The Ramanujan Journal _####################_
https://doi.org/10.1007/s11139-025-01146-y

On Gerth's heuristics for a family of quadratic extensions of certain Galois number fields

C. G. K. Babu[1] · R. Bera[2] · J. Sivaraman[3] · B. Sury[4]

Received: 25 April 2025 / Accepted: 15 June 2025

Abstract

Gerth generalised Cohen–Lenstra heuristics to the prime $p = 2$. He conjectured that [1] for any positive integer m, the limit

$$\lim_{X\to\infty} \frac{\sum_{\substack{0<D\le X,\\ \text{squarefree}}} |\mathrm{Cl}^2_{\mathbb{Q}(\sqrt{D})}/\mathrm{Cl}^4_{\mathbb{Q}(\sqrt{D})}|^m}{\sum_{\substack{0<D\le X,\\ \text{squarefree}}} 1}$$

exists and proposed a value for the limit. Gerth's conjecture was proved by Fouvry and Kluners in 2007. In this paper, we generalize their result by obtaining lower bounds for the average value of $|\mathrm{Cl}^2_{\mathbf{L}}/\mathrm{Cl}^4_{\mathbf{L}}|^m$, where $\mathbf{L}$ varies over an infinite family of quadratic extensions of certain Galois number fields. As a special case of our theorem we obtain lower bounds for the average value of $|\mathrm{Cl}^2_{\mathbf{L}}/\mathrm{Cl}^4_{\mathbf{L}}|^m$ as we vary $\mathbf{L}$ in an infinite family [2] of quadratic extensions of certain Galois number fields of class number 1 containing $\mathbb{Q}(i)$.

Keywords Class groups · Quadratic extensions

Mathematics Subject Classification Primary: 11R29 · 11R11 · Secondary: 11R45

1 Introduction

In 1984, based on some numerical evidence, Cohen and Lenstra made striking con- [3] jectures on the structure of the odd part of the (narrow) class group, and on divisibility

✉ J. Sivaraman
jyothsnaa.s@iisertvm.ac.in

[1] Indian Statistical Institute, Kolkata, West Bengal 700108, India

[2] Indian Statistical Institute, New Delhi, Delhi 110016, India

[3] Indian Institute of Science Education and Research Thiruvananthapuram, Maruthamala P. O., Vithura, Kerala 695551, India

[4] Indian Statistical Institute, 8th Mile, Mysore Rd, RVCE Post, Bengaluru, Karnataka 560059, India

properties for class numbers of quadratic fields. For instance, their predictions imply that, for any positive integer n, quadratic fields with class number divisible by n, must have positive density among the family of all quadratic fields. Among other things, Cohen–Lenstra's conjecture asserts that the probability that the class number of a real quadratic field is divisible by an odd prime p is

$$1-\prod_{n=2}^{\infty}(1-1/p^{n}).$$

A key idea of Cohen–Lenstra is to associate as a weight to the class group, the reciprocal of the order of its automorphism group. In 1987, F. Gerth modified the Cohen–Lenstra heuristics to the prime $p=2$ by considering the square of the class group. Twenty years later, E. Fouvry and J. Kluners ([3], [4]) confirmed these predictions on the 4-ranks of class groups $\mathrm{Cl}_{\mathbf{K}}$ of quadratic fields $\mathbf{K}$. Here, 4-rank refers to the $\mathbb{F}_2$-dimension of $\mathrm{Cl}_{\mathbf{K}}^2/\mathrm{Cl}_{\mathbf{K}}^4$. If f is a sufficiently nice, real-valued, positive function on the set of discriminants, one can define its average value in a natural manner. When f is the characteristic function of a set of discriminants satisfying some specific property, this average value - if it exists - is said to be the density of this set of discriminants. If $f(D)$ is of the form

$$\prod_{i=0}^{r}\left(2^{\dim_{\mathbb{F}_2}\left(\mathrm{Cl}^2_{\mathbb{Q}(\sqrt{D})}/\mathrm{Cl}^4_{\mathbb{Q}(\sqrt{D})}\right)}-2^{i}\right)$$

for some positive integer r, Fouvry-Kluners obtain the densities both for positive as well as negative fundamental discriminants D, thereby confirming Gerth's conjecture. In this paper, we follow their technique to treat the more general case of quadratic extensions of a class of number fields that have certain nice properties. We obtain lower bounds for the densities. The lower bound involves the number of subspaces of cardinality 2^m in $\mathbb{F}_2^{2m}$. This idea of employing the geometry of $\mathbb{F}_2$-vector spaces was a novel one introduced by Fouvry and Kluners. The idea was inspired by the work of Heath-Brown in [7] and [8]. In order to use their ideas, we restrict our base field to a family of class number one fields. Even though the outline of our proofs follows that of Fouvry and Kluners, we need to carry out a number of technical generalizations to adapt their proof. We use generalized versions of the Hilbert and Jacobi symbols, and of the Siegel-Walfisz theorem and other analytic estimates to complete our proof. Throughout this article, $\mathbf{K}$ will be a number field such that:

(1) the extension $\mathbf{K}/\mathbb{Q}$ is Galois,
(2) the ring of integers $\mathcal{O}_{\mathbf{K}}$ is a principal ideal domain, and
(3) there exists a unit $\varepsilon\in\mathcal{O}_{\mathbf{K}}^{*}$ such that the order of ε mod $\mathfrak{p}^2$ is 2 for all $\mathfrak{p}\mid 2\mathcal{O}_{\mathbf{K}}$.

Examples of quadratic fields satisfying the above conditions are $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{3})$ to name a few. Further, we show in Sect. 7 that certain Galois number fields with class number 1, containing $\mathbb{Q}(i)$ will also satisfy the above three conditions. We refer the reader to Sect. 7 for several explicit examples. For a number field $\mathbf{K}$, we shall use $n_{\mathbf{K}}$, $r_{\mathbf{K}}$ and $\mathfrak{N}$ to denote, respectively, its degree, rank of the unit group, and the norm map to $\mathbb{Q}$. Further, for a field extension $\mathbf{L}$ of $\mathbf{K}$, $\mathrm{Cl}_{\mathbf{L}}$ will denote the class group of $\mathbf{L}$ and $\mathrm{rk}_4(\mathrm{C}_{\mathbf{L}})$ will be used to denote the 4-rank of $\mathbf{L}$, viz.

$$\dim_{\mathbb{F}_2}\left(\mathrm{Cl}_{\mathbf{L}}^2/\mathrm{Cl}_{\mathbf{L}}^4\right).$$

Our aim is to obtain, for a family $\mathcal{F}$ of quadratic extensions of $\mathbf{K}$ and any positive integer m, a non-trivial lower bound for

$$\liminf_{X\to\infty}\frac{\sum_{\mathbf{L}\in\mathcal{F}(X)}2^{m\cdot\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})}}{\sum_{\mathbf{L}\in\mathcal{F}(X)}1}$$

where $\mathcal{F}(X)$ is used to denote the set of number of fields in $\mathcal{F}$ for which the absolute norm of relative discriminant of $\mathbf{L}/\mathbf{K}$ is at most X.

We became aware of some results due to Alexander Smith (“The Distribution of ℓ^∞-Selmer groups in Degree ℓ Twist Families I” - arxiv:2207.05674v2 [math.NT] 8 Feb 2023, and “The Distribution of ℓ^∞-Selmer groups in Degree ℓ Twist Families II" - arxiv:2207.05143v2 [math.NT] 8 Feb 2023). Smith's methods are very general, and address also Selmer groups associated to elliptic curves. We have not succeeded so far in deducing our results from those of Smith. In [17], he considers in Theorem 1.12, number fields F which do not contain the 2ℓ-th roots of unity. On page 17 of [18], prior to Remark 3.12, he also makes the comment: “In our estimation, it should be challenging but possible to adjust the methods of this paper and [17] to compute the distribution of class groups in the presence of extra roots of unity." We are able to consider some families of fields containing i as well (see the last section). Our methods are comparatively elementary, and considering that it is not obvious to us how they may follow from Smith's work, we feel that publishing them would be of interest to others.

Choosing the family $\mathcal{F}$ of quadratic extensions of K

We state first a lemma due to Smith [19] to help us in selecting an appropriate family of quadratic extensions of $\mathbf{K}$.

Lemma 1 (H. Smith [19]) *Let $\mathfrak{p}$ be a prime above $2\mathbb{Z}$ in $\mathbf{K}$. We use f to denote the residue class degree of $\mathfrak{p}$ over $\mathbb{Q}$. Let $\mathbf{L}=\mathbf{K}(\sqrt{\alpha})$ for some $\alpha\in\mathcal{O}_{\mathbf{K}}$. Then $\mathcal{O}_{\mathbf{L}}=\mathcal{O}_{\mathbf{K}}[\sqrt{\alpha}]$ if and only if $\alpha\mathcal{O}_{\mathbf{K}}$ is square free and*

$$\alpha^{2^f}\not\equiv\alpha \bmod \mathfrak{p}^2 \qquad \textit{for all } \mathfrak{p}\mid 2\mathcal{O}_{\mathbf{K}}.$$

Let $\mathbf{M}$ be the compositum of $\mathbf{K}_{4\mathcal{O}_{\mathbf{K}}}$ and $\mathbf{K}((\mathcal{O}_{\mathbf{K}}^*)^{1/2})$ and let $\mathfrak{f}$ be the conductor of $\mathbf{M}/\mathbf{K}$. Here $\mathbf{K}_{4\mathcal{O}_{\mathbf{K}}}$ (resp. $\mathbf{K}_{\mathfrak{f}}$) is the ray class field of $\mathbf{K}$ with respect to the modulus $4\mathcal{O}_{\mathbf{K}}$ (resp. $\mathfrak{f}$). We will now define a family of quadratic extensions of such a field $\mathbf{K}$.

Definition 2 Let ζ_j be a generator of the subgroup of the roots of unity in K and let $S=\{\varepsilon_1,\ldots,\varepsilon_r\}$ be a set of fundamental units generating $\mathcal{O}_{\mathbf{K}}^*$ modulo its torsion part.

We denote by $\mathcal{C}$ the product of the absolute norms of the conductors of the orders $\mathcal{O}_{\mathbf{K}}[\sqrt{\varepsilon}]$ in $\mathcal{O}_{\mathbf{K}(\sqrt{\varepsilon})}$ as we vary ε in the set $S \cup \{\zeta_j\}$. Let

$$\mathcal{P}_{\mathbf{K}} = \{\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}} : (\mathfrak{p}, \mathcal{C}\mathcal{O}_{\mathbf{K}}) = \mathcal{O}_{\mathbf{K}} \text{ and } \mathfrak{p} \text{ splits in } \mathbf{K}_{\mathfrak{f}}\} \text{ and we set } P_{\mathbf{K}}(X) = \prod_{\substack{\mathfrak{p}\in\mathcal{P}_{\mathbf{K}},\\ \mathfrak{N}(\mathfrak{p})\leq X}} \mathfrak{p}.$$

Definition 3 Let

$$\mathcal{W} = \{\alpha\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_{\mathbf{K}} : \mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}} \implies \mathfrak{p} \in \mathcal{P}_{\mathbf{K}}, \alpha\mathcal{O}_{\mathbf{K}} \text{ square free } \} \text{ and} \tag{1}$$

$$\mathcal{W}(X) = \{\alpha\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_{\mathbf{K}} : \mathfrak{N}(\alpha\mathcal{O}_{\mathbf{K}}) \leq X,\ \alpha\mathcal{O}_{\mathbf{K}} \mid P_{\mathbf{K}}(X)\}. \tag{2}$$

For a generator α of $\alpha\mathcal{O}_{\mathbf{K}}$ such that

$$\alpha^{2^f} \not\equiv \alpha \bmod \mathfrak{p}^2 \quad \text{for all } \mathfrak{p} \mid 2\mathcal{O}_{\mathbf{K}}, \tag{3}$$

we set $\mathbf{L}_\alpha$ to be $\mathbf{K}(\sqrt{\alpha})$.

It stands to question why an α satisfying (3) should exist for $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$. To see this, we note that by condition 3 there exists a unit $\varepsilon \in \mathcal{O}_{\mathbf{K}}^*$ such that order of ε mod $\mathfrak{p}^2$ is 2 for all $\mathfrak{p} \mid 2\mathcal{O}_{\mathbf{K}}$. If there exists a generator α for the ideal $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$ satisfying (3), we are done. If not, the generator $\varepsilon\alpha$ will satisfy (3).

Finally we define

$$\mathcal{F}' := \{\mathbf{L}_\alpha : \alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}\}.$$

For each such $\mathbf{L}_\alpha \in \mathcal{F}'$, by Lemma 1 we now have $\mathcal{O}_{\mathbf{L}_\alpha} = \mathcal{O}_{\mathbf{K}}[\sqrt{\alpha}]$. Since $\{1, \sqrt{\alpha}\}$ is a relative integral basis of $\mathcal{O}_{\mathbf{L}_\alpha}/\mathcal{O}_{\mathbf{K}}$, we know that $\mathfrak{d}_{\mathbf{L}_\alpha/\mathbf{K}} = 4\alpha\mathcal{O}_{\mathbf{K}}$. We now choose a set $\mathcal{F} \subset \mathcal{F}'$ such that

- for any $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$, $\mathbf{L}_{\alpha_1} \in \mathcal{F}$ for exactly one generator α_1 of $\alpha\mathcal{O}_{\mathbf{K}}$.

Let us also set for convenience the following notation:

$$\mathcal{F}(X) := \{\mathbf{L} \in \mathcal{F} : \mathfrak{N}(\mathfrak{d}_{\mathbf{L}/\mathbf{K}}) \leq 4X\}.$$

We state the main theorem of our article now.

Theorem 4 *For any positive integer m and X varying in* $\mathbb{R}$,

$$\liminf_{X\to\infty} \frac{\sum_{\mathbf{L}\in\mathcal{F}(X)} 2^{m\cdot rk_4(\mathrm{Cl}_{\mathbf{L}})}}{\sum_{\mathbf{L}\in\mathcal{F}(X)} 1} \geq \frac{\mathcal{N}(2m, 2)}{2^{m(r_{\mathbf{K}}+1)}}.$$

Here $\mathcal{N}(2m, 2)$ *is used to denote the number of subspaces of* $\mathbb{F}_2^{2m}$ *of* 2^m *elements.*

Infinitude of the family $\mathcal{F}$ follows from Chebotarev's density theorem. In Sect. 2, we compute an asymptotic for the cardinality of the set $\mathcal{F}(X)$ as $X \to \infty$. In order to prove our theorem, an important ingredient is a lower bound for $2^{rk_4(\mathrm{Cl}_{\mathbf{L}})}$ for $\mathbf{L} \in \mathcal{F}$.

This is computed in Sect. 3. In Sect. 4 we recall the definition of Ray class groups and introduce an analogue of the Jacobi symbol which will play the main role in the proof of Theorem 4. We also prove certain properties of this new symbol. Section 5 has been divided into two parts. Section 5.1 deals with the divisor function, some of its variants and their average orders. In Sect. 5.2 we state some important character sum results such as the Large Sieve inequality for number fields, Siegel-Walfisz for number fields and prove a generalisation of a Lemma of Heilbronn. In Sect. 6 we begin computing a lower bound for the average of $2^{m\cdot \mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})}$ as $\mathbf{L}$ varies in $\mathcal{F}$, for any positive integer m. This section is divided into several parts. Sections 6.1 and 6.2 are devoted to rewriting the main sum and bounding the contribution of certain subsums, culminating in Propostion 39. In Proposition 41 we state a result on the indices of this new sum which are not "linked" (see Sect. 6 for definition). This will be used to rewrite the main sum of Proposition 39 in Sect. 6.4. We complete the proof of Theorem 4 in Sect. 6.4. Finally, we conclude with examples of fields $\mathbf{K}$ which satisfy conditions 1, 2 and 3 in Sect. 7.

2 Cardinality of $\mathcal{F}(X)$

We begin by noting that

$$\#\mathcal{F}(X) = \#\{\alpha\mathcal{O}_{\mathbf{K}} : \alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}(X)\} = \sum_{\substack{\mathfrak{N}(\alpha\mathcal{O}_{\mathbf{K}})\le X,\\ \alpha\mathcal{O}_{\mathbf{K}} | P_{\mathbf{K}}(X)}} 1$$

We recall here a version of the Tauberian theorem as seen in [15]. Let us define the Dirichlet series

$$f(s) = \sum_{\substack{\mathfrak{a}\neq(0)\\ \mathfrak{a}\subset\mathcal{O}_{\mathbf{K}}}} \frac{b_{\mathfrak{a}}}{\mathfrak{N}\mathfrak{a}^s} = \prod_{\mathfrak{p}\in\mathcal{P}_{\mathbf{K}}} \left(1 + \frac{1}{\mathfrak{N}\mathfrak{p}^s}\right), \ \Re(s) > 1 \tag{4}$$

where $b_{\mathfrak{a}} = 1$ if and only if $\mathfrak{a}$ is squarefree and composed only of the primes in $\mathcal{P}_{\mathbf{K}}$. If $a_n = \sum_{\mathfrak{N}\mathfrak{a}=n} b_{\mathfrak{a}}$, we have

$$f(s) = \sum_{n>0} \frac{a_n}{n^s}. \tag{5}$$

Theorem 5 *Let* $0 < \kappa < 1$ *be a real number. Suppose that we can write*

$$f(s) = \frac{h(s)}{(s-1)^{1-\kappa}}$$

for some $h(s)$ holomorphic in $\Re(s) \geq 1$ and non-zero there. Then

$$\sum_{n \leq x} a_n \sim \frac{d(\kappa) x}{(\log x)^{\kappa}}$$

where $d(\kappa) = h(1)/\Gamma(1-\kappa)$.

In $\Re(s) > 1$, since f does not vanish in this region, one may take logarithms on either side of (4). Now applying the series expansion for logarithms, we get

$$\log f(s) = \sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1 \\ (\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} + \sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1 \\ (\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \sum_{m \geq 2} \frac{(-1)^{m+1}}{m \mathfrak{N}\mathfrak{p}^{ms}} = \sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1, \\ (p,\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} + \theta(s)$$

where

$$\theta(s) = \sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1 \\ (\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \sum_{m \geq 2} \frac{(-1)^{m+1}}{m \mathfrak{N}\mathfrak{p}^{ms}} \quad \text{and}$$

$(\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})$ is the Artin symbol of $\mathfrak{p}$ with respect to the abeiian extensnion $\mathbf{K}_{\mathfrak{f}}/\mathbf{K}$. Note that for $\Re(s) = \sigma$,

$$|\theta(s)| \leq \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{1}{m \mathfrak{N}\mathfrak{p}^{m\sigma}} \leq \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}\mathfrak{p}^{\sigma}(\mathfrak{N}\mathfrak{p}^{\sigma} - 1)} \leq n_{\mathbf{K}} \sum_{p} \frac{1}{p^{\sigma}(p^{\sigma} - 1)}$$

where $n_{\mathbf{K}} = [\mathbf{K} : \mathbb{Q}]$. Therefore, $\theta(s)$ is holomorphic on $\Re(s) > 1/2$. By orthogonality of generalised Dirichlet characters modulo $\mathfrak{f}$ we get

$$\sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1 \\ (\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} = \frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|} \sum_{(\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}} \sum_{\chi \bmod \mathfrak{f}} \frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s}.$$

In $\Re(s) > 1$ we can interchange the sums to get

$$\begin{aligned}
\sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1 \\ (\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} &= \frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|} \sum_{\chi \bmod \mathfrak{f}} \sum_{(\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}} \frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s} \\
&= \frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|} \sum_{\chi \bmod \mathfrak{f}} \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s} + \frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|} \sum_{\chi \bmod \mathfrak{f}} \sum_{\mathfrak{p} | \mathcal{C}\mathcal{O}_{\mathbf{K}}} \frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s}.
\end{aligned}$$

However this now gives us

$$\sum_{\substack{(\mathfrak{p},\mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1 \\ (\mathfrak{p},\mathcal{C}\mathcal{O}_{\mathbf{K}})=\mathcal{O}_{\mathbf{K}}}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} = \frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|} \sum_{\chi \bmod \mathfrak{f}} (\log L(s,\chi) + \theta_{1,\chi}(s)) \tag{6}$$

where $\theta_{1,\chi}(s)$ is holomorphic on $\Re(s) \geq 1/2$ for all χ modulo $\mathfrak{f}$ (by the same argument as seen above for $f(s)$). Since $L(s, \chi_0)$ extends to a meromorphic function on $\mathbb{C}$ with only a simple pole at $s = 1$ we have

$$L(s, \chi_0) = \frac{\theta_2(s)}{(s-1)}$$

with $\theta_2(s)$ entire. We have

$$\theta_2(s) = (s-1)L(s, \chi_0) = (s-1)\zeta_{\mathbf{K}}(s) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \frac{1}{\mathfrak{N}\mathfrak{p}^s}\right)$$

and the product

$$\prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \frac{1}{\mathfrak{N}\mathfrak{p}^s}\right)$$

is entire and non-zero in $\Re(s) \geq 1/2$. Now by the zero free region for $\zeta_{\mathbf{K}}(s)$ (see lemma 8.1 and 8.2 of [11]), we have a simply connected region containing $\Re(s) \geq 1$ in which $\theta_2(s)$ is non-zero. Therefore

$$\log L(s, \chi_0) = \log \frac{1}{(s-1)} + \theta_3(s)$$

where $\theta_3(s) = \log \theta_2(s)$ which is holomorphic in $\Re(s) \geq 1$. For $\chi \neq \chi_0$, $L(s, \chi)$ extends to an entire function (see corollary 8.6 on page 503 of [14]). Again by the zero free regions for each $L(s, \chi)$ (from the zero free region for $\zeta_{\mathbf{K}_\mathfrak{f}}(s)$ and the factorisation $\zeta_{\mathbf{K}_\mathfrak{f}}(s) = \prod_{\chi \bmod \mathfrak{f}} L(s, \chi^*)$) we have a simply connected region containing $\Re(s) \geq 1$ in which $L(s, \chi)$ is non-zero. In this region it follows that $\log L(s, \chi)$ can be defined and is holomorphic. Combining all these observations and substituting in (6) we get

$$\sum_{\substack{(\mathfrak{p}, \mathbf{K}_\mathfrak{f}/\mathbf{K})=1 \\ (\mathfrak{p}, \mathcal{C}\mathcal{O}_\mathbf{K})=\mathcal{O}_\mathbf{K}}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} = -\frac{1}{|H_\mathfrak{f}(\mathbf{K})|} \log(s-1) + \theta_4(s)$$

where $\theta_4(s)$ is holomorphic on $\Re(s) \geq 1$. Taking exponentials, we get

$$f(s) = \frac{h(s)}{(s-1)^{\frac{1}{|H_\mathfrak{f}(\mathbf{K})|}}}$$

with $h(s) = e^{\theta(s)+\theta_4(s)}$ holomorphic in $\Re(s) \geq 1$ and non-zero there. We can now apply the above Tauberian theorem to deduce that

$$\#\{\alpha\mathcal{O}_\mathbf{K} : \alpha\mathcal{O}_\mathbf{K} \in \mathcal{W}(X)\} \sim \frac{d_\mathcal{C}(1 - 1/|H_\mathfrak{f}(\mathbf{K})|)X}{(\log X)^{1-\frac{1}{|H_\mathfrak{f}(\mathbf{K})|}}}.$$

Therefore, we have

$$\mathcal{F}(X) \sim \frac{d_{\mathcal{C}}(1 - 1/|H_{\mathfrak{f}}(\mathbf{K})|)X}{(\log X)^{1-\frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|}}}.$$

3 Lower bound for $2^{\mathrm{rk}_4(\mathrm{Cl}_\mathbf{L})}$

Throughout this section we assume $\mathbf{L} \in \mathcal{F}$.

