\mathbb{Q}(\sqrt{-19},\sqrt{-31})}\theta_{589}(-1) =$$
$$= \mathsf{res}_{\mathbb{Q}(\zeta_{589})/\mathbb{Q}(\sqrt{-19},\sqrt{-31})} \sum_{(a,589)=1} \langle \frac{a}{589} \rangle \sigma_a^{-1} =$$
$$= \mathsf{res}_{\mathbb{Q}(\zeta_{589})/\mathbb{Q}(\sqrt{-19},\sqrt{-31})}(68 \cdot id_1 \cdot id_2 + 68 \cdot id_1 \cdot \sigma_2 + 67 \cdot \sigma_1 \cdot id_2 + 67 \cdot \sigma_1 \cdot \sigma_2) =$$
$$= 68 \cdot id + 68 \cdot \tau_1 + 67 \cdot \tau_2 + 67 \cdot \tau_3,$$

где автоморфизмы τ_i – это автоморфизмы поля $\mathbb{Q}(\sqrt{-19}, \sqrt{-31})$, а именно,

$$id_1 \cdot id_2 = id : \sqrt{19} + \sqrt{31} \to \sqrt{19} + \sqrt{31},$$
$$id_1 \cdot \sigma_2 = \tau_1 : \sqrt{19} + \sqrt{31} \to \sqrt{19} - \sqrt{31},$$
$$\sigma_1 \cdot id_2 = \tau_2 : \sqrt{19} + \sqrt{31} \to -\sqrt{19} + \sqrt{31},$$
$$\sigma_1 \cdot \sigma_2 = \tau_3 : \sqrt{19} + \sqrt{31} \to -\sqrt{19} - \sqrt{31}.$$

Аналогично, для других биквадратичных подполей получаем:

$$\mathsf{res}_{\mathbb{Q}(\zeta_{817})/\mathbb{Q}(\sqrt{-19},\sqrt{-43})}\theta_{817}(-1) = 95 \cdot id' + 94 \cdot \tau_1' + 95 \cdot \tau_2' + 94 \cdot \tau_3',$$
$$\mathsf{res}_{\mathbb{Q}(\zeta_{1333})/\mathbb{Q}(\sqrt{-31},\sqrt{-43})}\theta_{1333}(-1) = 159 \cdot id'' + 159 \cdot \tau_1'' + 156 \cdot \tau_2'' + 156 \cdot \tau_3''.$$

Рассмотрим оставшееся подполе $\mathbb{Q}(\sqrt{-19}, \sqrt{-31}, \sqrt{-43})$ и вычислим действие отображения res:

$$\mathsf{res}_{\mathbb{Q}(\zeta_{25327})/\mathbb{Q}(\sqrt{-19},\sqrt{-31},\sqrt{-43})\cap\mathbb{Q}(\zeta_{25327})}\theta_{25327}(-1) = \mathsf{res}_{\mathbb{Q}(\zeta_{25327})/\mathbb{Q}(\sqrt{-19},\sqrt{-31},\sqrt{-43})}\theta_{25327}(-1) =$$
$$= \mathsf{res}_{\mathbb{Q}(\zeta_{25327})/\mathbb{Q}(\sqrt{-19},\sqrt{-31},\sqrt{-43})} \sum_{(a,25327)=1} \langle \frac{a}{25327} \rangle \sigma_a^{-1} =$$

$\mathsf{res}_{\mathbb{Q}(\zeta_{589})/\mathbb{Q}(\sqrt{-19},\sqrt{-31},\sqrt{-43})}(1423 \cdot id_1 \cdot id_2 \cdot id_3 + 1412 \cdot id_1 \cdot id_2 \cdot \sigma_3 + 1412 \cdot id_1 \cdot \sigma_2 \cdot id_3 + 1423 \cdot id_1 \cdot \sigma_2 \cdot \sigma_3 +$
$+ 1412 \cdot \sigma_1 \cdot id_2 \cdot id_3 + 1423 \cdot \sigma_1 \cdot id_2 \cdot \sigma_3 + 1423 \cdot \sigma_1 \cdot \sigma_2 \cdot id_3 + 1412 \cdot \sigma_1 \cdot \sigma_2 \cdot \sigma_3) =$
$1423 \cdot id''' + 1412 \cdot \tau_1''' + 1412 \cdot \tau_2''' + 1423 \cdot \tau_3''' + 1412 \cdot \tau_4''' + 1423 \cdot \tau_5''' + 1423 \cdot \tau_6''' + 1412 \cdot \tau_7''',$