Definition 6 We say that a class $[\mathfrak{a}]$ in the group $Cl_\mathbf{L}$ is strongly ambiguous if it contains an ideal $\mathfrak{a}$ such that $\mathfrak{a} = \sigma(\mathfrak{a})$ for a generator $\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. We denote the subgroup of all such classes in the class group by $\mathrm{Am}_{st}(\mathbf{L}/\mathbf{K})$.

We now recall the class number formula for strongly ambiguous classes.

Theorem 7 *(*see [13]*) The number of strongly ambiguous classes is given by*

$$\#\mathrm{Am}_{st}(\mathbf{L}/\mathbf{K}) = h(\mathbf{K}) \cdot \frac{2^{t_{1,\mathbf{L}}+t_{2,\mathbf{L}}-1}}{[\mathcal{O}_\mathbf{K}^* : N_{\mathbf{L}/\mathbf{K}}(\mathcal{O}_\mathbf{L}^*)]}$$

where $t_{1,\mathbf{L}}$ is the number of prime ideals in $\mathcal{O}_\mathbf{K}$ ramified in $\mathbf{L}$ and $t_{2,\mathbf{L}}$ is the number of primes at infinity of $\mathbf{K}$ which ramify in $\mathbf{L}$.

The subgroup of classes in $Cl_\mathbf{L}$, generated by the primes of $\mathbf{K}$ which ramify in $\mathbf{L}$ is contained in the group of strongly ambiguous classes of the class group. On the other hand consider a strongly ambiguous class represented by a fractional ideal $\mathfrak{a}$ of $\mathbf{L}$ such that $\mathfrak{a} = \sigma(\mathfrak{a})$, then let $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_k^{s_k}$ with all the $\mathfrak{p}_i$ being distinct prime ideals of $\mathcal{O}_\mathbf{L}$. Since $\sigma(\mathfrak{a}) = \mathfrak{a}$ every prime $\mathfrak{p}_i = \sigma(\mathfrak{p}_j)$ for some $1 \leq j \leq k$ and $s_i = s_j$ (by unique factorisation of ideals in a Dedekind domain and distinctness of the $\sigma(\mathfrak{p}_j)$'s). This implies that if $\mathfrak{p}_i$ lies above a prime of $\mathbf{K}$ that splits in $\mathbf{L}$, $I := \mathfrak{p}_i\mathfrak{p}_j = \mathfrak{p}_i\sigma(\mathfrak{p}_i)$ divides $\mathfrak{a}$ and I is principal. If $\mathfrak{p}_i = \sigma(\mathfrak{p}_i)$ it lies above a prime of $\mathbf{K}$ that is either inert or ramified. If $\mathfrak{p}_i$ is above an inert prime, it is already principal since $\mathcal{O}_\mathbf{K}$ is a PID. Any other $\mathfrak{p}_i$ must lie above a ramified prime. This implies that $\mathrm{Am}_{st}(\mathbf{L}/\mathbf{K})$ lies in the subgroup generated by the classes of ramified primes of $\mathbf{L}/\mathbf{K}$.

Remark 8 We note that in our context $h(\mathbf{K}) = 1$ and we set $[\mathcal{O}_\mathbf{K}^* : N_{\mathbf{L}/\mathbf{K}}(\mathcal{O}_\mathbf{L}^*)] = 2^{\tilde{e}_\mathbf{L}}$.

Definition 9 We will use $\tilde{\mathfrak{B}}_\mathbf{L}$ to denote the set of ideals

$$\{\mathfrak{P}'^{e_1}_1 \mathfrak{P}'^{e_2}_2 \cdots \mathfrak{P}'^{e_{t_{1,\mathbf{L}}}}_{t_{1,\mathbf{L}}} : \mathfrak{P}'_i \mid 4\alpha\mathcal{O}_\mathbf{L} \text{ prime, } e_i \in \{0, 1\} \text{ for all } i \in \{1, \ldots t_{1,\mathbf{L}}\}\}.$$

Further let $\mathfrak{B}_\mathbf{L}$ denote the set of ideals

$$\{\mathfrak{P}^{e_1}_1 \mathfrak{P}^{e_2}_2 \cdots \mathfrak{P}^{e_{t'_{1,\mathbf{L}}}}_{t'_{1,\mathbf{L}}} : \mathfrak{P}_i \mid \alpha\mathcal{O}_\mathbf{L} \text{ prime, } e_i \in \{0, 1\} \text{ for all } i \in \{1, \ldots t'_{1,\mathbf{L}}\}\}$$

where $t'_{1,\mathbf{L}}$ is used to denote the primes of $\mathbf{K}$, not lying above $2\mathbb{Z}$ but ramifying in $\mathbf{L}$.

Remark 10 We have $\mathrm{Am}_{st}(\mathbf{L}/\mathbf{K}) = \{[\mathfrak{b}] : \mathfrak{b} \in \tilde{\mathfrak{B}}_{\mathbf{L}}\}$. Given a $[\mathfrak{b}] \in \mathrm{Am}_{st}(\mathbf{L}/\mathbf{K})$ there is a bijection between

$$\{\mathfrak{b}_1 \in \tilde{\mathfrak{B}}_{\mathbf{L}} : \mathfrak{b}_1 \text{ principal }\} \leftrightarrow \{\mathfrak{b}_2 \in \tilde{\mathfrak{B}}_{\mathbf{L}} : \mathfrak{b}_2 \in [\mathfrak{b}]\}.$$

The map from the left to right is obtained by sending $\mathfrak{b}_1$ to $\mathfrak{b}\mathfrak{b}_1/\gcd(\mathfrak{b}, \mathfrak{b}_1)^2$. Further, the inverse map is also given by sending $\mathfrak{b}_2$ to $\mathfrak{b}\mathfrak{b}_2/\gcd(\mathfrak{b}, \mathfrak{b}_2)^2$. Since

$$\frac{\mathfrak{b} \cdot \mathfrak{b}\mathfrak{b}_1/\gcd(\mathfrak{b}, \mathfrak{b}_1)^2}{\gcd(\mathfrak{b}, \mathfrak{b}\mathfrak{b}_1/\gcd(\mathfrak{b}, \mathfrak{b}_1)^2)^2} = \mathfrak{b}_1$$

these maps constitute bijections. We now conclude that each class $[\mathfrak{b}] \in \tilde{\mathfrak{B}}_{\mathbf{L}}$ has exactly k representatives in $\tilde{\mathfrak{B}}_{\mathbf{L}}$ where

$$k = \#\{\mathfrak{b}_1 \in \tilde{\mathfrak{B}}_{\mathbf{L}} : \mathfrak{b}_1 \text{ principal }\}.$$

We now observe that

$$\#\tilde{\mathfrak{B}}_{\mathbf{L}} = \sum_{[\mathfrak{b}] \in \mathrm{Am}_{st}(\mathbf{L}/\mathbf{K})} \#\{\mathfrak{b}_2 \in \tilde{\mathfrak{B}}_{\mathbf{L}} : \mathfrak{b}_2 \in [\mathfrak{b}]\} = k \cdot \#\mathrm{Am}_{st}(\mathbf{L}/\mathbf{K}).$$

It follows from the ambiguous class number formula that

$$k = 2^{1-t_{2,\mathbf{L}}}[\mathcal{O}_{\mathbf{K}}^* : N_{\mathbf{L}/\mathbf{K}}(\mathcal{O}_{\mathbf{L}}^*)] = 2^{\tilde{e}_{\mathbf{L}}+1-t_{2,\mathbf{L}}}.$$

Further, we have

$$[\mathcal{O}_{\mathbf{K}}^* : N_{\mathbf{L}/\mathbf{K}}(\mathcal{O}_{\mathbf{L}}^*)] \leq [\mathcal{O}_{\mathbf{K}}^* : (\mathcal{O}_{\mathbf{K}}^*)^2] \leq 2^{r_{\mathbf{K}}+1}.$$

where $r_{\mathbf{K}}$ is the unit rank of $\mathcal{O}_{\mathbf{K}}^*$. So $\tilde{e}_{\mathbf{L}} \leq r_{\mathbf{K}} + 1$.

Lemma 11 *For any* $\mathbf{L} \in \mathcal{F}$,

$$2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})} \geq \frac{1}{2^{r_{\mathbf{K}}+2}} |\{\mathfrak{b} \in \mathfrak{B}_{\mathbf{L}} : [\mathfrak{b}] \in \mathrm{Cl}_{\mathbf{L}}, [\mathfrak{b}] = [\mathfrak{a}^2] \text{ for some non-zero fractional ideal } \mathfrak{a} \text{ of } \mathcal{O}_{\mathbf{L}}\}|.$$

Proof By definition

$$\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}}) = \dim_{\mathbb{F}_2}\left(\mathrm{Cl}_{\mathbf{L}}^2/\mathrm{Cl}_{\mathbf{L}}^4\right).$$

Therefore

$$2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})} = |\mathrm{Cl}_{\mathbf{L}}^2/\mathrm{Cl}_{\mathbf{L}}^4| = |\{B^2 \in \mathrm{Cl}_{\mathbf{L}} : B^4 = [\mathcal{O}_{\mathbf{L}}]\}|.$$

However

$$\{B^2 \in \mathrm{Cl}_{\mathbf{L}} : B^4 = [\mathcal{O}_{\mathbf{L}}]\} \supseteq \{[\mathfrak{b}] \in \mathrm{Cl}_{\mathbf{L}} : \mathfrak{b} \in \tilde{\mathfrak{B}}_{\mathbf{L}}, [\mathfrak{b}] = [\mathfrak{a}^2] \text{ for some non-zero fractional ideal } \mathfrak{a} \text{ of } \mathcal{O}_{\mathbf{L}}\}.$$

Therefore we have

$$\begin{aligned}2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})} &\geq \frac{1}{2^{r_{\mathbf{K}}+2}}|\{\mathfrak{b}\in \tilde{\mathfrak{B}}_{\mathbf{L}} : [\mathfrak{b}]\in \mathrm{Cl}_{\mathbf{L}}, [\mathfrak{b}]=[\mathfrak{a}^2]\\ &\quad\ \text{for some non-zero fractional ideal } \mathfrak{a} \text{ of } \mathcal{O}_{\mathbf{L}}\}|\\ &\geq \frac{1}{2^{r_{\mathbf{K}}+2}}|\{\mathfrak{b}\in \mathfrak{B}_{\mathbf{L}} : [\mathfrak{b}]\in \mathrm{Cl}_{\mathbf{L}}, [\mathfrak{b}]=[\mathfrak{a}^2]\\ &\quad\ \text{for some non-zero fractional ideal } \mathfrak{a} \text{ of } \mathcal{O}_{\mathbf{L}}\}|.\end{aligned}$$

□

We now define an analogue of the usual Hilbert symbol and some of its properties with an aim to characterise the lower bound in Lemma 11.

Definition 12 For $a, b \in \mathbf{K}^*$, we define

$$(a|b)\ :\ \mathbf{K}^* \times \mathbf{K}^* \to \{0, 1\}$$

where

$$(a|b) = \begin{cases} 1 & \text{if } x^2 = ay^2 + bz^2 \text{ has a non-zero solution in } \mathbf{K}^3 \\ 0 & \text{otherwise.}\end{cases}$$

The next proposition shows the equivalence of three useful properties which will be used to simplify the bound in Lemma 11.

Proposition 13 *For any $\mathbf{L} = \mathbf{L}_\alpha \in \mathcal{F}$ and $\mathfrak{b} \in \mathfrak{B}_{\mathbf{L}}$, we denote by $b\mathcal{O}_{\mathbf{K}}$ the ideal $\mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\mathfrak{b})$. Then the following are equivalent:*

(1) $[\mathfrak{b}] = [\mathfrak{a}^2]$ *for some non-zero fractional ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbf{L}}$.*
(2) $b\varepsilon$ *is a norm of an element in $\mathbf{L}^*$ for some $\varepsilon \in \mathcal{O}_{\mathbf{K}}^*$.*
(3) $(\alpha|b\varepsilon) = 1$.

Proof (1) $\iff$ (2):
For the forward implication, suppose $(\gamma_2) = \mathfrak{a}^2\mathfrak{b}^{-1}$. Taking norms on both sides we get

$$\mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\gamma_2\mathcal{O}_{\mathbf{L}}) = b\frac{\mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\mathfrak{a}^2)}{b^2}$$

where $b\mathcal{O}_{\mathbf{K}} = \mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\mathfrak{b})$. Since $\mathcal{O}_{\mathbf{K}}$ is a PID we have a $\gamma_3 \in \mathbf{K}^*$ such that $(\gamma_3) = \mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\mathfrak{a})$. By Lemma 13 on page 25 of [20], we have

$$\mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\gamma_2\mathcal{O}_{\mathbf{L}}) = N_{\mathbf{L}/\mathbf{K}}(\gamma_2)\mathcal{O}_{\mathbf{K}}.$$

Therefore

$$\mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\gamma_2\mathcal{O}_{\mathbf{L}}) = N_{\mathbf{L}/\mathbf{K}}(\gamma_2)\mathcal{O}_{\mathbf{K}} = b\frac{\gamma_3^2}{b^2}\mathcal{O}_{\mathbf{K}} = bN_{\mathbf{L}/\mathbf{K}}(\gamma_3/b)\mathcal{O}_{\mathbf{K}}.$$

This gives us assertion (2).

Conversely, let $b\varepsilon = N_{\mathbf{L}/\mathbf{K}}(\gamma_4)$ for some $\gamma_4 \in \mathbf{L}^*$. We know that γ_4 must be of the form γ_5/γ_6 where $\gamma_5 \in \mathcal{O}_{\mathbf{L}}$ and $\gamma_6 \in \mathcal{O}_{\mathbf{K}}$. Rationalising denominators, we get

$$b\varepsilon\gamma_6^2 = N_{\mathbf{L}/\mathbf{K}}(\gamma_5).$$

If a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$ divides $\gamma_5\mathcal{O}_{\mathbf{L}}$, that is, $\mathfrak{p}\mathcal{O}_{\mathbf{L}} \mid \gamma_5\mathcal{O}_{\mathbf{L}}$, then $\mathfrak{p}^2 \mid b\varepsilon\gamma_6^2\mathcal{O}_{\mathbf{K}}$. Since $b\mathcal{O}_{\mathbf{K}}$ is square-free, $\mathfrak{p}^2 \mid \gamma_6^2\mathcal{O}_{\mathbf{K}}$. Therefore by dividing on both sides by a generator of the principal ideal $\mathfrak{p}^2$, we may assume that $\mathfrak{p}\mathcal{O}_{\mathbf{L}} \nmid \gamma_5\mathcal{O}_{\mathbf{L}}$ for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$. However for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$ dividing $\gamma_6\mathcal{O}_{\mathbf{K}}$ we must have $\mathfrak{p}^2 \mid \mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\gamma_5\mathcal{O}_{\mathbf{L}})$. Therefore there exists an ideal $I \subset \mathcal{O}_{\mathbf{L}}$ with $I^2 \mid \gamma_5\mathcal{O}_{\mathbf{L}}$ and $\mathfrak{N}(I) = \mathfrak{p}$. Finally, there is a unique ideal of norm $b\mathcal{O}_{\mathbf{K}}$ given by some $\mathfrak{b} \in \mathfrak{B}_{\mathbf{L}}$. Combining the above we get

$$\gamma_5\mathcal{O}_{\mathbf{L}} = \mathfrak{b}\mathfrak{a}^2 \text{ for some non-zero integral ideal } \mathfrak{a} \text{ of } \mathcal{O}_{\mathbf{L}}.$$

(2) $\iff$ (3):

For the forward implication, if $b\varepsilon$ is a norm in $\mathbf{K}$ of an element of $\mathbf{L}$, then there exist $x, y \in \mathbf{K}$ such that $x^2 - \alpha y^2 = b\varepsilon$. Therefore $(\alpha|b\varepsilon) = 1$. Conversely, if $(\alpha|b\varepsilon) = 1$, there exists a non-trivial tuple $(x, y, z) \in \mathbf{K}^3$ such that

$$\alpha x^2 + b\varepsilon y^2 = z^2.$$

Rewriting the same, we get

$$b\varepsilon y^2 = z^2 - \alpha x^2.$$

Since the ideal $\alpha\mathcal{O}_{\mathbf{K}}$ is square-free, $\sqrt{\alpha} \notin \mathbf{K}$. Therefore y is non-zero. Now dividing by y^2 we get the lemma. □

We will now prove some properties of the aforementioned analogue of the Hilbert symbol.

Lemma 14 *[4] We have $(a|b) = (b|a) = (a|-ab)$ and $(ac^2|b) = (a|b)$.*

Remark 15 For an arbitrary squarefree integral ideal $I \subset \mathcal{O}_{\mathbf{K}}$, we say that an element $\gamma \in \mathcal{O}_{\mathbf{K}}$, with $(\gamma\mathcal{O}_{\mathbf{K}}, I) = \mathcal{O}_{\mathbf{K}}$, is a square modulo I if it is a quadratic residue modulo every prime ideal $\mathfrak{p} \mid I$.

Lemma 16 *For any ideal $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$, we have*

$$2 \mid [(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^* : \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{p}], \textit{ for all } \mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}}.$$

Proof By definition of $\alpha\mathcal{O}_{\mathbf{K}}$, $(\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K}) = 1$ for all $\mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}}$. Now consider the field $\mathbf{K}(\sqrt{\varepsilon})$ for any element ε of the set $S \cup \{\zeta_j\}$ considered in definition 2. Since $\mathbf{K}(\sqrt{\varepsilon}) \subset \mathbf{K}_{\mathfrak{f}}$, $\mathfrak{p}$ splits in $\mathbf{K}_1 = \mathbf{K}(\sqrt{\varepsilon})$. To apply the Dedekind-Kummer theorem (see page 47 of [14]) , we note that any prime $\mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}}$ is co-prime to the conductor of

$\mathcal{O}_{\mathbf{K}}[\sqrt{\varepsilon}]$ in $\mathcal{O}_{\mathbf{K}_1}$. Therefore $X^2-\varepsilon$ splits modulo $\mathfrak{p}$. Therefore for any element, ε of $S\cup\{\zeta_j\}$, we have

$$2 \mid [(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^* : \langle\varepsilon\rangle \bmod \mathfrak{p}].$$

Applying the same to all the elements of $S\cup\{\zeta_j\}$ and using the fact that $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^*$ is cyclic, we have the lemma. □

Lemma 17 *Let $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$. Suppose $\alpha\mathcal{O}_{\mathbf{K}} = ab\mathcal{O}_{\mathbf{K}}$ and $(\alpha|b\varepsilon) = 1$ for some $\varepsilon \in \mathcal{O}_{\mathbf{K}}^*$, then a is a square modulo $b\mathcal{O}_{\mathbf{K}}$ and b is a square modulo $a\mathcal{O}_{\mathbf{K}}$.*

Proof Since $\alpha\mathcal{O}_{\mathbf{K}} = ab\mathcal{O}_{\mathbf{K}}$, we have $ab\varepsilon_1 = \alpha$ for some $\varepsilon_1 \in \mathcal{O}_{\mathbf{K}}^*$. From Lemma 14, we have

$$1 = (\alpha|b\varepsilon) = (ab\varepsilon_1|b\varepsilon) = (-ab\varepsilon_1\cdot b\varepsilon|b\varepsilon) = (a\varepsilon_3|b\varepsilon)$$

where each $\varepsilon_i \in \mathcal{O}_{\mathbf{K}}^*$. Since we have $(a\varepsilon_3|b\varepsilon) = 1$, we have

$$b\varepsilon z^2 = x^2 - a\varepsilon_3 y^2 \text{ for some non-zero tuple } (x, y, z) \in \mathbf{K}^3. \tag{7}$$

Since the ideal $a\mathcal{O}_{\mathbf{K}}$ is square-free, $\sqrt{a\varepsilon_3} \notin \mathbf{K}$. Therefore z is non-zero. Further z is coprime to every prime ideal dividing $a\mathcal{O}_{\mathbf{K}}$. This is because if $\mathfrak{p} \mid \gcd(z\mathcal{O}_{\mathbf{K}}, a\mathcal{O}_{\mathbf{K}})$ then $\mathfrak{p}^2 \mid ay^2\mathcal{O}_{\mathbf{K}}$. Therefore an odd power of $\mathfrak{p}$ will divide $ay^2\mathcal{O}_{\mathbf{K}}$ ($a\mathcal{O}_{\mathbf{K}}$ is square free) and an even power of $\mathfrak{p}$ will divide the other two terms (since $\gcd(a\mathcal{O}_{\mathbf{K}}, b\mathcal{O}_{\mathbf{K}}) = \mathcal{O}_{\mathbf{K}}$). Similarly $\sqrt{b\varepsilon} \notin \mathbf{K}$ and y is coprime to every prime ideal dividing $b\mathcal{O}_{\mathbf{K}}$. Further, by Lemma 16

$$2 \mid [(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^* : \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{p}],\ \text{ for all } \mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}}$$

and in particular for all $\mathfrak{p} \mid a\mathcal{O}_{\mathbf{K}}$, we get that $\mathcal{O}_{\mathbf{K}}^*$ mod $\mathfrak{p}$ is in the subgroup of quadratic residues modulo $\mathfrak{p}$. Now reading (7) modulo $a\mathcal{O}_{\mathbf{K}}$, we get that b is a square modulo $a\mathcal{O}_{\mathbf{K}}$. The argument for a modulo $b\mathcal{O}_{\mathbf{K}}$ is similar. □

Theorem 18 *We have, for $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$ with $\mathbf{L} = \mathbf{L}_\alpha \in \mathcal{F}$,*

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})} \geq \frac{1}{2^{r_{\mathbf{K}}+2}}|\{&(a\mathcal{O}_{\mathbf{K}}, b\mathcal{O}_{\mathbf{K}}) : a\mathcal{O}_{\mathbf{K}}, b\mathcal{O}_{\mathbf{K}} \textit{ square free }, \alpha\mathcal{O}_{\mathbf{K}} = ab\mathcal{O}_{\mathbf{K}},\\ &a \textit{ is a square modulo } b\mathcal{O}_{\mathbf{K}} \textit{ and } b \textit{ is a square modulo } a\mathcal{O}_{\mathbf{K}}\}|. \end{aligned}$$

Proof

$$\begin{aligned} 2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})} &\geq \frac{1}{2^{r_{\mathbf{K}}+2}}|\{\mathfrak{b} \in \mathfrak{B}_{\mathbf{L}} : [\mathfrak{b}] \in \mathrm{Cl}_{\mathbf{L}}, [\mathfrak{b}] = [\mathfrak{a}^2]\\ &\qquad \text{for some non-zero fractional ideal } \mathfrak{a} \text{ of } \mathcal{O}_{\mathbf{L}}\}|\\ &= \frac{1}{2^{r_{\mathbf{K}}+2}}|\{\mathfrak{b} \in \mathfrak{B}_{\mathbf{L}} : \mathfrak{N}_{\mathbf{L}/\mathbf{K}}(\mathfrak{b}) = b\mathcal{O}_{\mathbf{K}}, (\alpha|b\varepsilon) = 1 \text{ for some } \varepsilon \in \mathcal{O}_{\mathbf{K}}^*\}| \end{aligned}$$

Since there is a unique ideal $\mathfrak{b} \in \mathfrak{B}_{\mathbf{L}}$ of norm $b\mathcal{O}_{\mathbf{K}}$ for every $b\mathcal{O}_{\mathbf{K}} \mid \alpha\mathcal{O}_{\mathbf{K}}$, we get

$$2^{rk_4(\mathrm{Cl}_{\mathbf{L}})} \geq \frac{1}{2^{r_{\mathbf{K}}+2}}|\{b\mathcal{O}_{\mathbf{K}} \mid \alpha\mathcal{O}_{\mathbf{K}} : (\alpha|b\varepsilon) = 1 \text{ for some } \varepsilon \in \mathcal{O}_{\mathbf{K}}^*\}|$$

$$\geq \frac{1}{2^{r_{\mathbf{K}}+2}}|\{(a\mathcal{O}_{\mathbf{K}}, b\mathcal{O}_{\mathbf{K}}) : \alpha\mathcal{O}_{\mathbf{K}} = ab\mathcal{O}_{\mathbf{K}}, (\alpha|b\varepsilon) = 1 \text{ for some } \varepsilon \in \mathcal{O}_{\mathbf{K}}^{*}\}|.$$

Now by Lemma 17, we have the theorem.

4 Algebraic preliminaries

Definition 19 Let $\mathfrak{p}$ be an any prime ideal in $\mathcal{O}_{\mathbf{K}}$, co-prime to $2\mathcal{O}_{\mathbf{K}}$, and let $a \in \mathcal{O}_{\mathbf{K}}$. We define the quadratic residue symbol as

$$\left(\frac{a}{\mathfrak{p}}\right) = \begin{cases} 0 & \textit{if } a \in \mathfrak{p}, \\ 1 & \textit{if } a \notin \mathfrak{p} \text{ and } a \textit{ is square } \mod \mathfrak{p}, \\ -1 & \textit{otherwise}. \end{cases}$$

Let $\mathfrak{p}$ be a prime ideal and I be an ideal in $\mathcal{O}_{\mathbf{K}}$ such that $\mathfrak{p}$ and I are co-prime. Since $\mathcal{O}_{\mathbf{K}}$ is a PID, we can express I as $I = i\mathcal{O}_{\mathbf{K}}$. For $\mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}}$, we define $\Phi_{\mathfrak{p}}(I)$ as:

$$\Phi_{\mathfrak{p}}(I) := \left(\frac{I}{\mathfrak{p}}\right) := \left(\frac{i}{\mathfrak{p}}\right)$$

Since $2|\left[(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{*} : \mathcal{O}_{\mathbf{K}}^{*} \pmod{\mathfrak{p}}\right]$, the mapping is well-defined. Firstly, we will define ray class group mod $\mathfrak{p}$ of $\mathbf{K}$ and then we will prove that $\Phi_{\mathfrak{p}}$ is a character on that group. We generically denote places by the symbol ν, but for non-archimedean places, we may use $\mathfrak{q}$ to denote both a prime of $\mathbf{K}$ and the place corresponding to the absolute value $|.|_{\mathfrak{q}}$. We write $\nu|\infty$ to indicate that ν is an archimedean place, which is real or complex and $M_{\mathbf{K}}$ to be the set of all inequivalent places of $\mathbf{K}$.

Definition 20 Let $g : M_{\mathbf{K}} \to \mathbb{Z}_{\geq 0}$ be a function with finite support such that for $\nu \in M_{\mathbf{K}}$ and $\nu|\infty$ we have $g(\nu) \leq 1$ with $g(\nu) = 0$ unless ν is a real place. Then any modulus $\mathfrak{b}$ in $\mathbf{K}$ can be viewed as a formal product

$$\mathfrak{b} = \mathfrak{b}_0\mathfrak{b}_\infty, \quad \textit{with } \mathfrak{b}_0 = \prod_{\mathfrak{q}\nmid\infty, \mathfrak{q}|\mathfrak{b}} \mathfrak{q}^{g(\mathfrak{q})} \quad \textit{and } \mathfrak{b}_\infty = \prod_{\nu|\infty} \nu^{g(\nu)}.$$

where $\mathfrak{b}_0$ corresponds to an $\mathcal{O}_{\mathbf{K}}$ -ideal and $\mathfrak{b}_\infty$ represents a subset of the real places of $\mathbf{K}$.

Now we define the following notation in $\mathcal{O}_{\mathbf{K}}$:

(1) $\mathcal{I}_{\mathbf{K}}$ be the set of all non-zero fractional ideals in $\mathcal{O}_{\mathbf{K}}$.
(2) $\mathcal{I}_{\mathbf{K}}^{\mathfrak{b}} \subseteq \mathcal{I}_{\mathbf{K}}$ is the subgroup of fractional ideals which is prime to $\mathfrak{b}$.
(3) $\mathbf{K}^{\mathfrak{b}} \subseteq \mathbf{K}^{*}$ is the subgroup of elements $\alpha \in \mathbf{K}^{*}$ for which $(\alpha) \in \mathcal{I}_{\mathbf{K}}^{\mathfrak{b}}$.
(4) $\mathbf{K}^{\mathfrak{b},1} \subseteq \mathbf{K}^{\mathfrak{b}}$ is the subgroup of elements $\alpha \in \mathbf{K}^{\mathfrak{b}}$ for which $\nu_{\mathfrak{q}}(\alpha - 1) \geq \nu_{\mathfrak{q}}(\mathfrak{b}_0)$ for all primes $\mathfrak{q}|\mathfrak{b}_0$ and $\alpha_\nu > 0$ for $\nu|\mathfrak{b}_\infty$ (here $\alpha_\nu \in \mathbb{R}$ is the image of α under the real-embedding ν).

(5) $\mathcal{P}_{\mathbf{K}}^{\mathfrak{b}} \subseteq \mathcal{I}_{\mathbf{K}}^{\mathfrak{b}}$ is the subgroup of principal fractional ideals $(\alpha) \in \mathcal{I}_{\mathbf{K}}^{\mathfrak{b}}$ with $\alpha \in \mathbf{K}^{\mathfrak{b},1}$.

Definition 21 The ray class group of $\mathbf{K}$ for the modulus $\mathfrak{b}$ is the quotient

$$H_{\mathfrak{b}}(\mathbf{K}) := \mathcal{I}_{\mathbf{K}}^{\mathfrak{b}}/\mathcal{P}_{\mathbf{K}}^{\mathfrak{b}}.$$

Recall that for $\mathfrak{p} \mid \alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$, $\Phi_{\mathfrak{p}}(I) = \left(\frac{i}{\mathfrak{p}}\right)$, if $I = i\mathcal{O}_{\mathbf{K}}$ with $\gcd(I, \mathfrak{p}) = \mathcal{O}_{\mathbf{K}}$. Since the power residue symbol is multiplicative, it immediately follows that $\Phi_{\mathfrak{p}}$ is also multiplicative. If $i\varepsilon \equiv 1 \bmod \mathfrak{p}$ for some $\varepsilon \in \mathcal{O}_{\mathbf{K}}^*$ then $\Phi_{\mathfrak{p}}(I) = 1$. Therefore, $\Phi_{\mathfrak{p}}$ is a character on $H_{\mathfrak{p}}(\mathbf{K})$. Such a character is called a generalized Dirichlet character (a special instance of a Hecke character). Let $\mathfrak{a}$ be a square-free ideal in $\mathcal{O}_{\mathbf{K}}$ such that $\mathfrak{a} \mid \alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$. Then we define the symbol $\left(\frac{\cdot}{\mathfrak{a}}\right)$ from $\mathcal{I}_{\mathbf{K}}^{\mathfrak{a}}$ to $\{\pm 1\}$ by

$$\left(\frac{\cdot}{\mathfrak{a}}\right) = \prod_{\mathfrak{q} \mid \mathfrak{a}} \left(\frac{\cdot}{\mathfrak{q}}\right).$$

This map is multiplicative since the power residue symbol is multiplicative. Let $I = i\mathcal{O}_{\mathbf{K}}$ be an ideal with $\gcd(I, \mathfrak{a}) = \mathcal{O}_{\mathbf{K}}$ and $i\varepsilon \equiv 1 \bmod \mathfrak{a}$ for some $\varepsilon \in \mathcal{O}_{\mathbf{K}}^*$. Then, we have

$$\left(\frac{i}{\mathfrak{a}}\right) = \prod_{\mathfrak{p} \mid \mathfrak{a}} \left(\frac{i}{\mathfrak{p}}\right) = 1.$$

This makes $\left(\frac{\cdot}{\mathfrak{a}}\right)$ a character on $H_{\mathfrak{a}}(\mathbf{K})$. We now recall a theorem of Bauer from Class field theory.

Theorem 22 (Bauer, Theorem 8.19 of [1]) *Given two finite degree Galois extensions $\mathbf{F}_1$ and $\mathbf{F}_2$ of a number field $\mathbf{K}$, if*

$$|\{\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}} : \mathfrak{p} \textit{ splits in } \mathbf{F}_1\} \setminus \{\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}} : \mathfrak{p} \textit{ splits in } \mathbf{F}_2\}| < \infty,$$

then $\mathbf{F}_2 \subset \mathbf{F}_1$.

We now introduce some notation. Let $s\mathcal{O}_{\mathbf{K}}$ be a squarefree ideal of $\mathcal{O}_{\mathbf{K}}$. If s satisfies (3), we set $\varepsilon_s = 1$. If s does not satisfy (3), we choose $\varepsilon \in \mathcal{O}_{\mathbf{K}}^*$ such the order of ε modulo each $\mathfrak{p}^2$ for $\mathfrak{p} \mid 2\mathcal{O}_{\mathbf{K}}$ is 2 (This is condition (3) on $\mathbf{K}$) . We now set $\varepsilon_s = \varepsilon$. We now consider the field $\mathbf{L}_{s\varepsilon_s}/\mathbf{K}$ ($\mathbf{L}_{s\varepsilon_s} := \mathbf{K}(\sqrt{s\varepsilon_s})$) and apply the above theorem of Bauer to prove the following lemma.

Lemma 23 *Consider the map*

$$\left(\frac{s\varepsilon_s}{\cdot}\right) : \mathcal{I}_{\mathbf{K}}^{s\mathcal{O}_{\mathbf{K}}} \to \{\pm 1\},$$

given by

$$\left(\frac{s\varepsilon_s}{\partial}\right) = \prod_{\mathfrak{p}^r \| \partial} \left(\frac{s\varepsilon_s}{\mathfrak{p}}\right)^r, \textit{ for all } (\partial, s\mathcal{O}_{\mathbf{K}}) = 1.$$

The map, $\left(\frac{s\varepsilon_s}{\cdot}\right)$*, defines a primitive character of* $H_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}(\mathbf{K})$.

Proof Clearly, $\left(\frac{s\varepsilon_s}{\cdot}\right)$ is multiplicative. The extension $\mathbf{L}_{s\varepsilon_s}/\mathbf{K}$ has degree 2 and relative discriminant $\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}} = 4s\mathcal{O}_{\mathbf{K}}$. We may think of $\left(\frac{s\varepsilon_s}{\cdot}\right)$ as a character on $\mathcal{I}_{\mathbf{K}}^{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}$ defined by

$$\left(\frac{s\varepsilon_s}{\partial}\right) = \prod_{\mathfrak{p}^r||\partial}\left(\frac{s\varepsilon_s}{\mathfrak{p}}\right)^r, \text{ for all } \gcd(\partial, \mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}) = 1.$$

By Lemma 1 and the Dedekind-Kummer theorem, we know that for any prime ideal $\mathfrak{q}$ satisfying the condition $\gcd(\mathfrak{q}, 4\,s\mathcal{O}_{\mathbf{K}}) = \mathcal{O}_{\mathbf{K}}$,

$$\begin{aligned}\left(\frac{s\varepsilon_s}{\mathfrak{q}}\right) = 1 \ &\text{ if and only if } \ X^2 - s\varepsilon_s \text{ splits modulo } \mathfrak{q}\\ &\text{ if and only if } \ (\mathfrak{q}, \mathbf{L}_{s\varepsilon_s}/\mathbf{K}) = 1.\end{aligned} \tag{8}$$

Here $(\mathfrak{q}, \mathbf{L}_{s\varepsilon_s}/\mathbf{K})$ denotes the Artin symbol of $\mathfrak{q}$ with respect to the relative extension $\mathbf{L}_{s\varepsilon_s}/\mathbf{K}$. Hence for an ideal ∂, $\gcd(\partial, 4\,s\mathcal{O}_{\mathbf{K}}) = \mathcal{O}_{\mathbf{K}}$,

$$\left(\frac{s\varepsilon_s}{\partial}\right) = 1 \text{ if and only if } \prod_{\mathfrak{q}^r||\partial}(\mathfrak{q}, \mathbf{L}_{s\varepsilon_s}/\mathbf{K})^r = 1. \tag{9}$$

By Conductor-discriminant formula, we have that the conductor of the extension $\mathbf{L}_{s\varepsilon_s}/\mathbf{K}$ satisfies $\mathfrak{f}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}} = \mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}$. This implies $\mathbf{L}_{s\varepsilon_s} \subseteq \mathbf{K}_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}$, where $\mathbf{K}_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}$ is a ray class field of modulus $\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}$ with respect to the number field $\mathbf{K}$.

By Class field theory, $H_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}(\mathbf{K}) \cong \mathrm{Gal}(\mathbf{K}_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}/\mathbf{K})$ via the map

$$[\mathfrak{a}] \rightarrow \prod_{\mathfrak{q}^r\|\mathfrak{a}}(\mathfrak{q}, \mathbf{K}_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}/\mathbf{K})^r.$$

Now suppose we have an ideal $\partial = b\mathcal{O}_{\mathbf{K}}$ with $b \equiv 1(\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}})$, then $[\partial]$ is trivial on the left. Therefore $\prod_{\mathfrak{q}^r||\partial}(\mathfrak{q}, \mathbf{K}_{\mathfrak{d}_{L_{s\varepsilon_s}/\mathbf{K}}}/\mathbf{K})^r = 1$. By properties of the Artin Symbol, we have

$$1 = \prod_{\mathfrak{q}^r||\partial}(\mathfrak{q}, \mathbf{K}_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}/\mathbf{K})^r\big|_{\mathbf{L}_{s\varepsilon_s}} = \prod_{\mathfrak{q}^r||\partial}(\mathfrak{q}, \mathbf{L}_{s\varepsilon_s}/\mathbf{K})^r.$$

By (9) this implies that $\left(\frac{s\varepsilon_s}{\cdot}\right)$ is a character on $H_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}(\mathbf{K})$.

We will now prove the claim about the primitivity of $\left(\frac{s\varepsilon_s}{\cdot}\right)$ as a character on $H_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}(\mathbf{K})$. Suppose that $\left(\frac{s\varepsilon_s}{\cdot}\right)$ is a character on $H_{\mathfrak{a}}(\mathbf{K})$ for some $\mathfrak{a} \mid \mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}$. We have $H_{\mathfrak{a}}(\mathbf{K}) \cong \mathrm{Gal}(\mathbf{K}_{\mathfrak{a}}/\mathbf{K})$ via the map

$$[\mathfrak{b}] \rightarrow \prod_{\mathfrak{q}^r\|\mathfrak{b}}(\mathfrak{q}, \mathbf{K}_{\mathfrak{a}}/\mathbf{K})^r.$$

Therefore, any prime $\mathfrak{q}$ of $\mathcal{O}_{\mathbf{K}}$ which splits in $\mathbf{K}_{\mathfrak{a}}/\mathbf{K}$ would also satisfy $[\mathfrak{q}] = 1$ in $H_{\mathfrak{a}}(\mathbf{K})$. Since $\left(\frac{s\varepsilon_s}{\cdot}\right)$ is a character on $H_{\mathfrak{a}}(\mathbf{K})$, we would then have $\left(\frac{s\varepsilon_s}{\mathfrak{q}}\right) = 1$. By (8), this means that if $\gcd(\mathfrak{q}, 4s\mathcal{O}_{\mathbf{K}}) = \mathcal{O}_{\mathbf{K}}$, $\mathfrak{q}$ will also split in $\mathbf{L}_{s\varepsilon_s}/\mathbf{K}$. Bauer's theorem (Theorem 22) would now imply that $\mathbf{L}_{s\varepsilon_s} \subset \mathbf{K}_{\mathfrak{a}}$, implying that $\mathfrak{a} = \mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}$. Therefore $\left(\frac{s\varepsilon_s}{\cdot}\right)$ is a primitive character of $H_{\mathfrak{d}_{\mathbf{L}_{s\varepsilon_s}/\mathbf{K}}}(\mathbf{K})$. □

4.1 Analogue of quadratic reciprocity

Lemma 24 *For an integral ideal* $\mathfrak{a}$ *of* $\mathcal{O}_{\mathbf{K}}$ *we have*

$$H_{\mathfrak{a}}(\mathbf{K}) \cong (\mathcal{O}_{\mathbf{K}}/\mathfrak{a})^* \,/\mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{a}.$$

Here $\mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{a} = \{u \bmod \mathfrak{a} : u \in \mathcal{O}_{\mathbf{K}}^*\}$. *We shall denote this isomorphism by* $\xi_{\mathfrak{a}}$.