где автоморфизмы τ_i''' – это автоморфизмы поля $\mathbb{Q}(\sqrt{-19}, \sqrt{-31}, \sqrt{-43})$, а именно,

$$id_1 \cdot id_2 \cdot id_3 = id''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to \sqrt{19} + \sqrt{31} + \sqrt{-43},$$
$$id_1 \cdot id_2 \cdot \sigma_3 = \tau_1''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to \sqrt{19} + \sqrt{31} - \sqrt{-43},$$
$$id_1 \cdot \sigma_2 \cdot id_3 = \tau_2''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to \sqrt{19} - \sqrt{31} + \sqrt{-43},$$
$$id_1 \cdot \sigma_2 \cdot \sigma_3 = \tau_3''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to \sqrt{19} - \sqrt{31} - \sqrt{-43},$$
$$\sigma_1 \cdot id_2 \cdot id_3 = \tau_4''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to -\sqrt{19} + \sqrt{31} + \sqrt{-43},$$
$$\sigma_1 \cdot id_2 \cdot \sigma_3 = \tau_5''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to -\sqrt{19} + \sqrt{31} - \sqrt{-43},$$
$$\sigma_1 \cdot \sigma_2 \cdot id_3 = \tau_6''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to -\sqrt{19} - \sqrt{31} + \sqrt{-43},$$
$$\sigma_1 \cdot \sigma_2 \cdot \sigma_3 = \tau_7''' : \sqrt{19} + \sqrt{31} + \sqrt{-43} \to -\sqrt{19} - \sqrt{31} - \sqrt{-43}.$$

Теперь нам необходимо для всех получившихся res вычислить действие отображения cor. Это значит, что мы осуществим переход к автоморфиз-

мам поля K, а именно,

$$\begin{aligned}
id &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to \sqrt{19}+\sqrt{31}+\sqrt{-43},\\
\rho_1 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to \sqrt{19}+\sqrt{31}-\sqrt{-43},\\
\rho_2 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to \sqrt{19}-\sqrt{31}+\sqrt{-43},\\
\rho_3 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to \sqrt{19}-\sqrt{31}-\sqrt{-43},\\
\rho_4 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to -\sqrt{19}+\sqrt{31}+\sqrt{-43},\\
\rho_5 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to -\sqrt{19}+\sqrt{31}-\sqrt{-43},\\
\rho_6 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to -\sqrt{19}-\sqrt{31}+\sqrt{-43},\\
\rho_7 &: \sqrt{19}+\sqrt{31}+\sqrt{-43} \to -\sqrt{19}-\sqrt{31}-\sqrt{-43}.
\end{aligned}$$

Рассмотрим $\mathsf{res}_{\mathbb{Q}(\zeta_{19})/\mathbb{Q}(\sqrt{-19})}\theta_{19}(-1) = 4\cdot id_1 + 5\cdot\sigma_1$. Мы знаем, что $id_1 : \sqrt{-19}\to\sqrt{-19}$, $\sigma_1 : \sqrt{-19}\to-\sqrt{-19}$. Выбираем, какие автоморфизмы поля K действуют на $\sqrt{-19}$ как id_1. Таковыми будут являться id, ρ_1, ρ_2, ρ_3. Аналогично для σ_1: ρ_4, ρ_5, ρ_6, ρ_7. Таким образом, для подполя $\mathbb{Q}(\sqrt{-19})$ мы получаем следующий элемент Штикельбергера:

$$\theta'_{19}(-1) = 4\cdot id + 4\cdot\rho_1 + 4\cdot\rho_2 + 4\cdot\rho_3 + 5\cdot\rho_4 + 5\cdot\rho_5 + 5\cdot\rho_6 + 5\cdot\rho_7.$$

Распространим аналогичные рассуждения на остальные подполя:

$$\begin{aligned}
\theta'_{31}(-1) &= 6\cdot id + 6\cdot\rho_1 + 9\cdot\rho_2 + 9\cdot\rho_3 + 6\cdot\rho_4 + 6\cdot\rho_5 + 9\cdot\rho_6 + 9\cdot\rho_7,\\
\theta'_{43}(-1) &= 10\cdot id + 11\cdot\rho_1 + 10\cdot\rho_2 + 11\cdot\rho_3 + 10\cdot\rho_4 + 11\cdot\rho_5 + 10\cdot\rho_6 + 11\cdot\rho_7,\\
\theta'_{589}(-1) &= 68\cdot id + 68\cdot\rho_1 + 68\cdot\rho_2 + 68\cdot\rho_3 + 67\cdot\rho_4 + 67\cdot\rho_5 + 67\cdot\rho_6 + 67\cdot\rho_7,\\
\theta'_{817}(-1) &= 95\cdot id + 94\cdot\rho_1 + 95\cdot\rho_2 + 94\cdot\rho_3 + 95\cdot\rho_4 + 94\cdot\rho_5 + 95\cdot\rho_6 + 94\cdot\rho_7,\\
\theta'_{1333}(-1) &= 159\cdot id + 159\cdot\rho_1 + 156\cdot\rho_2 + 156\cdot\rho_3 + 159\cdot\rho_4 + 159\cdot\rho_5 + 156\cdot\rho_6 + 156\cdot\rho_7,\\
\theta'_{25327}(-1) &= 1423\cdot id + 1412\cdot\rho_1 + 1412\cdot\rho_2 + 1423\cdot\rho_3 + 1412\cdot\rho_4 + 1423\cdot\rho_5 +\\
&\quad + 1423\cdot\rho_6 + 1412\cdot\rho_7
\end{aligned}$$