Proof Since $\mathcal{O}_{\mathbf{K}}$ is a PID, we may define

$$\begin{aligned} \xi : \mathcal{I}_{\mathbf{K}}^{\mathfrak{a}} &\to (\mathcal{O}_{\mathbf{K}}/\mathfrak{a})^* \,/\mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{a} \\ \mathfrak{b} &\to \bar{b}, \qquad \text{where } \mathfrak{b} = b\mathcal{O}_{\mathbf{K}}. \end{aligned}$$

Surjectivity of ξ is obvious. We now consider injectivity. To do so, we note

$$\begin{aligned} \ker \xi &= \{\mathfrak{b} \in \mathcal{I}_{\mathbf{K}}^{\mathfrak{a}} : \bar{b}\varepsilon \equiv 1 \bmod \mathfrak{a} \textit{ for some } \varepsilon \in \mathcal{O}_{\mathbf{K}}^*\} \\ &= \{\mathfrak{b} \in \mathcal{I}_{\mathbf{K}}^{\mathfrak{a}} : \mathfrak{b} \textit{ has a generator which is } 1 \bmod \mathfrak{a}\}. \end{aligned}$$

Hence, $\mathcal{I}_{\mathbf{K}}^{\mathfrak{a}}/\mathcal{P}_{\mathbf{K}}^{\mathfrak{a}} \cong (\mathcal{O}_{\mathbf{K}}/\mathfrak{a})^* \,/\mathcal{O}_{\mathbf{K}}^*(\mathfrak{a})$. □

Class field theory tells us that

$$\mathcal{I}_{\mathbf{K}}^{\mathfrak{a}}/\mathcal{P}_{\mathbf{K}}^{\mathfrak{a}} \cong \mathrm{Gal}\,(\mathbf{K}_{\mathfrak{a}}/\mathbf{K})$$

via the Artin map, denoted $\Psi_{\mathfrak{a}}$. From Lemma 24, we now have the following corollary.

Corollary 25 *For an integral ideal* $\mathfrak{a}$ *of* $\mathcal{O}_{\mathbf{K}}$ *we have*

$$\mathrm{Gal}\,(\mathbf{K}_{\mathfrak{a}}/\mathbf{K}) \cong (\mathcal{O}_{\mathbf{K}}/\mathfrak{a})^* \,/\mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{a}$$

under the map $\xi_{\mathfrak{a}} \circ \Psi_{\mathfrak{a}}^{-1}$.

Let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals in $\mathcal{W}$. Since $\mathcal{O}_{\mathbf{K}}$ is a PID, we have $\mathfrak{p} = (p)$ and $\mathfrak{q} = (q)$ for elements $p, q \in \mathcal{O}_{\mathbf{K}}$. Without loss of generality, by the definition of $\mathcal{W}$, we may assume

$$q \equiv 1 \bmod 4\mathcal{O}_{\mathbf{K}}.$$

Now,

$$\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = \left(\frac{q}{\mathfrak{p}}\right) = 1 \text{ if and only if } x^2 - q \text{ splits modulo } \mathfrak{p}.$$

Let $\mathbf{L}'_{\mathfrak{q}} = \mathbf{K}(\sqrt{q})$, where $\dfrac{1+\sqrt{q}}{2} \in \mathcal{O}_{\mathbf{L}'_{\mathfrak{q}}}$. Then $\left\{1, \dfrac{1+\sqrt{q}}{2}\right\}$ is an basis of $\mathbf{L}'_{\mathfrak{q}}$ over $\mathbf{K}$. Therefore $\mathfrak{d}_{\mathbf{L}'_{\mathfrak{q}}/\mathbf{K}} \mid \mathfrak{q}$. However since $\mathfrak{q}$ is prime and it ramifies in $\mathbf{L}'_{\mathfrak{q}}$, we have $\mathfrak{d}_{\mathbf{L}'_{\mathfrak{q}}/\mathbf{K}} = \mathfrak{q}$. We claim that $\mathcal{O}_{\mathbf{L}'_{\mathfrak{q}}} = \mathcal{O}_{\mathbf{K}}\left[\dfrac{1+\sqrt{q}}{2}\right]$.

Lemma 26 *Let* $\mathbf{K}_1$ *be any quadratic extension of* $\mathbf{K}$*, and* $\mathcal{O}_{\mathbf{K}}$ *be PID, then* $\mathcal{O}_{\mathbf{K}_1} = \mathcal{O}_{\mathbf{K}}[\alpha]$ *for some* $\alpha \in \mathbf{K}_1$.

By Lemma 26, we have $\mathcal{O}_{\mathbf{L}'_{\mathfrak{q}}} = \mathcal{O}_{\mathbf{K}}[\theta]$ for some $\theta \in \mathcal{O}_{\mathbf{L}'_{\mathfrak{q}}}$. Since $\dfrac{1+\sqrt{q}}{2} \in \mathcal{O}_{\mathbf{L}'_{\mathfrak{q}}}$ and $\mathcal{O}_{\mathbf{L}'_{\mathfrak{q}}}$ is a free $\mathcal{O}_{\mathbf{K}}$ module with basis $\{1, \theta\}$, we have a matrix M with entries in $\mathcal{O}_{\mathbf{K}}$ such that

$$M\begin{pmatrix} 1 & 1 \\ \theta & \sigma(\theta) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{q}}{2} & \frac{1-\sqrt{q}}{2} \end{pmatrix}.$$

Since

$$\det(M)^2 \mathrm{disc}\{1, \theta\}\mathcal{O}_{\mathbf{K}} = \mathrm{disc}\left\{1, \frac{1+\sqrt{q}}{2}\right\}\mathcal{O}_{\mathbf{K}} = \mathfrak{q} = \mathfrak{d}_{\mathbf{L}'_{\mathfrak{q}}/\mathbf{K}}$$

we have that $\det(M)^2 \in \mathcal{O}_{\mathbf{K}}^*$. But $\det(M) \in \mathcal{O}_{\mathbf{K}}$ and therefore $\det(M) \in \mathcal{O}_{\mathbf{K}}^*$. This implies that M is invertible and therefore we have our claim. Now we have the following diagram:

$$\begin{tikzcd}
\mathbf{K}_{\mathfrak{q}} \arrow[d, dash, "G_1"'] \arrow[dd, dash, bend left=60, "G"] \\
\mathbf{L}'_{\mathfrak{q}} \arrow[d, dash, "2"] \\
\mathbf{K}
\end{tikzcd}$$

Observe that, $G \cong (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^*$ mod $\mathfrak{q}$ (under the map $\xi_{\mathfrak{q}} \circ \Psi_{\mathfrak{q}}^{-1}$) is cyclic. Hence

$$\begin{aligned}
\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = 1 \;\; &\text{if and only if } \; x^2 - q \text{ splits in modulo } \mathfrak{p}, \\
&\text{if and only if } \; (2x-1)^2 - q \text{ splits in modulo } \mathfrak{p} \text{ (}\mathfrak{p} \text{ does not lie above } 2\mathbb{Z}\text{)}, \\
&\text{if and only if } \; \mathfrak{p} \text{ splits in } \mathbf{L}'_{\mathfrak{q}} \text{ (by Dedekind-Kummer Theorem)}.
\end{aligned}$$

Now by the properties of the Artin Symbol, we have

$$\begin{aligned}
\mathfrak{p} \text{ splits in } \mathbf{L}'_{\mathfrak{q}} \;\; &\text{if and only if } \; (\mathfrak{p}, \mathbf{L}'_{\mathfrak{q}}/\mathbf{K}) = 1 \\
&\text{if and only if } \; (\mathfrak{p}, \mathbf{K}_{\mathfrak{q}}/\mathbf{K}) \in G_1
\end{aligned}$$

Let us now consider $\xi_{\mathfrak{q}} \circ \Psi_{\mathfrak{q}}^{-1}((\mathfrak{p}, \mathbf{K}_{\mathfrak{q}}/\mathbf{K}))$. By the definition of the Artin map $\Psi_{\mathfrak{q}}$, we have

$$\xi_{\mathfrak{q}} \circ \Psi_{\mathfrak{q}}^{-1}((\mathfrak{p}, \mathbf{K}_{\mathfrak{q}}/\mathbf{K})) = \xi_{\mathfrak{q}}([\mathfrak{p}]).$$

If the ideal $\mathfrak{p} = p\mathcal{O}_{\mathbf{K}}$, we have $\xi_{\mathfrak{q}}([\mathfrak{p}]) = \bar{p} \in (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}$.

$$\begin{aligned}\mathfrak{p} \text{ splits in } \mathbf{L}'_{\mathfrak{q}} \quad &\text{if and only if} \quad (\mathfrak{p}, \mathbf{K}_{\mathfrak{q}}/\mathbf{K}) \in G_1,\\ &\text{if and only if} \quad \bar{p} \text{ is in the unique subgroup of index 2 in } (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}.\end{aligned}$$

The last observation follows from Corollary 25. We have a natural surjective homomorphism given by

$$\begin{aligned}\pi : (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* &\to (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}\\ a \bmod \mathfrak{q} &\to \bar{a}.\end{aligned}$$

For $\mathfrak{p} \in \mathcal{W}$, by Lemma 16 we know that $\mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}$ is contained in the subgroup of quadratic residues in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^*$. Let us denote the subgroup of quadratic residues in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^*$ by $R_{\mathfrak{q}}$. Then we observe that $\pi(R_{\mathfrak{q}})$ has index 2 in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}$. This is because

$$\frac{(\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}}{R_{\mathfrak{q}}/\mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}} \cong (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / R_{\mathfrak{q}}.$$

Therefore, the unique subgroup of index 2 in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q}$ is $\pi(R_{\mathfrak{q}})$. We may now conclude that

$$\begin{aligned}\mathfrak{p} \text{ splits in } \mathbf{L}'_{\mathfrak{q}} \quad &\text{if and only if} \quad \bar{p} \text{ is in the unique subgroup of index 2 in } (\mathcal{O}_{\mathbf{K}}/\mathfrak{q})^* / \mathcal{O}_{\mathbf{K}}^* \bmod \mathfrak{q},\\ &\text{if and only if} \quad p \text{ is a quadratic residue modulo } \mathfrak{q},\\ &\text{if and only if} \quad x^2 - p \text{ splits in modulo } \mathfrak{q},\\ &\text{if and only if} \quad \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = 1.\end{aligned}$$

Therefore, for primes $\mathfrak{p}$ and $\mathfrak{q}$ in $\mathcal{W}$, we have $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)$.

By multiplicativity, we obtain the following lemma.

Lemma 27 *Let $\mathfrak{d}_{\bar{v}}$ and $\mathfrak{d}_{\bar{u}}$ be two ideals in $\mathcal{W}$. Then $\left(\frac{\mathfrak{d}_{\bar{v}}}{\mathfrak{d}_{\bar{u}}}\right) = \left(\frac{\mathfrak{d}_{\bar{u}}}{\mathfrak{d}_{\bar{v}}}\right)$.*

5 Analytic preliminaries

5.1 Divisor function and some variants

We begin with an upper bound on the number of squarefree integral ideals with norm atmost x and a prescribed number of prime divisors.

Lemma 28 *There exists a constant $B_0 = B_0(\mathbf{K})$ such that for every $X \geq 3$ and $\ell \geq 1$ we have*

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_{\mathbf{K}} : \mathfrak{N}(\mathfrak{a}) \leq X, \omega_{\mathbf{K}}(\mathfrak{a}) = \ell, \mu^2(\mathfrak{a}) = 1\} \ll_{\mathbf{K}} \frac{X}{\log X} \frac{(\log\log X + B_0)^{\ell-1}}{(\ell-1)!}.$$

Here $\mathfrak{N}$ denotes the norm map from $\mathbf{K}$ to $\mathbb{Q}$.

Proof We prove this by induction. For $\ell = 1$, the required inequality holds by prime ideal theorem. We now assume the result for ℓ and prove for $\ell + 1$. Let

$$M_\ell(X) = \{\mathfrak{a} \subseteq \mathcal{O}_{\mathbf{K}} : \mathfrak{N}(\mathfrak{a}) \le X, \omega_{\mathbf{K}}(\mathfrak{a}) = \ell, \mu^2(\mathfrak{a}) = 1\}.$$

Let us consider an element $\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{\ell+1} \in M_{\ell+1}(X)$ such that

$$\mathfrak{N}(\mathfrak{p}_1) < \mathfrak{N}(\mathfrak{p}_2) < \cdots < \mathfrak{N}(\mathfrak{p}_{\ell+1}).$$

Since $\mathfrak{N}(\mathfrak{a}_1) \le X$, $\mathfrak{N}(\mathfrak{p}_i) \le \sqrt{X}$ for all $1 \le i \le \ell$. In other words $\mathfrak{N}(\mathfrak{p}_i^2) \le X$ for all $1 \le i \le \ell$. We also have

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_{\ell+1} \in M_\ell(X/\mathfrak{N}(\mathfrak{p}_i)) \text{ for all } 1 \le i \le \ell.$$

This implies that

$$\ell M_{\ell+1}(X) \le \sum_{\mathfrak{N}(\mathfrak{p}^2) \le X} M_\ell(X/\mathfrak{N}(\mathfrak{p})).$$

Applying the induction hypothesis, we now have

$$\ell M_{\ell+1}(X) \ll \sum_{\mathfrak{N}(\mathfrak{p}^2) \le X} \frac{X}{\mathfrak{N}(\mathfrak{p})} \cdot \frac{1}{\log(X/\mathfrak{N}(\mathfrak{p}))} \frac{(\log\log X + B_1)^{\ell-1}}{(\ell-1)!}.$$

Therefore, we have

$$M_{\ell+1} \ll \frac{(\log\log X + B_1)^{\ell-1}}{\ell!} X \sum_{\mathfrak{N}(\mathfrak{p}^2) \le X} \frac{1}{\mathfrak{N}(\mathfrak{p}) \log(X/\mathfrak{N}(\mathfrak{p}))}.$$

Since $\mathfrak{N}(\mathfrak{p}) \le \sqrt{X}$, we have $X/\mathfrak{N}(\mathfrak{p}) \ge \sqrt{X}$, and hence by Theorem 1 of [5], we obtain

$$M_{\ell+1} \ll \frac{(\log\log X + B_1)^{\ell-1}}{\ell!} \frac{X}{\log X} \sum_{\mathfrak{N}(\mathfrak{p}^2) \le X} \frac{1}{\mathfrak{N}\mathfrak{p}} \ll \frac{X}{\log X} \frac{(\log\log X + B_0)^{\ell}}{\ell!}.$$

□

Next we would like to obtain an upper bound for the average value of $\gamma^{\omega_{\mathbf{K}}(\mathfrak{a})}$ for any positive real γ as $\mathfrak{N}(\mathfrak{a})$ varies in an interval. To this end, we recall here a theorem of Shiu which we will apply to bound certain sums in short intervals. Consider a class E of arithmetic functions f which are non-negative, multiplicative and satisfy the following two conditions:

(1) There exists a positive constant A such that

$$f(p^\ell) \le A_1^\ell, \ p \text{ prime and } \ell \ge 1.$$

(2) For every $\beta_1 > 0$ there exists a postiive constant $A_2 = A_2(\beta_1)$ such that

$$f(n) \le A_2 n^{\beta_1},\ n \ge 1.$$

We now state the theorem of Shiu [16].

Theorem 29 (Shiu) *Let $f \in E$, as $X \to \infty$,*

$$\sum_{X-Y \le n \le X} f(n) \ll \frac{Y}{\log X} \exp\left(\sum_{p \le X} \frac{f(p)}{p} \right)$$

uniformly in Y, provided that $2 \le X \exp(-\sqrt{\log X}) \le Y < X$.

We now make an observation which will be useful in the proof of the following lemma. By the Chebotarev density theorem, we have

$$\sum_{\substack{\mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) \le x, \\ (\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1}} 1 = \frac{x}{|H_{\mathfrak{f}}(\mathbf{K})| \log x} + \mathrm{O}_{\mathbf{K}}\left(\frac{x}{\log^2 x} \right).$$

Now by partial summation formula, we get

$$\begin{aligned} \sum_{\substack{\mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) \le x, \\ (\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1}} \frac{1}{\mathfrak{N}(\mathfrak{p})} &= \sum_{m \le x} \frac{\sum_{\mathfrak{N}(\mathfrak{p})=m, (\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1} 1}{m} \\ &= \mathrm{O}_{\mathbf{K}}\left(\frac{1}{\log x} \right) + \int_2^x \frac{\sum_{m \le t} \sum_{\mathfrak{N}(\mathfrak{p})=m, (\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1} 1}{t^2} dt \\ &= \int_2^x \frac{\sum_{\mathfrak{N}(\mathfrak{p}) \le t, (\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1} 1}{t^2} dt + \mathrm{O}_{\mathbf{K}}\left(\frac{1}{\log x} \right) \\ &= \int_2^x \frac{t}{|H_{\mathfrak{f}}(\mathbf{K})| t^2 \log t} dt + \mathrm{O}_{\mathbf{K}}\left(\int_2^x \frac{t}{t^2 \log^2 t} dt \right) + \mathrm{O}_{\mathbf{K}}\left(\frac{1}{\log x} \right) \end{aligned}$$

On computing the above integrals, we have

$$\sum_{\substack{\mathfrak{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{p}) \le x, \\ (\mathfrak{p}, \mathbf{K}_{\mathfrak{f}}/\mathbf{K})=1}} \frac{1}{\mathfrak{N}(\mathfrak{p})} = \frac{\log \log x}{|H_{\mathfrak{f}}(\mathbf{K})|} + \mathrm{O}_{\mathbf{K}}(1). \tag{10}$$

We now proceed to apply the theorem of Shiu.

Lemma 30 *Let $\gamma \in \mathbb{R}_{>0}$, then*

$$\sum_{\substack{X-Y\le \mathfrak{N}(\mathfrak{a})\le X\\ \mathfrak{a}\in\mathcal{W}}} \gamma^{\omega_{\mathbf{K}}(\mathfrak{a})} \ll_{\mathbf{K},\gamma} Y(\log X)^{\frac{\gamma}{|H_{\mathfrak{f}}(\mathbf{K})|}-1}$$

holds uniformly for $2 \le X\exp(-\sqrt{\log X}) \le Y < X$.

Proof Let $f(m) = \sum_{\mathfrak{N}(\mathfrak{a})=m,\mathfrak{a}\in\mathcal{W}} \gamma^{\omega_{\mathbf{K}}(\mathfrak{a})}$ with the convention that the empty sum is 0. We claim that f is multiplicative. This can be seen as follows. Consider

$$\sum_{\substack{\mathfrak{a}\neq(o),\\ \mathfrak{a}\subset\mathcal{O}_{\mathbf{K}}\\ \mathfrak{a}\in\mathcal{W}}} \frac{\gamma^{\omega_{\mathbf{K}}(\mathfrak{a})}}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}\left(1+\frac{\gamma}{\mathfrak{N}(\mathfrak{p})^s}\right) = \sum_{n=1}^{\infty}\frac{f(n)}{n^s}.$$

For any positive integer n which is a norm of an ideal in $\mathcal{W}$ we have that $f(n)$ is the coefficient of n^s in $\prod_{p|n}\prod_{\substack{\mathfrak{p}|p\mathcal{O}_{\mathbf{K}}\\ \mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}}\left(1+\frac{\gamma}{\mathfrak{N}(\mathfrak{p})^s}\right)$. Similarly if m is also the norm of an ideal in $\mathcal{W}$ and $(m,n)=1$ we have that $f(mn)$ is the coefficient of $(mn)^s$ in

$$\prod_{p|mn}\prod_{\substack{\mathfrak{p}|p\mathcal{O}_{\mathbf{K}}\\ \mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}}\left(1+\frac{\gamma}{\mathfrak{N}(\mathfrak{p})^s}\right) = \prod_{p|m}\prod_{\substack{\mathfrak{p}|p\mathcal{O}_{\mathbf{K}}\\ \mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}}\left(1+\frac{\gamma}{\mathfrak{N}(\mathfrak{p})^s}\right)\prod_{p|n}\prod_{\substack{\mathfrak{p}|p\mathcal{O}_{\mathbf{K}}\\ \mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}}\left(1+\frac{\gamma}{\mathfrak{N}(\mathfrak{p})^s}\right).$$

The last equality follows from the fact that $(m,n)=1$. This proves the claim. We have

$$f(m) = \sum_{\mathfrak{N}(\mathfrak{a})=m,\mathfrak{a}\in\mathcal{W}} \gamma^{\omega_{\mathbf{K}}(\mathfrak{a})} \le \sum_{\mathfrak{N}(\mathfrak{a})=m} \gamma^{n_{\mathbf{K}}\omega(m)} \le \gamma^{n_{\mathbf{K}}\omega(m)}\tau_{n_{\mathbf{K}}}(m).$$

For a prime power $m=p^{\ell}$, we have $f(m)\le\gamma^{n_{\mathbf{K}}}n_{\mathbf{K}}^{\ell}$. For all m and any $\beta_1>0$, we have

$$f(m)\le\gamma^{n_{\mathbf{K}}\omega(m)}\tau_{n_{\mathbf{K}}}(m) \ll 2^{n_{\mathbf{K}}\omega(m)\log_2\gamma}(\tau(m))^{n_{\mathbf{K}}} \ll_{\beta_1} m^{\beta_1}.$$

We now apply Shiu's theorem (Theorem 29), to get

$$\sum_{\substack{X-Y\le\mathfrak{N}\mathfrak{a}\le X\\ \mathfrak{a}\in\mathcal{W}}} \gamma^{\omega_{\mathbf{K}}(\mathfrak{a})} = \sum_{X-Y\le m\le X} f(m) \ll \frac{Y}{\log X}\exp\left(\sum_{p\le X}\frac{f(p)}{p}\right).$$

Note that

$$\sum_{p\le X}\frac{f(p)}{p} = \sum_{p\le X}\frac{\sum_{\mathfrak{N}(\mathfrak{a})=p,\mathfrak{a}\in\mathcal{W}}\gamma^{\omega_{\mathbf{K}}(\mathfrak{a})}}{p} = \sum_{\substack{\mathfrak{N}(\mathfrak{p})\le X,\\ \mathfrak{N}(\mathfrak{p})\text{ is prime}\\ \mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}}\frac{\gamma}{\mathfrak{N}(\mathfrak{p})} \le \sum_{\substack{\mathfrak{N}(\mathfrak{p})\le X\\ \mathfrak{p}\in\mathcal{P}_{\mathbf{K}}}}\frac{\gamma}{\mathfrak{N}(\mathfrak{p})}$$

$$= \frac{\gamma \log\log X}{|H_{\mathfrak{f}(\mathbf{K})}|} + \mathrm{O}_{\mathbf{K}}(\gamma)$$

where the last step follows from (10). This gives us the required lemma. □

We conclude this subsection with the average order of the function which counts the number of ordered factorisations of an integral ideal of $\mathbf{K}$ into exactly g integral ideals. Let $g \geq 1$ be an integer. For any ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbf{K}}$, $\tau_{\mathbf{K},g}(\mathfrak{a})$ denotes the number of ways the ideal $\mathfrak{a}$ can be written as an ordered product of g ideals. For a number field $\mathbf{K}$, we have the following lemma.

Lemma 31 *For any positive integer $g \geq 1$, we have*

$$\sum_{\mathfrak{N}(\mathfrak{a}) \leq x} \tau_{\mathbf{K},g}(\mathfrak{a}) = \alpha_{\mathbf{K}}^{g} \frac{x(\log x)^{g-1}}{(g-1)!} + O_{\mathbf{K}}(x(\log x)^{g-2}).$$

Proof We use the induction hypothesis to prove the claim. It is well-known that (see; [12])

$$\sum_{\mathfrak{N}(\mathfrak{c}) \leq x} 1 = \alpha_{\mathbf{K}} x + O(x^{1-\frac{1}{n_{\mathbf{K}}}}), \tag{11}$$

where $n_{\mathbf{K}}$ is the degree of $\mathbf{K}/\mathbb{Q}$. By using (11), we obtain

$$\begin{aligned}
\sum_{\mathfrak{N}(\mathfrak{a}) \leq x} \tau_{\mathbf{K},2}(\mathfrak{a}) &= \sum_{\mathfrak{N}(\mathfrak{a}) \leq x} \sum_{\mathfrak{c} | \mathfrak{a}} 1 = \sum_{\mathfrak{N}(\mathfrak{c}) \leq x} \sum_{\mathfrak{N}(b) \leq \frac{x}{\mathfrak{N}(\mathfrak{c})}} 1 \\
&= \sum_{\mathfrak{N}(\mathfrak{c}) \leq x} \left(\alpha_{\mathbf{K}} \frac{x}{\mathfrak{N}(\mathfrak{c})} + O_{\mathbf{K}}\left(\left(\frac{x}{\mathfrak{N}(\mathfrak{c})} \right)^{1-\frac{1}{n_{\mathbf{K}}}} \right) \right) \\
&= \alpha_{\mathbf{K}} x \sum_{\mathfrak{N}(\mathfrak{c}) \leq x} \frac{1}{\mathfrak{N}(\mathfrak{c})} + O_{\mathbf{K}}\left(x^{1-\frac{1}{n_{\mathbf{K}}}} \sum_{\mathfrak{N}(\mathfrak{c}) \leq x} \frac{1}{\mathfrak{N}(\mathfrak{c})^{1-\frac{1}{n_{\mathbf{K}}}}} \right).
\end{aligned}$$

Also, using (11) and partial summation formula it is easy to see that

$$\sum_{1 \leq \mathfrak{N}(\mathfrak{c}) \leq x} \frac{1}{\mathfrak{N}(\mathfrak{c})} = \alpha_{\mathbf{K}} \log x + \mathrm{O}_{\mathbf{K}}(1) \ \text{ and } \sum_{1 \leq \mathfrak{N}(\mathfrak{c}) \leq x} \frac{1}{\mathfrak{N}(\mathfrak{c})^{1-\frac{1}{n_{\mathbf{K}}}}} \ll_{\mathbf{K}} x^{\frac{1}{n_{\mathbf{K}}}}.$$

Thus, we have

$$\sum_{\mathfrak{N}(\mathfrak{a}) \leq x} \tau_{\mathbf{K},2}(\mathfrak{a}) = \alpha_{\mathbf{K}}^{2} x \log x + O_{\mathbf{K}}(x).$$

Now, we assume that the claim is true for $\tau_{\mathbf{K},g-1}$. Therefore, we have

$$\sum_{\mathfrak{N}(\mathfrak{c}) \leq x} \tau_{\mathbf{K},g-1}(\mathfrak{c}) = \alpha_{\mathbf{K}}^{g-1} \frac{x(\log x)^{g-2}}{(g-2)!} + O_{\mathbf{K}}(x(\log x)^{g-3}).$$

Since $\tau_{\mathbf{K},g}(\mathfrak{a}) = \sum_{\mathfrak{c}|\mathfrak{a}} \tau_{\mathbf{K},g-1}(\mathfrak{c})$, we obtain

$$\sum_{\mathfrak{N}(\mathfrak{a})\leq x} \tau_{\mathbf{K},g}(\mathfrak{a}) = \alpha_{\mathbf{K}}^{g} \frac{x(\log x)^{g-1}}{(g-1)!} + O_{\mathbf{K}}(x(\log x)^{g-2}).$$

□

5.2 Important analytic prerequisites

The aim of this subsection is to introduce a few character sum estimates which will be used in the due course of the article. We begin by recalling the Large Sieve inequality for number fields due to Wilson ([21]).

Lemma 32 ([21], Wilson) *Let* $\mathbf{K}$ *be a number field and* $\mathcal{O}_{\mathbf{K}}$ *its ring of integers. Let* $\{t_{\mathfrak{a}}\}_{\mathfrak{a}\subseteq\mathcal{O}_{\mathbf{K}}}$ *be a sequence of complex numbers. Let* χ *be a character of* $H_{\mathfrak{q}}(\mathbf{K})$. *Define* $S_M(\chi) = \sum_{\mathfrak{N}(\mathfrak{a})\leq M} t_{\mathfrak{a}}\chi(\mathfrak{a})$. *Then*

$$\sum_{\mathfrak{N}(\mathfrak{q})\leq Q} \frac{\mathfrak{N}(\mathfrak{q})}{\phi(\mathfrak{q})} \sum_{\chi \bmod \mathfrak{q}}^{*} |S_M(\chi)|^2 \leq (Q^2 + M) \sum_{\mathfrak{N}(\mathfrak{a})\leq M} |t_{\mathfrak{a}}|^2,$$

where the summation $\sum^{*}$ *is over primitive characters and* ϕ *is the Euler-Totient function defined on the integral ideals of* $\mathbf{K}$ *in the following manner* $\phi(\mathfrak{q}) = \mathfrak{N}(\mathfrak{q})\prod_{\mathfrak{p}|\mathfrak{q}}\left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)$.

The following lemma is a generalisation of the Siegel-Walfisz theorem due to L. J. Goldstein [6].

Lemma 33 [6] *Let* $\mathbf{K}$ *be a normal algebraic number field of finite degree* $n_{\mathbf{K}}$ *and discriminant* $d_{\mathbf{K}}$. *Let* χ *be a nontrivial generalised Dirichlet character on* $H_{\mathfrak{f}}(\mathbf{K})$. *Let* $\epsilon > 0$, *there exists a positive constant* $c = c(\epsilon)$ *not depending on* $\mathbf{K}$ *or* χ, *such that*

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p})\leq x\\ (\mathfrak{p},\mathfrak{f})=\mathcal{O}_{\mathbf{K}}}} \chi(\mathfrak{p}) \ll Dx(\log^2 x)\exp(-cn_{\mathbf{K}}(\log x)^{1/2}/D),$$

where $D = n_{\mathbf{K}}^{3}(|d_{\mathbf{K}}|\mathfrak{N}(\mathfrak{f}))^{\epsilon}c^{-n_{\mathbf{K}}}$.

We conclude this section with a generalisation of a lemma of Heilbronn on Generalised Dirichlet characters of Ray class groups. A key ingredient in the proof is following character sum estimate of Heilbronn.

Lemma 34 (Heilbronn, Lemma 2 of [9]) *Let* $\mathbf{K}$ *be an algebraic number field of discriminant* $d_{\mathbf{K}}$ *and degree* $n_{\mathbf{K}}$. *Let* χ *be a non-principal Hecke character defined on*

$H_{\mathfrak{b}}(\mathbf{K})$, for an ideal $\mathfrak{b}$ with $\mathfrak{N}(\mathfrak{b}) = b$. Then for any real $x > 1$ and $\epsilon > 0$, we have

$$\sum_{\mathfrak{N}(\mathfrak{a}) \le x} \chi(\mathfrak{a}) = \mathrm{O}(x^{n_{\mathbf{K}}} |d_{\mathbf{K}}|b)^{\frac{1}{n_{\mathbf{K}}+2}+\epsilon},$$

where the constant implied by the symbol O depends on $n_{\mathbf{K}}$ and ϵ.

We now prove our generalisation of Heilbronn's result from [9].

Lemma 35 *For $i \in \{1, \dots, N\}$ and integral ideals $\mathfrak{c}$ with $\mathfrak{N}(\mathfrak{c}) \le x$, let $a_i, b_{\mathfrak{c}}$ be complex numbers satisfying $|a_i|, |b_{\mathfrak{c}}| \le 1$. Further let g be any positive integer. We also assume that we have N distinct Hecke characters $\{\chi_j\}_{j=1}^{N}$ modulo ideals of norm $\{\tilde{b}_j\}_{j=1}^{N}$, respectively. Then, we have*

$$\sum_{i=1}^{N} \sum_{\mathfrak{N}(\mathfrak{c}) \le x} a_i b_{\mathfrak{c}} \chi_i(\mathfrak{c}) \ll_g N^{1-\frac{1}{4g}} x \log x + N^{1-\frac{1}{2g}} x^{1-\frac{1}{2(n_{\mathbf{K}}+1)}} (\log x) \Bigg(\sum_{i_1=1}^{N} \sum_{\substack{i_2=1 \\ i_1 \ne i_2}}^{N} (\tilde{b}_{i_1} \tilde{b}_{i_2})^{\frac{2}{n_{\mathbf{K}}+1}} \Bigg)^{\frac{1}{4g}}.$$

Proof By Hölder's inequality, we have

$$\begin{aligned}
\left| \sum_{i=1}^{N} \sum_{\mathfrak{N}(\mathfrak{c}) \le x} a_i b_{\mathfrak{c}} \chi_i(\mathfrak{c}) \right| &\le N^{1-\frac{1}{2g}} \left(\sum_{i=1}^{N} \left| \sum_{\mathfrak{N}(\mathfrak{c}) \le x} b_{\mathfrak{c}} \chi_i(\mathfrak{c}) \right|^{2g} \right)^{\frac{1}{2g}} \\
&\le N^{1-\frac{1}{2g}} \left(\sum_{i=1}^{N} \left(\sum_{\mathfrak{N}(\mathfrak{c}_1), \mathfrak{N}(\mathfrak{c}_2) \le x} b_{\mathfrak{c}_1} \overline{b}_{\mathfrak{c}_2} \chi_i(\mathfrak{c}_1) \overline{\chi}_i(\mathfrak{c}_2) \right)^{g} \right)^{\frac{1}{2g}} \\
&\le N^{1-\frac{1}{2g}} \left(\sum_{\mathfrak{N}(\mathfrak{e}_1) \le x^g} f(\mathfrak{e}_1) \sum_{\mathfrak{N}(\mathfrak{e}_2) \le x^g} \overline{f}(\mathfrak{e}_2) \sum_{i=1}^{N} \chi_i(\mathfrak{e}_1) \bar{\chi}_i(\mathfrak{e}_2) \right)^{\frac{1}{2g}},
\end{aligned}$$

where

$$f(\mathfrak{e}_j) = \sum_{\substack{\mathfrak{e}_j = \mathfrak{c}_{j,1} \cdots \mathfrak{c}_{j,g} \\ \mathfrak{N}(\mathfrak{c}_{j,k}) \le x}} b_{c_{j,1}} \cdots b_{c_{j,g}} \text{ for } j \in \{1, 2\}.$$

We observe that $|f(\mathfrak{e}_j)| \le \tau_{\mathbf{K},g}(\mathfrak{e}_j)$. By multiplicativity of $\tau_{\mathbf{K},g}$, we have $\tau_{\mathbf{K},g}(\mathfrak{e}_j) = \prod_{\mathfrak{p}^s || \mathfrak{e}_j} \tau_{\mathbf{K},g}(\mathfrak{p}^s)$. We note that $\tau_{\mathbf{K},g}(\mathfrak{p}^s)^2 \le (s+1)^{2g} \ll_g \frac{(s+2g)!}{(2g)!s!}$. Since $\tau_{\mathbf{K},2g+1}(\mathfrak{p}^s) = \frac{(s+2g)!}{(2g)!s!}$, we have $\tau_{\mathbf{K},g}(\mathfrak{e}_j)^2 \ll_g \tau_{\mathbf{K},2g+1}(\mathfrak{e}_j)$. Therefore, it follows from Lemma 31 that

$$\sum_{\substack{\mathfrak{e} \subseteq \mathcal{O}_{\mathbf{K}} \\ \mathfrak{N}(\mathfrak{e}) \le x^g}} |f(\mathfrak{e})|^2 \ll_{\mathbf{K},g} x^g (\log x)^{2g}.$$

By applying the Cauchy-Schwarz inequality twice, we get

$$\left| \sum_{i=1}^{N} \sum_{\mathfrak{N}(\mathfrak{c}) \le x} a_i b_{\mathfrak{c}} \chi_i(\mathfrak{c}) \right| \le N^{1-\frac{1}{2g}} \left(\sum_{\mathfrak{N}(\mathfrak{e}_1) \le x^g} |f(\mathfrak{e}_1)|^2 \sum_{\mathfrak{N}(\mathfrak{e}_2) \le x^g} |f(\mathfrak{e}_2)|^2 \right)^{\frac{1}{4g}}$$

$$\times\left(\sum_{\substack{\mathfrak{N}(\mathfrak{e}_1)\le x^g\\ \mathfrak{N}(\mathfrak{e}_2)\le x^g}}\left|\sum_{i=1}^{N}\chi_i(\mathfrak{e}_1)\bar{\chi}_i(\mathfrak{e}_2)\right|^2\right)^{\frac{1}{4g}}$$

$$\ll N^{1-\frac{1}{2g}}(x^{2g}(\log x)^{4g})^{\frac{1}{4g}}$$

$$\left(\sum_{i_1}\sum_{i_2}\sum_{\mathfrak{e}_1}\sum_{\mathfrak{e}_2}\chi_{i_1}(\mathfrak{e}_1)\bar{\chi}_{i_1}(\mathfrak{e}_2)\chi_{i_2}(\mathfrak{e}_2)\bar{\chi}_{i_2}(\mathfrak{e}_1)\right)^{\frac{1}{4g}} \tag{12}$$

If we split the inner sums in (12) into two, one over the diagonal terms (that is $i_1 = i_2$) and otherwise, we get

$$\left|\sum_{i=1}^{N}\sum_{\mathfrak{N}(\mathfrak{c})\le x}a_i b_{\mathfrak{c}}\chi_i(\mathfrak{c})\right| \ll N^{1-\frac{1}{2g}}(x^{2g}(\log x)^{4g})^{\frac{1}{4g}}\left(\sum_{i_1}\sum_{i_2}\left|\sum_{\mathfrak{N}(\mathfrak{a})\le x^g}\chi_{i_1}\bar{\chi}_{i_2}(\mathfrak{a})\right|^2\right)^{\frac{1}{4g}}$$

$$\ll N^{1-\frac{1}{2g}}(x^{2g}(\log x)^{4g})^{\frac{1}{4g}}$$

$$\left(Nx^{2g}+\sum_{i_1}\sum_{\substack{i_2\\ i_1\neq i_2}}\left|\sum_{\mathfrak{N}(\mathfrak{a})\le x^g}\chi_{i_1}\bar{\chi}_{i_2}(\mathfrak{a})\right|^2\right)^{\frac{1}{4g}}$$

Using Lemma 34, we have

$$\left|\sum_{i=1}^{N}\sum_{\mathfrak{N}(\mathfrak{c})\le x}a_i b_{\mathfrak{c}}\chi_i(\mathfrak{c})\right| \ll N^{1-\frac{1}{4g}}x\log x + N^{1-\frac{1}{2g}}x^{\frac{1}{2}}\log x$$

$$\left(\sum_{i_1}\sum_{\substack{i_2\\ i_1\neq i_2}}\left|\sum_{\mathfrak{N}(\mathfrak{a})\le x^g}\chi_{i_1}\bar{\chi}_{i_2}(\mathfrak{a})\right|^2\right)^{\frac{1}{4g}}$$

$$\ll_g N^{1-\frac{1}{4g}}x\log x + N^{1-\frac{1}{2g}}x^{\frac{1}{2}}\log x$$

$$\left(\sum_{i_1}\sum_{\substack{i_2\\ i_1\neq i_2}}(x^{gn_{\mathbf{K}}}|d_{\mathbf{K}}|\tilde{b}_{i_1}\tilde{b}_{i_2})^{\frac{2}{n_{\mathbf{K}}+2}+\beta}\right)^{\frac{1}{4g}}$$

$$\ll_g N^{1-\frac{1}{4g}}x\log x + N^{1-\frac{1}{2g}}x^{1-\frac{1}{2(n_{\mathbf{K}}+1)}}(\log x)$$

$$\left(\sum_{i_1}\sum_{\substack{i_2\\ i_1\neq i_2}}(\tilde{b}_{i_1}\tilde{b}_{i_2})^{\frac{2}{n_{\mathbf{K}}+1}}\right)^{\frac{1}{4g}}.$$

□

6 Computing the average value of $2^{m\cdot \mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})}$ for $\mathbf{L} \in \mathcal{F}$

Let $a \in \mathcal{O}_{\mathbf{K}}$. For any ideal $\delta\mathcal{O}_{\mathbf{K}}$ satisfying $(\delta\mathcal{O}_{\mathbf{K}}, a\mathcal{O}_{\mathbf{K}}) = \mathcal{O}_{\mathbf{K}}$, we set

$$\chi_{a\mathcal{O}_{\mathbf{K}}}(\delta) = \frac{1}{2^{\omega_{\mathbf{K}}(a\mathcal{O}_{\mathbf{K}})}}\left(\prod_{\mathfrak{p}|a\mathcal{O}_{\mathbf{K}}}\left(\left(\frac{\delta}{\mathfrak{p}}\right)+1\right)\right).$$

Therefore, by Theorem 18, for $\alpha\mathcal{O}_{\mathbf{K}} \in \mathcal{W}$ and $\mathbf{L} = \mathbf{L}_\alpha \in \mathcal{F}$, we have

$$2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{L}})} \geq \frac{1}{2^{r_{\mathbf{K}}+2}} \sum_{\substack{(a\mathcal{O}_{\mathbf{K}}, b\mathcal{O}_{\mathbf{K}})\\ \alpha\mathcal{O}_{\mathbf{K}} = ab\mathcal{O}_{\mathbf{K}}}} \chi_{a\mathcal{O}_{\mathbf{K}}}(b)\chi_{b\mathcal{O}_{\mathbf{K}}}(a).$$

We shall use $T(\alpha\mathcal{O}_{\mathbf{K}})$ to denote the sum $\sum_{\substack{(a\mathcal{O}_{\mathbf{K}}, b\mathcal{O}_{\mathbf{K}})\\ \alpha\mathcal{O}_{\mathbf{K}} = ab\mathcal{O}_{\mathbf{K}}}} \chi_{a\mathcal{O}_{\mathbf{K}}}(b)\chi_{b\mathcal{O}_{\mathbf{K}}}(a)$. Then

$$\begin{aligned} T(\alpha\mathcal{O}_{\mathbf{K}}) &= \sum_{ab\mathcal{O}_{\mathbf{K}} = \alpha\mathcal{O}_{\mathbf{K}}} \frac{1}{2^{\omega_{\mathbf{K}}(\alpha\mathcal{O}_{\mathbf{K}})}} \prod_{\mathfrak{p}|a\mathcal{O}_{\mathbf{K}}}\left(1+\left(\frac{b}{\mathfrak{p}}\right)\right)\prod_{\mathfrak{p}|b\mathcal{O}_{\mathbf{K}}}\left(1+\left(\frac{a}{\mathfrak{p}}\right)\right)\\ &= \frac{1}{2^{\omega_{\mathbf{K}}(\alpha\mathcal{O}_{\mathbf{K}})}} \sum_{ab\mathcal{O}_{\mathbf{K}} = \alpha\mathcal{O}_{\mathbf{K}}} \sum_{c\mathcal{O}_{\mathbf{K}}|a\mathcal{O}_{\mathbf{K}}} \left(\frac{b\mathcal{O}_{\mathbf{K}}}{c\mathcal{O}_{\mathbf{K}}}\right) \sum_{d\mathcal{O}_{\mathbf{K}}|b\mathcal{O}_{\mathbf{K}}} \left(\frac{a\mathcal{O}_{\mathbf{K}}}{d\mathcal{O}_{\mathbf{K}}}\right). \end{aligned}$$