Теперь перейдем к вычислению идеала Штикельбергера I. Первоначально мы умножаем каждый элемент Штикельбергера на автоморфизмы поля K, т.е. на $\{id, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7\}$. Рассмотрим $\theta'_{19}(-1)$ и умножим его на все автоморфизмы поля K:

$$\begin{aligned}
id\cdot\theta'_{19}(-1) &= 4\cdot id + 4\cdot\rho_1 + 4\cdot\rho_2 + 4\cdot\rho_3 + 5\cdot\rho_4 + 5\cdot\rho_5 + 5\cdot\rho_6 + 5\cdot\rho_7,\\
\rho_1\cdot\theta'_{19}(-1) &= 4\cdot id + 4\cdot\rho_1 + 4\cdot\rho_2 + 4\cdot\rho_3 + 5\cdot\rho_4 + 5\cdot\rho_5 + 5\cdot\rho_6 + 5\cdot\rho_7,\\
\rho_2\cdot\theta'_{19}(-1) &= 4\cdot id + 4\cdot\rho_1 + 4\cdot\rho_2 + 4\cdot\rho_3 + 5\cdot\rho_4 + 5\cdot\rho_5 + 5\cdot\rho_6 + 5\cdot\rho_7,\\
\rho_3\cdot\theta'_{19}(-1) &= 4\cdot id + 4\cdot\rho_1 + 4\cdot\rho_2 + 4\cdot\rho_3 + 5\cdot\rho_4 + 5\cdot\rho_5 + 5\cdot\rho_6 + 5\cdot\rho_7,\\
\rho_4\cdot\theta'_{19}(-1) &= 5\cdot id + 5\cdot\rho_1 + 5\cdot\rho_2 + 5\cdot\rho_3 + 4\cdot\rho_4 + 4\cdot\rho_5 + 4\cdot\rho_6 + 4\cdot\rho_7,\\
\rho_5\cdot\theta'_{19}(-1) &= 5\cdot id + 5\cdot\rho_1 + 5\cdot\rho_2 + 5\cdot\rho_3 + 4\cdot\rho_4 + 4\cdot\rho_5 + 4\cdot\rho_6 + 4\cdot\rho_7,\\
\rho_6\cdot\theta'_{19}(-1) &= 5\cdot id + 5\cdot\rho_1 + 5\cdot\rho_2 + 5\cdot\rho_3 + 4\cdot\rho_4 + 4\cdot\rho_5 + 4\cdot\rho_6 + 4\cdot\rho_7,\\
\rho_7\cdot\theta'_{19}(-1) &= 5\cdot id + 5\cdot\rho_1 + 5\cdot\rho_2 + 5\cdot\rho_3 + 4\cdot\rho_4 + 4\cdot\rho_5 + 4\cdot\rho_6 + 4\cdot\rho_7.
\end{aligned}$$

Заметим, что мы получили всего два различных элемента, а именно, $id \cdot \theta'_{19}(-1) = \rho_1 \cdot \theta'_{19}(-1) = \rho_2 \cdot \theta'_{19}(-1) = \rho_3 \cdot \theta'_{19}(-1)$ и $\rho_4 \cdot \theta'_{19}(-1) = \rho_5 \cdot \theta'_{19}(-1) = \rho_6 \cdot \theta'_{19}(-1) = \rho_7 \cdot \theta'_{19}(-1)$. Это произошло потому, что в элементе Штикельбергера $\theta'_{19}(-1)$ было всего два различных коэффициента. Если мы посмотрим на остальные элементы Штикельбергера, то заметим, что в их записях различных коэффициентов также два (однако это – частный случай, так будет не всегда). Запишем все различные элементы в множество I'. В нашем случае $\#I' = 14$. Окончательно идеал Штикельбергера заданного поля K примет вид:

$$
\begin{aligned}
I = (&4 \cdot id + 4 \cdot \rho_1 + 4 \cdot \rho_2 + 4 \cdot \rho_3 + 5 \cdot \rho_4 + 5 \cdot \rho_5 + 5 \cdot \rho_6 + 5 \cdot \rho_7,\\
&5 \cdot id + 5 \cdot \rho_1 + 5 \cdot \rho_2 + 5 \cdot \rho_3 + 4 \cdot \rho_4 + 4 \cdot \rho_5 + 4 \cdot \rho_6 + 4 \cdot \rho_7,\\
&6 \cdot id + 6 \cdot \rho_1 + 9 \cdot \rho_2 + 9 \cdot \rho_3 + 6 \cdot \rho_4 + 6 \cdot \rho_5 + 9 \cdot \rho_6 + 9 \cdot \rho_7,\\
&9 \cdot id + 9 \cdot \rho_1 + 6 \cdot \rho_2 + 6 \cdot \rho_3 + 9 \cdot \rho_4 + 9 \cdot \rho_5 + 6 \cdot \rho_6 + 6 \cdot \rho_7,\\
&10 \cdot id + 11 \cdot \rho_1 + 10 \cdot \rho_2 + 11 \cdot \rho_3 + 10 \cdot \rho_4 + 11 \cdot \rho_5 + 10 \cdot \rho_6 + 11 \cdot \rho_7,\\
&11 \cdot id + 10 \cdot \rho_1 + 11 \cdot \rho_2 + 10 \cdot \rho_3 + 11 \cdot \rho_4 + 10 \cdot \rho_5 + 11 \cdot \rho_6 + 10 \cdot \rho_7,\\
&68 \cdot id + 68 \cdot \rho_1 + 68 \cdot \rho_2 + 68 \cdot \rho_3 + 67 \cdot \rho_4 + 67 \cdot \rho_5 + 67 \cdot \rho_6 + 67 \cdot \rho_7,\\
&67 \cdot id + 67 \cdot \rho_1 + 67 \cdot \rho_2 + 67 \cdot \rho_3 + 68 \cdot \rho_4 + 68 \cdot \rho_5 + 68 \cdot \rho_6 + 68 \cdot \rho_7,\\
&95 \cdot id + 94 \cdot \rho_1 + 95 \cdot \rho_2 + 94 \cdot \rho_3 + 95 \cdot \rho_4 + 94 \cdot \rho_5 + 95 \cdot \rho_6 + 94 \cdot \rho_7,\\
&94 \cdot id + 95 \cdot \rho_1 + 94 \cdot \rho_2 + 95 \cdot \rho_3 + 94 \cdot \rho_4 + 95 \cdot \rho_5 + 94 \cdot \rho_6 + 95 \cdot \rho_7,\\
&159 \cdot id + 159 \cdot \rho_1 + 156 \cdot \rho_2 + 156 \cdot \rho_3 + 159 \cdot \rho_4 + 159 \cdot \rho_5 + 156 \cdot \rho_6 + 156 \cdot \rho_7,\\
&156 \cdot id + 156 \cdot \rho_1 + 159 \cdot \rho_2 + 159 \cdot \rho_3 + 156 \cdot \rho_4 + 156 \cdot \rho_5 + 159 \cdot \rho_6 + 159 \cdot \rho_7,\\
&1423 \cdot id + 1412 \cdot \rho_1 + 1412 \cdot \rho_2 + 1423 \cdot \rho_3 + 1412 \cdot \rho_4 + 1423 \cdot \rho_5 +\\
&\qquad + 1423 \cdot \rho_6 + 1412 \cdot \rho_7,\\
&1412 \cdot id + 1423 \cdot \rho_1 + 1423 \cdot \rho_2 + 1412 \cdot \rho_3 + 1423 \cdot \rho_4 + 1412 \cdot \rho_5 +\\
&\qquad + 1412 \cdot \rho_6 + 1423 \cdot \rho_7)
\end{aligned}
$$

Список литературы

[BBdV+17] Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal. Short generators without quantum computers: The case of multiquadratics. In Advances in Cryptology – EUROCRYPT 2017, pages 27–59, 2017.

[BEW98] Bruce C Berndt, Ronald J Evans, and Kenneth S Williams. Gauss and Jacobi sums. Wiley New York, 1998.

[BV19] Jean-Fransois Biasse and Christine Vredendaal. Fast multiquadratic s-unit computation and application to the calculation of class groups. The Open Book Series, 2:103–118, 01 2019.

[CDW17] Ronald Cramer, Leo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In Eucrocrypt, pages 324–348, 04 2017.

[HP08] Cohen H. and Stevenhagen P. Computational class field theory. https://arxiv.org/pdf/0802.3843.pdf, 2008.

[R.96] Kucera R. On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields. Journal of number theory 56, 1996.

[S09] Weintraub S. Galois Theory. Second Edition. Springer, 2009.

[Sin81] W. Sinnott. On the stickelberger ideal and the circular units of anabelian field. Inventiones Mathematicae, 62:181–234, 1980/81.

[Was82] L.C. Washington. Introduction to Cyclotomic Fields. Springer-Verlag, 1982.