Suppose $a\mathcal{O}_{\mathbf{K}} = \partial_0\partial_1$ and $b\mathcal{O}_{\mathbf{K}} = \partial_2\partial_3$, also let $\partial_0 = c\mathcal{O}_{\mathbf{K}}$ and $\partial_3 = d\mathcal{O}_{\mathbf{K}}$, then we have

$$T(\alpha\mathcal{O}_{\mathbf{K}}) = \frac{1}{2^{\omega_{\mathbf{K}}(\alpha\mathcal{O}_{\mathbf{K}})}} \sum_{\partial_0\partial_1\partial_2\partial_3 = \alpha\mathcal{O}_{\mathbf{K}}} \left(\frac{\partial_2}{\partial_0}\right)\left(\frac{\partial_3}{\partial_0}\right)\left(\frac{\partial_0}{\partial_3}\right)\left(\frac{\partial_1}{\partial_3}\right).$$

Define $\Phi_1 : \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$, by $\Phi_1(\bar{u}, \bar{v}) = (u_1 + v_1)(u_1 + v_2)$, where $\bar{u} = (u_1, u_2)$ and $\bar{v} = (v_1, v_2)$. Note that $\Phi_1(\bar{u}, \bar{v}) = 1$ if and only if

$$(\bar{u}, \bar{v}) \in \{((1,0),(0,0)), ((0,1),(1,1)), ((1,1),(0,0)), ((0,0),(1,1))\}.$$

If we write $\partial_0 = \partial_{00}$, $\partial_1 = \partial_{01}$, $\partial_2 = \partial_{10}$ and $\partial_3 = \partial_{11}$. Then it follows that

$$T(\alpha\mathcal{O}_{\mathbf{K}}) = \frac{1}{2^{\omega_{\mathbf{K}}(\alpha\mathcal{O}_{\mathbf{K}})}} \sum_{\alpha\mathcal{O}_{\mathbf{K}} = \partial_{00}\partial_{01}\partial_{10}\partial_{11}} \prod_{\bar{u},\bar{v}\in\mathbb{F}_2^2} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_1(\bar{u},\bar{v})}$$

We interpret the elements $0, 1 \in \mathbb{F}_2$ as $0, 1 \in \mathbb{N}$ with the convention that $0^0 = 1$. Now we consider the m-th moment of $2^{\mathrm{rk}_4(\mathrm{Cl}_{\mathbf{K}})}$, where $m \in \mathbb{N}$

$$T_m(\alpha\mathcal{O}_{\mathbf{K}}) := \frac{1}{2^{m\omega_{\mathbf{K}}(\alpha\mathcal{O}_{\mathbf{K}})}}$$

$$\times \sum_{\substack{\alpha\mathcal{O}_{\mathbf{K}}=\prod_{\bar{u}(1)} \partial^{(1)}_{\bar{u}(1)} \\ \vdots \\ \alpha\mathcal{O}_{\mathbf{K}}=\prod_{\bar{u}(m)} \partial^{(m)}_{\bar{u}(m)}}} \prod_{\bar{u}(1),\bar{v}(1)\in\mathbb{F}_2^2} \left(\frac{\partial^{(1)}_{\bar{u}(1)}}{\partial^{(1)}_{\bar{v}(1)}}\right)^{\Phi_1(\bar{u}(1),\bar{v}(1))} \cdots \prod_{\bar{u}(m),\bar{v}(m)\in\mathbb{F}_2^2} \left(\frac{\partial^{(m)}_{\bar{u}(m)}}{\partial^{(m)}_{\bar{v}(m)}}\right)^{\Phi_1(\bar{u}(m),\bar{v}(m))} \tag{13}$$

Suppose that $\alpha\mathcal{O}_{\mathbf{K}} = \prod_{\bar{u}(1)\in\mathbb{F}_2^2} \partial^{(1)}_{\bar{u}(1)} = \cdots = \prod_{\bar{u}(m)\in\mathbb{F}_2^2} \partial^{(m)}_{\bar{u}(m)}$ and we define

$$\partial_{\bar{u}(1),\ldots,\bar{u}(m)} = \gcd\left(\partial^{(1)}_{\bar{u}(1)}, \ldots, \partial^{(m)}_{\bar{u}(m)}\right)$$

and

$$m_{\bar{u}(\ell)} = \prod_{\bar{u}(1)\in\mathbb{F}_2^2} \cdots \prod_{\bar{u}(\ell-1)\in\mathbb{F}_2^2} \prod_{\bar{u}(\ell+1)\in\mathbb{F}_2^2} \cdots \prod_{\bar{u}(m)\in\mathbb{F}_2^2} \partial_{\bar{u}(1),\ldots,\bar{u}(m)}.$$

We claim that $m_{\bar{u}(\ell)} = \partial^{(\ell)}_{\bar{u}(\ell)}$. Recall that $\alpha\mathcal{O}_{\mathbf{K}} = \prod_{\bar{u}(\ell)\in\mathbb{F}_2^2} \partial^{(\ell)}_{\bar{u}(\ell)}$. Therefore, $\partial^{(\ell)}_{\bar{u}(\ell)}$ is square-free. If $\mathfrak{p}|\partial^{(\ell)}_{\bar{u}(\ell)}$, then it divides $\alpha\mathcal{O}_{\mathbf{K}}$ and this implies that $\mathfrak{p}|\partial^{(i)}_{\bar{u}(i)}$, for some $\bar{u}(i) \in \mathbb{F}_2^2$, for all i. Hence, $\mathfrak{p}|\partial_{\bar{u}(1),\ldots,\bar{u}(\ell),\ldots,\bar{u}(m)}$, for such $\bar{u}(i)$, where $i \neq \ell$ which implies $\mathfrak{p}|m_{\bar{u}(\ell)}$, thus $\partial^{(\ell)}_{\bar{u}(\ell)}|m_{\bar{u}(\ell)}$. Conversely, if $\mathfrak{p}|m_{\bar{u}(\ell)}$, then

$$\mathfrak{p}|\gcd\left(\partial^{(1)}_{\bar{u}(1)}, \ldots, \partial^{(\ell)}_{\bar{u}(\ell)}, \ldots, \partial^{(m)}_{\bar{u}(m)}\right) \text{ for some indices } \bar{u}(i) \in \mathbb{F}_2^2\ \forall\, i \neq \ell \Rightarrow \mathfrak{p}|\partial^{(\ell)}_{\bar{u}(\ell)}.$$

Moreover, $m_{\bar{u}(\ell)}$ is square-free. This proves our claim. Therefore we can write $\alpha\mathcal{O}_{\mathbf{K}}$ as

$$\alpha\mathcal{O}_{\mathbf{K}} = \prod_{\bar{u}(\ell)\in\mathbb{F}_2^2} \partial^{(\ell)}_{\bar{u}(\ell)} = \prod_{\bar{u}(1)\in\mathbb{F}_2^2} \cdots \prod_{\bar{u}(\ell)\in\mathbb{F}_2^2} \cdots \prod_{\bar{u}(m)\in\mathbb{F}_2^2} \partial_{\bar{u}(1),\ldots,\bar{u}(m)}.$$

Therefore, by replacing $\partial^{(\ell)}_{\bar{u}(\ell)}$ by $m_{\bar{u}(\ell)}$ in (13), we get

$$T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \frac{1}{2^{m\omega_{\mathbf{K}}(\alpha\mathcal{O}_{\mathbf{K}})}} \sum_{\substack{\alpha\mathcal{O}_{\mathbf{K}}=\prod \partial_{\bar{u}(1),\ldots,\bar{u}(m)} \\ \bar{u}(1),\ldots,\bar{u}(m)\in\mathbb{F}_2^2}} \prod_{\substack{\bar{u}(1),\ldots,\bar{u}(m)\in\mathbb{F}_2^2 \\ \bar{v}(1),\ldots,\bar{v}(m)\in\mathbb{F}_2^2}} \left(\frac{\partial_{\bar{u}(1),\ldots,\bar{u}(m)}}{\partial_{\bar{v}(1),\ldots,\bar{v}(m)}}\right)^{\sum_{i=1}^m \Phi_1(\bar{u}(i),\bar{v}(i))}.$$

Therefore, we have

$$\sum_{\mathbf{L}\in\mathcal{F}(X)} 2^{m(rk_4(\mathrm{Cl}_{\mathbf{L}}))} \geq \sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} \frac{1}{2^{m(r_{\mathbf{K}}+2)}} T_m(\alpha\mathcal{O}_{\mathbf{K}}) \;\geq\; \frac{1}{2^{m(r_{\mathbf{K}}+2)}} N.$$

where

$$N = \sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}). \tag{14}$$

Now, we need to estimate N. Let $\bar{u}, \bar{v} \in \mathbb{F}_2^{2\,m}$ with $\bar{u} = (\bar{u}(1), \ldots, \bar{u}(m))$ and $\bar{v} = (\bar{v}(1), \ldots, \bar{v}(m))$. We define

$$\Phi_m(\bar{u}, \bar{v}) = \sum_{i=1}^{m} \Phi_1(\bar{u}(i), \bar{v}(i)). \tag{15}$$

Therefore we have proved the following theorem.

Theorem 36 *We have*

$$N = \sum_{(\partial_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2m}} \in \mathcal{D}(X,m)} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathbb{F}_2^{2m}} \partial_{\bar{u}})}} \prod_{\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_m(\bar{u},\bar{v})},$$

where $\mathcal{D}(X, m)$ is the set of 4^m -tuples of squarefree and coprime ideals $\partial_{\bar{u}}$ such that

(1) the index $\bar{u} = (\bar{u}(1), \ldots, \bar{u}(m)) \in \mathbb{F}_2^{2\,m}$ and
(2) $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} \partial_{\bar{u}} \in \mathcal{W}(X)$.

6.1 Eliminating indices corresponding to a large number of prime divisors

For any ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbf{K}}$, $\tau_{\mathbf{K},m}(\mathfrak{a})$ denotes the number of ordered ways of writing $\mathfrak{a}$ as a product of m ideals. Let

$$\sum\nolimits_1 = \sum_{\substack{(\partial_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2\,m}} \in \mathcal{D}(X,m) \\ \omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathbb{F}_2^{2\,m}} \partial_{\bar{u}}) > \Omega}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathbb{F}_2^{2\,m}} \partial_{\bar{u}})}} \prod_{\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_m(\bar{u},\bar{v})}.$$

Here, the parameter Ω will be chosen later. Since $\tau_{\mathbf{K},4^m}(\mathfrak{a}) = 2^{2\,m\omega_{\mathbf{K}}(\mathfrak{a})}$ for any squarefree ideal $\mathfrak{a}$, we have

$$\sum\nolimits_1 \ll \sum_{\substack{\mathfrak{N}(\mathfrak{a})\le X \\ \omega_{\mathbf{K}}(\mathfrak{a})>\Omega}} \mu^2(\mathfrak{a}) \frac{\tau_{\mathbf{K},4^m}(\mathfrak{a})}{2^{m\omega_{\mathbf{K}}(\mathfrak{a})}} \ll \sum_{\substack{\mathfrak{N}(\mathfrak{a})\le X \\ \omega_{\mathbf{K}}(\mathfrak{a})>\Omega}} \mu^2(\mathfrak{a}) 2^{m\omega_{\mathbf{K}}(\mathfrak{a})}.$$

By using Lemma 28 and Stirling's formula, we write

$$\begin{aligned} \sum\nolimits_1 &\ll \sum_{v>\Omega} 2^{mv} \sum_{\substack{\mathfrak{N}(\mathfrak{a})\le X \\ \omega_{\mathbf{K}}(\mathfrak{a})=v}} \mu^2(\mathfrak{a}) \ll_{\mathbf{K}} \sum_{v>\Omega} 2^{mv} \frac{X}{\log X} \frac{(\log\log X + B_0)^{v-1}}{(v-1)!} \\ &\ll_{\mathbf{K},m} \sum_{v\ge\Omega} 2^{mv} \frac{X}{\log X} \frac{(\log\log X + B_1)^{v}}{v!} \ll_{\mathbf{K},m} \sum_{v\ge\Omega} \frac{(2^m(\log\log X + B_1))^{v}}{(v/e)^{v}} \cdot \frac{X}{\log X}. \end{aligned}$$

By choosing $\Omega = e4^m(\log\log X + B_1)$, we see that the sum

$$\sum_{v\ge\Omega} \frac{(2^m(\log\log X+B_1))^v}{(v/e)^v} \le \sum_{v\ge\Omega}\frac{1}{2^{mv}} = \mathrm{O}(1),$$

for any $m \ge 1$ and hence we have

$$\sum\nolimits_1 \ll_{\mathbf{K},m} \frac{X}{\log X}. \tag{16}$$

6.2 Dissection of the range of the variables $\partial_{\bar u}$ into sub-intervals

Let $\Delta = 1 + \log^{-2^m} X$ and $A_{\bar u} = \Delta^r$, for some positive integer r, for all $\bar u \in \mathbb{F}_2^{2\,m}$. For $A = (A_{\bar u})_{\bar u\in\mathbb{F}_2^{2\,m}}$, we define

$$T(X,m,A) = \sum_{(\partial_{\bar u})}\Bigg(\prod_{\bar u} 2^{-m\omega_{\mathbf{K}}(\partial_{\bar u})}\Bigg)\prod_{\bar u,\bar v}\left(\frac{\partial_{\bar u}}{\partial_{\bar v}}\right)^{\Phi_m(\bar u,\bar v)},$$

where the sum is over $\partial_{\bar u} \in \mathcal{D}(X,m)$ such that $A_{\bar u} \le \mathfrak{N}(\partial_{\bar u}) \le \Delta A_{\bar u}$, $\omega_{\mathbf{K}}(\prod_{\bar u\in\mathbb{F}_2^{2\,m}}\partial_{\bar u}) \le \Omega$ for all $\bar u \in \mathbb{F}_2^{2\,m}$. Here $\mathcal{D}(X,m)$ is defined as in Theorem 36. By using (16), we write

$$N = \sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \sum_{A} T(X,m,A) + \mathrm{O}\left(\frac{X}{\log X}\right), \tag{17}$$

where A is such that $\prod_{\bar u\in\mathbb{F}_2^{2\,m}} A_{\bar u} \le X$. We will now consider 4 families of tuples $(A_{\bar u})_{\bar u\in\mathbb{F}_2^{2m}}$ and show that their contribution is negligible.

First family: The first family is defined by: $(A_{\bar u})$ such that $\prod_{\bar u\in\mathbb{F}_2^{2\,m}} A_{\bar u} \ge \Delta^{-4^m}X$. We have

$$\sum_{\substack{A\\ \prod_{\bar u\in\mathbb{F}_2^{2m}} A_{\bar u}\ge\Delta^{-4^m}X}} |T(X,m,A)| \ll \sum_{\substack{\Delta^{-4^m}X\le\mathfrak{N}(\mathfrak{a})\le X\\ \mathfrak{a}\in\mathcal{W}}} \mu^2(\mathfrak{a})2^{m\omega_{\mathbf{K}}(\mathfrak{a})}.$$

Using Lemma 30, $\displaystyle\sum_{\substack{\Delta^{-4^m}X\le\mathfrak{N}(\mathfrak{a})\le X\\ \mathfrak{a}\in\mathcal{W}}} \mu^2(\mathfrak{a})2^{m\omega_{\mathbf{K}}(\mathfrak{a})} \ll_{\mathbf{K},\mathfrak{f},m} X(1-\Delta^{-4^m})(\log X)^{2^m-1}.$

We note that $\Delta^{-4^m} = (1+\log^{-2^m} X)^{-4^m} = 1 - 4^m\log^{-2^m} X + \mathrm{O}_m(\log^{-2^{m+1}} X)$; hence

$$\sum_{\substack{A\\ \prod_{\bar u\in\mathbb{F}_2^{2m}} A_{\bar u}\ge\Delta^{-4^m}X}} |T(X,m,A)| \ll_{\mathbf{K},m} \frac{X}{\log X}.$$

Remark 37 Note that if $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} \le \Delta^{-4^m} X$ then $\mathfrak{N}\big(\prod_{\bar{u}\in\mathbb{F}_2^{2m}} \partial_{\bar{u}}\big) \le \Delta^{4^m} \prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} \le X$.

To introduce the other families, we define

$$X^{\dagger} = (\log X)^{\max(20,10(n_{\mathbf{K}}+1))(2+4^m(1+2^m))}, \quad \eta(m) = 2^{-m}\beta \tag{18}$$

$$X^{\ddagger} \text{ is the least } \Delta^{\ell} \text{ such that } \Delta^{\ell} \ge \exp(\log^{\eta(m)} X), \tag{19}$$

where $\beta > 0$ is sufficiently small.

Second family: This consists of $(A_{\bar{u}})$ such that $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} < \Delta^{-4^m} X$ and

$$\text{at most } 2^m - 1 \text{ of the } A_{\bar{u}} \text{ in } A = (A_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2m}} \text{ are greater than } X^{\ddagger}. \tag{20}$$

Then

$$\sum_{A \text{ satisfies } (20)} |T(X,m,A)| \le \sum_{0\le r\le 2^m-1} \sum_{\mathfrak{N}(\tilde{\partial}_1)\le (X^{\ddagger})^{4^m-r}} \mu^2(\tilde{\partial}_1)\tau_{\mathbf{K},4^m-r}(\tilde{\partial}_1)2^{-m\omega_{\mathbf{K}}(\tilde{\partial}_1)}$$
$$\times \sum_{\substack{\mathfrak{N}(\tilde{\partial}_2)\le \frac{X}{\mathfrak{N}(\tilde{\partial}_1)} \\ \tilde{\partial}_2\in\mathcal{W}}} \mu^2(\tilde{\partial}_2)\tau_{\mathbf{K},r}(\tilde{\partial}_2)2^{-m\omega_{\mathbf{K}}(\tilde{\partial}_2)}.$$

By using Lemma 30, we bound the inner sum by

$$\sum_{\substack{\mathfrak{N}(\tilde{\partial}_2)\le \frac{X}{\mathfrak{N}(\tilde{\partial}_1)} \\ \tilde{\partial}_2\in\mathcal{W}}} \mu^2(\tilde{\partial}_2)\tau_{\mathbf{K},r}(\tilde{\partial}_2)2^{-m\omega_{\mathbf{K}}(\tilde{\partial}_2)} \ll \sum_{\substack{\mathfrak{N}(\tilde{\partial}_2)\le \frac{X}{\mathfrak{N}(\tilde{\partial}_1)} \\ \tilde{\partial}_2\in\mathcal{W}}} \tau_{\mathbf{K},2}(\tilde{\partial}_2)^{-m+\log_2 r}$$
$$\ll_{\mathbf{K},m} \frac{X}{\mathfrak{N}(\tilde{\partial}_1)} (\log X)^{\frac{r2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}-1}.$$

Thus

$$\sum_{A \text{ satisfies } (20)} |T(X,m,A)| \ll_{\mathbf{K},m} X \sum_{0\le r\le 2^m-1} (\log X)^{\frac{r2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}-1}$$
$$\sum_{\mathfrak{N}(\tilde{\partial}_1)\ll_{\mathbf{K},m}(X^{\ddagger})^{4^m-r}} \mu^2(\tilde{\partial}_1)\frac{2^{m\omega_{\mathbf{K}}(\tilde{\partial}_1)}}{\mathfrak{N}(\tilde{\partial}_1)}$$
$$\ll_{\mathbf{K},m} X \sum_{0\le r\le 2^m-1} (\log X)^{\frac{r2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}-1}$$
$$\prod_{\substack{\mathfrak{p} \\ \mathfrak{N}(\mathfrak{p})\le (X^{\ddagger})^{4^m-r}}} \left(1+\frac{2^m}{\mathfrak{N}(\mathfrak{p})}\right)$$

$$\ll_{\mathbf{K},m} X \sum_{0\le r\le 2^m-1} (\log X)^{\frac{r2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}-1}$$

$$\prod_{\substack{\mathfrak{p} \\ \mathfrak{N}(\mathfrak{p})\le (X^{\ddagger})^{4^m-r}}} \left(1-\frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^{-2^m}.$$

By using Mertens's theorem for number fields (Theorem 1, [5]), we have

$$\sum_{A \text{ satisfies } (20)} |T(X,m,A)| \ll_{\mathbf{K},m} \frac{X}{\log X}\left(\frac{(\log X)^{\frac{2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}\cdot 2^m}-1}{(\log X)^{\frac{2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}}-1}\right)(\log X^{\ddagger})^{2^m}$$

$$\ll_{\mathbf{K},m} X \log^{2^m\eta(m)-1+\frac{1-2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}} X.$$

Definition 38 The variables $\bar{u}$ and $\bar{v}$ are said to be linked if $\Phi_m(\bar{u},\bar{v})+\Phi_m(\bar{v},\bar{u})=1$.

Third family: This consists of $(A_{\bar{u}})$ such that

(i) $\prod_{\bar{u}} A_{\bar{u}} < \Delta^{-4^m} X$.
(ii) At least 2^m of the $A_{\bar{u}}$ in $A=(A_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2m}}$ are greater than $X^{\ddagger}$.
(iii) There exists two linked indices $\bar{u}, \bar{v}$ such that $A_{\bar{u}}, A_{\bar{v}} \ge X^{\dagger}$.

Without loss of generality, we assume $\Phi_m(\bar{u},\bar{v})=1$.

$$|T(X,m,A)| \ll \sum_{\substack{(\partial_{\bar{w}})_{\bar{w}\ne\bar{v},\bar{u}} \\ A_{\bar{w}}\le\mathfrak{N}(\partial_{\bar{w}})\le\Delta A_{\bar{w}}}} \prod_{\bar{w}\ne\bar{u},\bar{v}} 2^{-m\omega_{\mathbf{K}}(\partial_{\bar{w}})}$$
$$\times\left|\sum_{A_{\bar{u}}\le\mathfrak{N}(\partial_{\bar{u}})\le\Delta A_{\bar{u}}} \sum_{\substack{A_{\bar{v}}\le\mathfrak{N}(\partial_{\bar{v}})\le\Delta A_{\bar{v}} \\ \partial_{\bar{v}}\in\mathcal{W}}} a(\partial_{\bar{u}},(\partial_{\bar{w}})_{\bar{w}\ne\bar{v},\bar{u}})a(\partial_{\bar{v}},(\partial_{\bar{w}})_{\bar{w}\ne\bar{v},\bar{u}})\left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)\right|, \tag{21}$$

where $a(\partial_{\bar{u}},(\partial_{\bar{w}})_{\bar{w}\ne\bar{v},\bar{u}}) = 2^{-m\omega_{\mathbf{K}}(\partial_{\bar{u}})} \prod_{\bar{w}\ne\bar{u},\bar{v}} \left(\frac{\partial_{\bar{w}}}{\partial_{\bar{u}}}\right)^{\Phi_m(\bar{w},\bar{u})} \prod_{\bar{w}\ne\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{w}}}\right)^{\Phi_m(\bar{u},\bar{w})}$.

Analogously we have $a(\partial_{\bar{v}},(\partial_{\bar{w}})_{\bar{w}\ne\bar{v},\bar{u}})$. We would now like to apply Lemma 35. For this we note that $\left(\frac{\cdot}{\partial_{\bar{v}}}\right)$ is a primitive character modulo $\partial_{\bar{v}}$. Each character appearing in (21) is primitive with a distinct conductor. Hence these characters are distinct. We now apply Lemma 35, to obtain, for any integer $g>0$

$$|T(X,m,A)| \ll \prod_{\bar{w}\ne\bar{u},\bar{v}} A_{\bar{w}}\Bigg(A_{\bar{v}}A_{\bar{u}}(A_{\bar{v}}^{\frac{-1}{4g}}\log A_{\bar{u}}) + A_{\bar{v}}^{1-\frac{1}{2g}} A_{\bar{u}}^{1-\frac{1}{2(n_{\mathbf{K}}+1)}} \log A_{\bar{u}}$$
$$\left(\sum_{\mathfrak{N}(\mathfrak{a})\le A_{\bar{v}}} \mathfrak{N}(\mathfrak{a})^{\frac{2}{n_{\mathbf{K}}+1}}\right)^{\frac{1}{2g}}\Bigg)$$

$$\ll \prod_{\bar{w}\neq\bar{u},\bar{v}} A_{\bar{w}}\left(A_{\bar{v}}A_{\bar{u}}(A_{\bar{v}}^{\frac{-1}{4g}}\log A_{\bar{u}}) + A_{\bar{v}}A_{\bar{u}}^{1-\frac{1}{2(n_{\mathbf{K}}+1)}}A_{\bar{v}}^{\frac{1}{g(n_{\mathbf{K}}+1)}}\log A_{\bar{u}}\right)$$

$$\ll X((X^{\dagger})^{\frac{-1}{4g}}\log X) + X(A_{\bar{u}}^{\frac{-1}{2(n_{\mathbf{K}}+1)}}A_{\bar{v}}^{\frac{1}{g(n_{\mathbf{K}}+1)}})\log X.$$

By choosing $g = 5$, we see that if $A_{\bar{v}} \ll A_{\bar{u}}^2$ holds, then

$$|T(X, m, A)| \ll X(X^{\dagger})^{-\min\left(\frac{1}{10(n_{\mathbf{K}}+1)}, \frac{1}{20}\right)}\log X.$$

We now tackle the case $A_{\bar{u}}^2 \ll A_{\bar{v}}$. Using the Cauchy Schwarz inequality, we may bound the sum inside the absolute value in (21) by

$$\ll A_{\bar{u}}^{\frac{1}{2}}\left(\sum_{\partial_{\bar{u}}}\left|\sum_{\partial_{\bar{v}}} a(\partial_{\bar{v}}, (\partial_{\bar{w}})_{\bar{w}\neq\bar{v},\bar{u}})\left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)\right|^2\right)^{\frac{1}{2}}.$$

If $\partial_{\bar{u}} = s\mathcal{O}_{\mathbf{K}}$, then by definition of $\left(\frac{\cdot}{\partial_{\bar{v}}}\right)$ for $\partial_{\bar{v}} \in \mathcal{W}(X)$, $\left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right) = \left(\frac{s\varepsilon_s}{\partial_{\bar{v}}}\right)$. Here ε_s is as defined before Lemma 23. By Lemma 23, $\left(\frac{s\epsilon_s}{\cdot}\right)$ is a primitive character modulo $4\partial_{\bar{u}}$. Now, by Lemma 32, we obtain (when $A_{\bar{u}}^2 \ll A_{\bar{v}}$)

$$|T(X, m, A)| \ll \prod_{\bar{w}\neq\bar{u},\bar{v}} A_{\bar{w}}(A_{\bar{u}}^{\frac{1}{2}}A_{\bar{v}}^{\frac{1}{2}}(A_{\bar{u}}^2 + A_{\bar{v}})^{\frac{1}{2}}) \ll XA_{\bar{u}}^{\frac{-1}{2}} \ll X(X^{\dagger})^{\frac{-1}{2}}.$$

By summing over all $O((\log X)^{4^m(1+2^m)})$ possible A and using the definition of $X^{\dagger}$ we get

$$\sum_{A \text{ satisfies (i), (ii), (iii)}} |T(X, m, A)| \ll \frac{X}{\log X}.$$

Fourth family: This consists of $(A_{\bar{u}})$ such that

(i) $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} < \Delta^{-4^m}X$.
(ii) There exists two linked indices $\bar{u}, \bar{v}$ such that $2 \leq A_{\bar{v}} < X^{\dagger}$ and $A_{\bar{u}} \geq X^{\ddagger}$.
(iii) $\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathbb{F}_2^{2m}} \partial_{\bar{u}}) \leq \Omega$.
(iv) Two indices $\bar{u}, \bar{v}$ with $A_{\bar{u}}, A_{\bar{v}} > X^{\dagger}$ are always unlinked.
(v) At least 2^m of the $A_{\bar{u}}$ in $A = (A_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2m}}$ are greater than $X^{\ddagger}$.

By assumption (ii), there exists an index $\bar{v}$ which is linked to $\bar{u}$. We observe that there may be more than one index linked to $\bar{u}$. Recall that

$$T(X, m, A) = \sum_{(\partial_{\bar{u}})}\left(\prod_{\bar{u}} 2^{-m\omega_{\mathbf{K}}(\partial_{\bar{u}})}\right)\prod_{\bar{u},\bar{v}}\left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_m(\bar{u},\bar{v})}.$$

Let $I_1 \subset \mathbb{F}_2^{2m}$ be the set of all indices linked with $\bar{u}$ and let $I_2 \subset \mathbb{F}_2^{2m}$ be the set of all indices unlinked with $\bar{u}$. We now divide the above sum into three sums as follows

$$T(X, m, A) = \sum_{(\partial_{\bar{w}})_{\bar{w}\in I_1}} \sum_{(\partial_{\bar{w}_1})_{\bar{w}_1\in I_2}} \sum_{\partial_{\bar{u}}} \left(\prod_{\bar{u}_1\in\mathbb{F}_2^{2m}} 2^{-m\omega_{\mathbf{K}}(\partial_{\bar{u}_1})} \right) \prod_{\bar{u}_2,\bar{v}\in\mathbb{F}_2^{2m}} \left(\frac{\partial_{\bar{u}_2}}{\partial_{\bar{v}}}\right)^{\Phi_m(\bar{u}_2,\bar{v})}.$$

Taking absolute values, we get

$$|T(X, m, A)| \leq \sum_{(\partial_{\bar{w}})_{\bar{w}\in I_1}} \sum_{(\partial_{\bar{w}_1})_{\bar{w}_1\in I_2}} \left| \sum_{\partial_{\bar{u}}} \left(\prod_{\bar{u}_1\in\mathbb{F}_2^{2m}} 2^{-m\omega_{\mathbf{K}}(\partial_{\bar{u}_1})} \right) \prod_{\bar{u}_2,\bar{v}\in\mathbb{F}_2^{2m}} \left(\frac{\partial_{\bar{u}_2}}{\partial_{\bar{v}}}\right)^{\Phi_m(\bar{u}_2,\bar{v})} \right|.$$

Any term given by $\left(\frac{\partial_{\bar{u}_2}}{\partial_{\bar{v}}}\right)$ with $\bar{u}_2, \bar{v} \neq \bar{u}$, can be pulled out of the sum over $\partial_{\bar{u}}$ and can be bounded by 1. If we have a term given by $\left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)$ with $\bar{v} \in I_2$, then the term $\left(\frac{\partial_{\bar{v}}}{\partial_{\bar{u}}}\right)$ will also appear in the product and by Lemma 27, they can be multiplied to give 1. Finally we are left with terms given by $\left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)$ or $\left(\frac{\partial_{\bar{v}}}{\partial_{\bar{u}}}\right)$ with $\bar{v} \in I_1$. By Lemma 27 and multiplicativity of these characters, we get

$$\begin{aligned} |T(X, m, A)| &\leq \sum_{(\partial_{\bar{w}})_{\bar{w}\in I_1}} \sum_{(\partial_{\bar{w}_1})_{\bar{w}_1\in I_2}} \left| \sum_{\partial_{\bar{u}}} \frac{\mu^2(\prod \partial_{\bar{w}})}{2^{m\omega_{\mathbf{K}}(\partial_{\bar{u}})}} \left(\frac{\partial_{\bar{u}}}{\prod_{\bar{w}_1\in I_2} \partial_{\bar{w}_1}} \right) \right| \\ &\leq \sum_{(\partial_{\bar{w}})_{\bar{w}\in I_1}} \sum_{(\partial_{\bar{w}_1})_{\bar{w}_1\in I_2}} \sum_{0\leq \ell \leq \Omega} \frac{1}{2^{m\ell}} \left| \sum_{\substack{\partial_{\bar{u}} \\ \omega(\partial_{\bar{u}})=\ell}} \mu^2(\prod \partial_{\bar{w}}) \left(\frac{\partial_{\bar{u}}}{\prod_{\bar{w}_1\in I_2} \partial_{\bar{w}_1}} \right) \right|. \end{aligned}$$

Writing $\partial_{\bar{u}} = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell$ in ascending order of absolute norm, the inner sum is bounded by

$$\begin{aligned} &\left| \sum_{\substack{\partial_{\bar{u}} \\ \omega(\partial_{\bar{u}})=\ell}} \mu^2(\prod \partial_{\bar{w}}) \left(\frac{\partial_{\bar{u}}}{\prod_{\bar{w}_1\in I_2} \partial_{\bar{w}_1}} \right) \right| \\ &\leq \sum_{\mathfrak{p}_1} \cdots \sum_{\mathfrak{p}_{\ell-1}} \left| \sum_{\mathfrak{p}_\ell} \mu^2(\mathfrak{p}_1 \ldots \mathfrak{p}_\ell \prod_{\bar{w}\neq\bar{u}} \partial_{\bar{w}}) \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2} \partial_{\bar{w}_1}} \right) \right|, \end{aligned} \tag{22}$$

where $\left(\frac{\cdot}{\prod_{\bar{w}_1\in I_2} \partial_{\bar{w}_1}} \right)$ is non-trivial generalised Dirichlet character. We note here that

$$A_{\bar{u}}^{1/\ell} \leq \mathfrak{N}(\mathfrak{p}_\ell) \leq \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_{\ell-1})}. \tag{23}$$

If $\mathfrak{p}_\ell \mid \prod_{\bar{w}\neq\bar{u}} \partial_{\bar{w}}$ then the corresponding term in (22) is zero and number of such $\mathfrak{p}_\ell$ is at most Ω by condition (iii) above. Therefore, we have

$$\sum_{\mathfrak{N}(\mathfrak{p}_\ell)\leq\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\ldots,\mathfrak{p}_{\ell-1})}} \mu^2(\mathfrak{p}_1\ldots\mathfrak{p}_\ell \prod_{\bar{w}\neq\bar{u}} \partial_{\bar{w}})\left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right)$$

$$= \mu^2(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1} \prod_{\bar{w}\neq\bar{u}} \partial_{\bar{w}}) \sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\leq\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\ldots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}\neq\bar{u}}\partial_{\bar{w}})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right) + \mathrm{O}(\Omega).$$

However

$$\mu^2(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1} \prod_{\bar{w}\neq\bar{u}} \partial_{\bar{w}}) \sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\leq\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\ldots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}\neq\bar{u}}\partial_{\bar{w}})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right)$$

$$= \mu^2(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1} \prod_{\bar{w}\neq\bar{u}} \partial_{\bar{w}}) \sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\leq\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\ldots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right) + \mathrm{O}(\Omega).$$

Applying Lemma 33, we obtain for any $\beta_1 > 0$,

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\leq\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\ldots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right) \ll$$

$$\left(\mathfrak{N}\left(\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}\right)\right)^{\beta_1} \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})} \log^2 \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})}$$

$$\exp\left(-2c_{\mathbf{K},\epsilon}\frac{\left(\log\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})}\right)^{\frac{1}{2}}}{(\mathfrak{N}(\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}))^{\beta_1}}\right)$$

$$\ll_{\beta_1} \frac{\mathfrak{N}(\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})^{\beta_1(1+2B)}}{\log^{B-2}\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})}} \cdot \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})}.$$

Choosing $\beta_1 = \frac{1}{2(1+2B)}$, we obtain

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\leq\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\ldots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right) \ll_B \frac{\mathfrak{N}(\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})^{1/2}}{\log^{B-2}\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})}} \cdot \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1})}.$$

By (23) we have

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\le \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\dots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_\ell}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right) \ll_B \frac{\mathfrak{N}(\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})^{1/2}}{\log^{B-2} A_{\bar{u}}^{1/\ell}}\cdot\frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1\dots\mathfrak{p}_{\ell-1})}.$$

By the definition of the fourth family, we have $A_{\bar{u}} \ge X^{\ddagger} \ge \exp(\log^{\eta(m)} X)$. This implies that

$$\frac{\log^{B-2} A_{\bar{u}}}{\ell^{B-2}} \gg_{\mathbf{K},B} \frac{\log^{(B-2)\eta(m)} X}{(\log\log X)^{B-2}} \gg_{\mathbf{K},B} \log^{\frac{(B-2)\eta(m)}{2}} X.$$

Therefore, we have

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p}_\ell)\le \frac{\Delta A_{\bar{u}}}{\mathfrak{N}(\mathfrak{p}_1,\dots,\mathfrak{p}_{\ell-1})}\\ \gcd(\mathfrak{p}_\ell,\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})=\mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathfrak{p}_l}{\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1}}\right) \ll_B \Delta A_{\bar{u}}\frac{\mathfrak{N}(\prod_{\bar{w}_1\in I_2}\partial_{\bar{w}_1})^{1/2}}{\mathfrak{N}(\mathfrak{p}_1\dots\mathfrak{p}_{l-1})}\log^{-\frac{(B-2)\eta(m)}{2}} X.$$

Also, we see that

$$\sum_{\ell\le\Omega}\frac{1}{2^{m\ell}}\sum_{\mathfrak{N}(\mathfrak{p}_1\cdots\mathfrak{p}_{\ell-1})\le\Delta A_{\bar{u}}}\frac{\mu^2(\mathfrak{p}_1\dots\mathfrak{p}_{\ell-1})}{\mathfrak{N}(\mathfrak{p}_1\cdots\mathfrak{p}_{\ell-1})} \ll \log\Delta A_{\bar{u}} \ll \log X$$

and $\sum_{\mathfrak{N}(\partial_{\bar{w}_1})\le X^{\dagger}}\mathfrak{N}(\partial_{\bar{w}_1})^{\frac{1}{2}} \ll (X^{\dagger})^{\frac{3}{2}}$. Further

$$\sum_{(\partial_{\bar{w}})_{\bar{w}\in I_1}}\ \sum_{(\partial_{\bar{w}_1})_{\bar{w}_1\in I_2}}\ \sum_{0\le\ell\le\Omega}\frac{1}{2^{m\ell}}\sum_{\mathfrak{p}_1}\cdots\sum_{\substack{\mathfrak{p}_{\ell-1}\\ \mathfrak{N}(\mathfrak{p}_1\cdots\mathfrak{p}_{\ell-1})\le\Delta A_{\bar{u}}^{1-1/\ell}}} 1 \ll X(X^{\ddagger})^{-\frac{1}{\Omega}}.$$

Hence, for $B \gg 1$, we have

$$\begin{aligned}|T(X,m,A)| &\ll_B \prod_{\bar{w}\in I_1}A_{\bar{w}}\cdot\prod_{\bar{w}_1\in I_2}(X^{\dagger})^{\frac{3}{2}}\cdot((\log X)^{-B\eta(m)+1}A_{\bar{u}}) + \Omega X(X^{\ddagger})^{-\frac{1}{\Omega}}\\ &\ll_B X\left((\log X)^{-B\eta(m)+1}\cdot(X^{\dagger})^{\frac{4^m}{2}}+\frac{\log\log X}{(X^{\ddagger})^{1/\Omega}}\right) \ll_B \frac{X}{\log X}.\end{aligned}$$

Combining the estimates for all the four families and recalling $\eta(m) = 2^{-m}\beta$ we get:

Proposition 39 *For every $m \ge 1$ and $\beta > 0$ sufficiently small, we have*

$$\sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \sum_A{}^{*}\, T(X,m,A) + O\left(\frac{X}{(\log X)^{1-\frac{1}{|H_{\mathfrak{f}}(\mathbf{K})|}}}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}}(\mathbf{K})|}}\right), \quad (24)$$

where the sum is over tuples $(A_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2m}}$ satisfying the following conditions:

(i) $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} < \Delta^{-4^m} X$
(ii) *At least 2^m indices satisfy $A_{\bar{u}} > X^{\ddagger}$,*
(iii) *Two indices $\bar{u}, \bar{v}$ with $A_{\bar{u}}, A_{\bar{v}} \geq X^{\dagger}$ are always unlinked,*
(iv) *If two indices $\bar{u}, \bar{v}$ with $A_{\bar{v}} \leq A_{\bar{u}}$ are linked then either $A_{\bar{v}} = 1$ or $2 \leq A_{\bar{v}} < X^{\dagger}$ and $A_{\bar{u}} \leq X^{\ddagger}$.*

6.3 Geometry of unlinked indices

Lemma 40 (Lemma 18, [4]) *Let $m \geq 1$ be an integer and let $\mathcal{U} \subseteq \mathbb{F}_2^{2m}$ be a set of unlinked indices. Then $\#\mathcal{U} \leq 2^m$ and for any $\bar{u} \in \mathbb{F}_2^{2m}$, $\bar{u} + \mathcal{U}$ is also a set of unlinked indices. If $\#\mathcal{U} = 2^m$ then $\mathcal{U}$ is a vector subspace of dimension m in $\mathbb{F}_2^{2m}$ or a coset of such a subspace.*

Proposition 41 *For every $m \geq 1$ and $\beta > 0$, we have*

$$\sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \sum_{A}^{*} T(X, m, A) + O\left(\frac{X}{(\log X)^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}}}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right),$$

where the $(*)$ in the sum is used to indicate that A varies over

(i) $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} < \Delta^{-4^m} X,$
(ii) *$\mathcal{U} = \{\bar{u} : A_{\bar{u}} > X^{\ddagger}\}$ is a maximal set of unlinked indices,*
(iii) *$A_{\bar{u}} = 1$ for $\bar{u} \notin \mathcal{U}$.*

Proof For $B \gg_{m,\beta} 1$ we have $X^{\ddagger} > (\log^{\eta(m)} X)^B > X^{\dagger}$. Therefore, by part (iii) of Proposition 39, $\mathcal{U}$ is a set of unlinked indices. Further by part (ii) of Proposition 39, $\mathcal{U}$ contains at least 2^m elements. By Lemma 40, $\mathcal{U}$ must be a maximal set of unlinked indices. For $\bar{v} \notin \mathcal{U}$ there exists $\bar{u} \in \mathcal{U}$ such that $\bar{u}$ and $\bar{v}$ are linked. Since $A_{\bar{u}} \geq A_{\bar{v}}$, by part (iv) of Proposition 39 either $A_{\bar{v}} = 1$ or $2 \leq A_{\bar{v}} < X^{\dagger}$ and $A_{\bar{v}} \leq A_{\bar{u}} \leq X^{\ddagger}$. But $A_{\bar{u}} > X^{\ddagger}$ so $A_{\bar{v}} = 1$. □

Definition 42 Let $\mathcal{U} \subseteq \mathbb{F}_2^{2m}$ denote an unlinked set of 2^m indices. We say $A = (A_{\bar{u}})_{\bar{u}\in\mathbb{F}_2^{2m}}$ is admissible for $\mathcal{U}$ if it satisfies:

(i) $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} < \Delta^{-4^m} X,$
(ii) $\mathcal{U} = \{\bar{u} : A_{\bar{u}} > X^{\ddagger}\},$
(iii) $A_{\bar{u}} = 1$ for $\bar{u} \notin \mathcal{U}.$

Note: If $A_{\bar{u}} = 1$ then $\mathfrak{d}_{\bar{u}} = \mathcal{O}_{\mathbf{K}}$.

6.4 The final estimate

We begin by recalling the sum we want to estimate. Recall that

$$\sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \sum_{\substack{(\partial_{\bar{u}})\\ \prod\partial_{\bar{u}}\in\mathcal{W}(X)}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})}} \prod_{\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_{\mathbf{K}}(\bar{u},\bar{v})}.$$

By Proposition 41, we have

$$\begin{aligned}\sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) &= \sum_{\substack{(\partial_{\bar{u}})\\ \prod\partial_{\bar{u}}\in\mathcal{W}(X)}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})}} \prod_{\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_{\mathbf{K}}(\bar{u},\bar{v})}\\ &= \sum_{A}^{*} T(X,m,A) + O\left(\frac{X}{(\log X)^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}}} (\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right),\end{aligned}$$

where the $(*)$ in the sum is used to indicate that A varies over

(i) $\prod_{\bar{u}\in\mathbb{F}_2^{2m}} A_{\bar{u}} < \Delta^{-4^m} X$,

(ii) $\mathcal{U} = \{\bar{u} : A_{\bar{u}} > X^{\ddagger}\}$ is a maximal set of unlinked indices,

(iii) $A_{\bar{u}} = 1$ for $\bar{u} \notin \mathcal{U}$.

By the definition of admissible A (Definition 42), we get

$$\begin{aligned}\sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) &= \sum_{A}^{*} T(X,m,A)\\ &\quad + O\left(\frac{X}{(\log X)^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}}} (\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right)\\ &= \sum_{\mathcal{U}} \sum_{A \text{ admissible for } \mathcal{U}} T(X,m,A)\\ &\quad + O\left(\frac{X}{\log^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}} X} \log^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}} X\right).\end{aligned}$$

Here

$$T(X,m,A) = \sum_{\substack{(\partial_{\bar{u}}),\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})\le\Omega\\ A_{\bar{u}}\le\mathfrak{N}(\partial_{\bar{u}})\le\Delta A_{\bar{u}}\\ \prod\partial_{\bar{u}}\in\mathcal{W}(X)}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})}} \prod_{\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_{\mathbf{K}}(\bar{u},\bar{v})}.$$

Let us look at

$$\left|\sum_{A} \sum_{\substack{(\partial_{\bar{u}}),\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})>\Omega\\ A_{\bar{u}}\le\mathfrak{N}(\partial_{\bar{u}})\le\Delta A_{\bar{u}}\\ \prod\partial_{\bar{u}}\in\mathcal{W}(X)}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})}} \prod_{\bar{u},\bar{v}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_{\mathbf{K}}(\bar{u},\bar{v})}\right| \le \sum_{A} \sum_{\substack{(\partial_{\bar{u}}),\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})>\Omega\\ A_{\bar{u}}\le\mathfrak{N}(\partial_{\bar{u}})\le\Delta A_{\bar{u}}\\ \prod\partial_{\bar{u}}\in\mathcal{W}(X)}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod\partial_{\bar{u}})}}.$$

Since

$$\sum_{A} \sum_{\substack{(\partial_{\bar{u}}),\omega_{\mathbf{K}}(\prod \partial_{\bar{u}})>\Omega \\ A_{\bar{u}}\leq \mathfrak{N}(\partial_{\bar{u}})\leq \Delta A_{\bar{u}} \\ \prod \partial_{\bar{u}}\in \mathcal{W}(X)}} \frac{1}{2^{m\omega_{\mathbf{K}}(\prod \partial_{\bar{u}})}} \ll \sum_{\ell\geq\Omega} \sum_{\substack{\mathfrak{N}(\mathfrak{a})\leq X \\ \omega_{\mathbf{K}}(\mathfrak{a})=\ell}} 2^{-m\omega_{\mathbf{K}}(\mathfrak{a})}\tau_{4^m}(\mathfrak{a})$$

$$\ll \frac{X}{\log X}. \text{ (cf. subsection 6.1)}$$

For a set of maximally unlinked indices $\mathcal{U}$ and an A admissible for $\mathcal{U}$, we set

$$T'(X,m,A) = \sum_{\substack{(\partial_{\bar{u}})_{\bar{u}\in\mathcal{U}} \\ A_{\bar{u}}\leq \mathfrak{N}(\partial_{\bar{u}})\leq \Delta A_{\bar{u}} \\ \prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}\in \mathcal{W}(X)}} \mu^2\left(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}\right) 2^{-m\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}})} \prod_{\bar{u},\bar{v}\in\mathcal{U}} \left(\frac{\partial_{\bar{u}}}{\partial_{\bar{v}}}\right)^{\Phi_{\mathbf{K}}(\bar{u},\bar{v})}.$$

By Lemma 27 we get

$$T'(X,m,A) = \sum_{\substack{(\partial_{\bar{u}})_{\bar{u}\in\mathcal{U}} \\ A_{\bar{u}}\leq \mathfrak{N}(\partial_{\bar{u}})\leq \Delta A_{\bar{u}} \\ \prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}\in \mathcal{W}(X)}} \mu^2(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}) 2^{-m\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}})}.$$

Therefore we have

$$\sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \sum_{\mathcal{U}} \sum_{A \text{ admissible for } \mathcal{U}} T'(X,m,A)$$

$$+O\left(\frac{X}{\log^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}} X}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right).$$

We now consider the sum

$$\sum_{A \text{ admissible for } \mathcal{U}} \sum_{\substack{(\partial_{\bar{u}})_{\bar{u}\in\mathcal{U}} \\ A_{\bar{u}}\leq \mathfrak{N}(\partial_{\bar{u}})\leq \Delta A_{\bar{u}} \\ \prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}\in \mathcal{W}(X)}} \mu^2(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}) 2^{-m\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}})}.$$

Since A is admissible for $\mathcal{U}$, at least 2^m entries of the tuple A are 1 and these are all the entries with $A_{\bar{u}} \leq X^{\ddagger}$. We first note that any $\mathfrak{a} \in \mathcal{W}(\Delta^{-4^m}X)$, with norm greater than $X^{\ddagger}$, appears as a product of the form $\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}$, for some A admissible for $\mathcal{U}$. Each such $\mathfrak{a}$ appears as many times as the number of factorisations of $\mathfrak{a}$ into 2^m ideals each of norm greater than $X^{\ddagger}$. Therefore we have

$$\sum_{A \text{ admissible for } \mathcal{U}} T'(X,m,A) = \sum_{A \text{ admissible for } \mathcal{U}} \sum_{\substack{(\partial_{\bar{u}})_{\bar{u}\in\mathcal{U}} \\ A_{\bar{u}}\leq \mathfrak{N}(\partial_{\bar{u}})\leq \Delta A_{\bar{u}} \\ \prod \partial_{\bar{u}}\in \mathcal{W}(X)}} \mu^2(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}}) 2^{-m\omega_{\mathbf{K}}(\prod_{\bar{u}\in\mathcal{U}} \partial_{\bar{u}})}$$

$$
\begin{aligned}
&= \sum_{\mathfrak{a}\in\mathcal{W}(X)} \mu^2(\mathfrak{a})\tau_{\mathbf{K},2^m}(\mathfrak{a})2^{-m\omega_{\mathbf{K}}(\mathfrak{a})} \\
&\quad + O\Bigg(\sum_{\substack{\Delta^{-4^m} X\leq\mathfrak{N}(\mathfrak{a})\leq X \\ \mathfrak{a}\in\mathcal{W}(X)}} \mu^2(\mathfrak{a})\tau_{\mathbf{K},2^m}(\mathfrak{a})2^{-m\omega_{\mathbf{K}}(\mathfrak{a})}\Bigg) \\
&\quad + O\Bigg(\sum_{\mathfrak{b}\in\mathcal{W}(X^{\ddagger})} 2^{-m\omega_{\mathbf{K}}(\mathfrak{b})}\tau_{\mathbf{K},2^m}(\mathfrak{b})\mu^2(\mathfrak{b}) \\
&\quad \sum_{\mathfrak{c}\in\mathcal{W}(\frac{X}{\mathfrak{N}(b)})} 2^{-m\omega_{\mathbf{K}}(\mathfrak{c})}(2^m-1)^{\omega_{\mathbf{K}}(\mathfrak{c})}\mu^2(\mathfrak{c})\Bigg),
\end{aligned}
$$

where the last term corresponds to the summands which have at least one factor that is less than $X^{\ddagger}$. By using Lemma 30, the inner sum of the second error term is bounded by

$$
\begin{aligned}
I &= \sum_{\mathfrak{c}\in\mathcal{W}(\frac{X}{\mathfrak{N}(b)})} 2^{-m\omega_{\mathbf{K}}(\mathfrak{c})}(2^m-1)^{\omega_{\mathbf{K}}(\mathfrak{c})}\mu^2(\mathfrak{c}) = \sum_{\mathfrak{c}\in\mathcal{W}(\frac{X}{\mathfrak{N}(b)})} \tau_{\mathbf{K},2}(\mathfrak{c})^{-m+\log_2(2^m-1)} \\
&\ll \frac{X}{\mathfrak{N}(\mathfrak{b})}(\log X)^{\frac{2^{-m+\log_2(2^m-1)}}{|H_{\mathfrak{f}(\mathbf{K})}|}-1} \ll \frac{X}{\mathfrak{N}(\mathfrak{b})}(\log X)^{\frac{1-2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}-1}.
\end{aligned}
$$

Then by using Mertens's theorem for number fields (Theorem 1, [5]), we can bound the second O term as

$$
\begin{aligned}
X(\log X)^{\frac{1-2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}-1} \sum_{1\leq\mathfrak{N}(\mathfrak{b})\leq X^{\ddagger}} \frac{\mu^2(\mathfrak{b})}{\mathfrak{N}(\mathfrak{b})} &\ll X(\log X)^{\frac{1-2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}-1} \prod_{\mathfrak{N}(\mathfrak{p})\leq X^{\ddagger}} \left(1+\frac{1}{\mathfrak{N}(\mathfrak{p})}\right) \\
&\ll \frac{X}{\log^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}} X}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}
\end{aligned}
$$

By using similar arguments as in the estimate of the first family, we see that the first error term is bounded by $X/\log X$. Therefore, we have

$$
\begin{aligned}
\sum_{A \text{ admissible for } \mathcal{U}} T'(X,m,A) &= \sum_{\mathfrak{a}\in\mathcal{W}(X)} \mu^2(\mathfrak{a})\tau_{\mathbf{K},2^m}(\mathfrak{a})2^{-m\omega_{\mathbf{K}}(\mathfrak{a})} \\
&\quad + O\left(\frac{X}{\log^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}} X}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right).
\end{aligned}
$$

As noted before for a squarefree ideal $\mathfrak{a}$, $\tau_{\mathbf{K},2^m}(\mathfrak{a}) = 2^{m\omega_{\mathbf{K}}(\mathfrak{a})}$. This lets us conclude that

$$
\frac{1}{2^{m(r_{\mathbf{K}}+2)}} \sum_{\alpha\mathcal{O}_{\mathbf{K}}\in\mathcal{W}(X)} T_m(\alpha\mathcal{O}_{\mathbf{K}}) = \frac{1}{2^{m(r_{\mathbf{K}}+2)}} \sum_{\mathcal{U}} \sum_{\mathfrak{a}\in\mathcal{W}(X)} 1
$$

$$
\begin{aligned}
&+O\left(\frac{X}{\log^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}} X}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right)\\
&=\frac{\mathcal{N}(2m,2)}{2^{m(r_{\mathbf{K}}+1)}}\sum_{\mathfrak{a}\in\mathcal{W}(X)}1\\
&+O\left(\frac{X}{\log^{1-\frac{1}{|H_{\mathfrak{f}(\mathbf{K})}|}} X}(\log X)^{2^m\eta(m)-\frac{2^{-m}}{|H_{\mathfrak{f}(\mathbf{K})}|}}\right).
\end{aligned}
$$

7 Examples

In this section, we give examples of number fields which satisfy all the above conditions.

7.1 Example 1

$\mathbf{K}=\mathbb{Q}(i)$.

It is obvious that $\mathbb{Q}(i)$ satisfies conditions 1 and 2. We know that $2\mathbb{Z}$ ramifies in $\mathbf{K}$. For the unique prime $\mathfrak{p}\mid 2\mathcal{O}_{\mathbf{K}}$, $|(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^2)^*|=\mathfrak{N}(\mathfrak{p})(\mathfrak{N}(\mathfrak{p})-1)=2$. Since $1\not\equiv i \bmod \mathfrak{p}^2$, condition 3 is also satisfied.

7.2 Example 2

$\mathbf{K}=\mathbb{Q}(\sqrt{3})$.

Again, $\mathbf{K}$ is known to satisfy conditions 1 and 2. In this case $\mathcal{O}_{\mathbf{K}}^*=\{\pm 1\}\times\langle\sqrt{3}-2\rangle$. Again we note that $2\mathbb{Z}$ ramifies in $\mathbf{K}$. For the unique prime $\mathfrak{p}\mid 2\mathcal{O}_{\mathbf{K}}$, $|(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^2)^*|=\mathfrak{N}(\mathfrak{p})(\mathfrak{N}(\mathfrak{p})-1)=2$. In $\mathcal{O}_{\mathbf{K}}$, we have

$$\mathfrak{p}^2=2\mathcal{O}_{\mathbf{K}}=(1-\sqrt{3})\mathcal{O}_{\mathbf{K}}\cdot(1+\sqrt{3})\mathcal{O}_{\mathbf{K}}=(1-\sqrt{3})^2\mathcal{O}_{\mathbf{K}},$$

this shows that $2-\sqrt{3}\not\equiv 1 \bmod \mathfrak{p}^2$. Hence we have condition 3.

7.3 Other quadratic examples

Some other examples of fields for which the above argument can be applied are $\mathbb{Q}(\sqrt{d})$ for

$$d\in\{7,11,19,23,27,31,43,47,59,63,67,71,75,83,99\}.$$

These were generated using SAGE and many more can be generated in this fashion.

Table 1 Examples of Galois cubic fields with class number 1 in which $2\mathbb{Z}$ splits

Serial	Defining polynomial of the field	Serial	Defining polynomial of the field
1	$x^3 + x^2 - 10x - 8$	8	$x^3 - x^2 - 94x + 304$
2	$x^3 + x^2 - 14x - 8$	9	$x^3 - x^2 - 102x - 216$
3	$x^3 - 109x - 436$	10	$x^3 - 433x - 3464$
4	$x^3 + x^2 - 42x - 80$	11	$x^3 - x^2 - 146x + 504$
5	$x^3 + x^2 - 52x + 64$	12	$x^3 - x^2 - 152x + 220$
6	$x^3 - x^2 - 74x - 256$	13	$x^3 - x^2 - 166x - 536$
7	$x^3 - x^2 - 76x - 212$	14	$x^3 - x^2 - 200x - 512$

7.4 Example 3 (higher degree)

Let $\mathbf{K}$ be a Galois number field with class number 1. If $2\mathbb{Z}$ splits in $\mathbf{K}$, then for any prime $\mathfrak{p} \mid 2\mathcal{O}_\mathbf{K}$, we know that $2 \notin \mathfrak{p}^2$. This is because the valuation of $2\mathcal{O}_\mathbf{K}$ with respect to $\mathfrak{p}$ is 1. Therefore $1 \not\equiv -1 \bmod \mathfrak{p}^2$. This gives us condition 3 above. Here are some examples of such cubic fields.

7.5 Example 4 (Galois Field K with class number 1, containing $\mathbb{Q}(i)$, in which ramification index of $2\mathbb{Z}$ is 2)

In view of Example 7.1, we assume that $\mathbf{K} \neq \mathbb{Q}(i)$. We have already assumed that the field $\mathbf{K}$ satisfies conditions 1 and 2. We know that $2\mathbb{Z}$ ramifies in $\mathbf{K}$. Let the ramification index be $2e_1$. This implies that

$$2\mathcal{O}_\mathbf{K} = \prod_{\substack{\mathfrak{p} \mid 2\mathcal{O}_\mathbf{K} \\ \mathfrak{p} \subset \mathcal{O}_\mathbf{K} \text{ prime}}} \mathfrak{p}^{2e_1}.$$

If $e_1 = 1$, then we have

$$(1+i)\mathcal{O}_\mathbf{K} = \prod_{\substack{\mathfrak{p} \mid 2\mathcal{O}_\mathbf{K} \\ \mathfrak{p} \subset \mathcal{O}_\mathbf{K} \text{ prime}}} \mathfrak{p}.$$

This implies that $1 \not\equiv -i \bmod \mathfrak{p}^2$ for all $\mathfrak{p} \mid 2\mathcal{O}_\mathbf{K}$. This implies that if $e_1 = 1$, condition 3 is also satisfied.

Table 2 Examples of Galois number fields with class number 1, containing $Q(i)$ in which ramification index of $2\mathbb{Z}$ is 2

Serial	Defining polynomial of the field	Serial	Defining polynomial of the field
1	$x^4 - x^2 + 1$	6	$x^6 + 6x^4 + 9x^2 + 1$
2	$x^4 + 3x^2 + 1$	7	$x^{12} - x^6 + 1$
3	$x^8 - x^6 + x^4 - x^2 + 1$	8	$x^8 - 9x^6 + 19x^4 + 5x^2 + 4$
4	$x^6 + 5x^4 + 6x^2 + 1$	9	$x^{10} + 9x^8 + 28x^6 + 35x^4 + 15x^2 + 1$
5	$x^{20} - x^{18} + x^{16} - x^{14} + x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$	10	$x^4 + 7x^2 + 9$

Acknowledgements The authors would like to thank the Indian Statistical Institute, Bangalore (India), for providing academic support. The authors are grateful to Prof. Sanoli Gun and Prof. Purusottam Rath for their helpful comments on earlier versions of the draft. The second author would like to thank the National Board for Higher Mathematics (India) for financial support. The third author would like to thank the Indian Institute of Science Education and Research Thirvananthapuram (India) and the DST INSPIRE Faculty Award Program (India) for financial support. Finally, all the authors would like to thank the referee for his/her valuable comments and suggestions on this paper.

Author Contributions The details of the theorems and proofs in the submitted paper are a result of collaborative discussions among all the authors. The manuscript was also jointly prepared by all the authors.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Cox, D.: Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, Volume 116 of Pure and Applied Mathematics,: A Wiley Series of Texts. Wiley and Sons, New Jersey (1989)
2. Davenport, H.: Multiplicative Number Theory, Volume 74 of Graduate Texts in Mathematics. Springer, New York (2013)
3. Fouvry, É., Klüners, J.: Cohen-Lenstra Heuristics of Quadratic Number Fields. Lecture Notes in Computational Science, vol. 4076, pp. 40–55. Springer, Berlin (2006)
4. Fouvry, É., Klüners, J.: On the 4-rank of class groups of quadratic number fields. Invent. Math. **167**(3), 455–513 (2007)
5. Garcia, S.R., Lee, E.S.: Unconditional explicit Mertens' theorems for number fields and Dedekind zeta residue bounds. Ramanujan J. **57**(3), 1169–1191 (2022)
6. Goldstein, L.J.: A generalization of the Siegel-Walfisz theorem. Trans. Am. Math. Soc. **149**, 417–429 (1970)
7. Heath-Brown, D.R.: The size of Selmer groups for the congruent number problem. Invent. Math. **111**, 171–195 (1993)
8. Heath-Brown, D.R.: The size of Selmer groups for the congruent number problem II. Invent. Math. **118**, 331–370 (1994)
9. Heilbronn, H.: On the averages of some arithmetical functions of two variables. Mathematika **5**(9), 1–7 (1958)

10. Janusz, G.: Algebraic Number Fields, Volume 7 of Advances in the Mathematical Sciences Issue 7 of Graduate Studies in Mathematics. American Mathematical Society, Providence (1996)
11. Lagarias, J.C., Odlyzko, A.M.: Effective versions of the Chebotarev density theorem algebraic number fields. In: Frolich, A. (ed.) Proceedings of the 1975 Durham Symposium. Academic Press, London (1977)
12. Lang, S.: Algebraic Number Theory, Volume 110 of Graduate Texts in Mathematics, 2nd ed Springer, New York (1994)
13. Lemmermeyer, F.: The ambiguous class number formula revisited. J. Ramanujan Math. **28**(4), 415–421 (2013)
14. Neukirch, J.: Algebraic Number Theory. Springer, Berlin (1999)
15. Ram Murty, M.: Sieving using Dirichlet series. In: Adhikari, S.D., Katre, S.A., Ramakrishnan, B. (eds.) Current Trends in Number Theory, pp. 111–124. Hindustan Book Agency, New Delhi (2002)
16. Shiu, P.: A Brun-Titchmarsh theorem for multiplicative functions. J. Reine Angew. Math. **313**, 161–170 (1980)
17. Smith, A.: The Distribution of ℓ^{infty}-Selmer groups in Degree ℓ Twist Families I, arxiv:2207.05674v2 [math.NT] (8 Feb 2023)
18. Smith, A.: The Distribution of ℓ^{infty}-Selmer groups in Degree ℓ Twist Families II, arxiv:2207.05143v2 [math.NT] (8 Feb 2023)
19. Smith, H.: The monogeneity of radical extensions. Acta Arith. **198**(3), 313–327 (2021)
20. Swinnerton-Dyer, H.P.F.: A Brief Guide to Algebraic Number Theory. Cambridge University Press, Cambridge (2001)
21. Wilson, R.J.: The large sieve in algebraic number fields. Mathematika **16**, 189–204 (1969)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.