Universiteit Leiden
The Netherlands

**Diophantine equations in positive characteristic**
Koymans, P.H.

**Citation**
Koymans, P. H. (2019, June 19). *Diophantine equations in positive characteristic*. Retrieved from https://hdl.handle.net/1887/74294

Version: Not Applicable (or Unknown)
License: [Leiden University Non-exclusive license]
Downloaded from: [https://hdl.handle.net/1887/74294](https://hdl.handle.net/1887/74294)

**Note:** To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

Leiden University Repository

The handle http://hdl.handle.net/1887/74294 holds various files of this Leiden University dissertation.

**Author**: Koymans, P.H.
**Title**: Diophantine equations in positive characteristic
**Issue Date**: 2019-06-19

# Chapter 6

# Joint distribution of spins

*Joint work with Djordjo Milovic*

**Abstract**

We answer a question of Iwaniec, Friedlander, Mazur and Rubin [24] on the joint distribution of spin symbols. As an application we give a negative answer to a conjecture of Cohn and Lagarias on the existence of governing fields for the 16-rank of class groups under the assumption of a short character sum conjecture.

## 6.1 Introduction

One of the most fundamental and most prevalent objects in number theory are extensions of number fields; they arise naturally as fields of definitions of solutions to polynomial equations. Many interesting phenomena are encoded in the splitting of prime ideals in extensions. For instance, if $p$ and $q$ are distinct prime numbers congruent to 1 modulo 4, the statement that $p$ splits in $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ if and only if $q$ splits in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is nothing other than the law of quadratic reciprocity, a common ancestor to much of modern number theory.

Let $K$ be a number field, $\mathfrak{p}$ a prime ideal in its ring of integers $\mathcal{O}_K$, and $\alpha$ an element of the algebraic closure $\overline{K}$. Suppose we were to ask, as we vary $\mathfrak{p}$, how often $\mathfrak{p}$ splits completely in the extension $K(\alpha)/K$. If $\alpha$ is fixed as $\mathfrak{p}$ varies over all prime ideals in $\mathcal{O}_K$, a satisfactory answer is provided by the Chebotarev Density Theorem, which is grounded in the theory of $L$-functions and their zero-free regions. The Chebotarev Density Theorem, however, often cannot provide an answer if $\alpha$ varies along with $\mathfrak{p}$ in some prescribed manner. The purpose of this chapter is to fill this gap for quadratic extensions in a natural setting that arises in many applications. This setting, which we now describe, is inspired by the work of Friedlander, Iwaniec, Mazur, and Rubin [24] and is amenable to sieve theory involving sums of type I and type II, as opposed to the theory of $L$-functions.

Let $K/\mathbb{Q}$ be a Galois extension of degree $n$. Unlike in [24], we do *not* impose the very restrictive condition that $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic. For the moment, let us restrict to the setting where $K$ is totally real and where every totally positive unit in $\mathcal{O}_K$ is a square, as in [24]. To each non-trivial automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and each odd principal prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, we attach the quantity $\mathrm{spin}(\sigma, \mathfrak{p}) \in \{-1, 0, 1\}$, defined as

$$\mathrm{spin}(\sigma, \mathfrak{p}) = \left(\frac{\pi}{\sigma(\pi)}\right)_{K,2}, \tag{6.1}$$

where $\pi$ is any totally positive generator of $\mathfrak{p}$ and $\left(\frac{\cdot}{\cdot}\right)_{K,2}$ denotes the quadratic residue symbol in $K$. If we let $\alpha^2 = \sigma^{-1}(\pi)$, then $\mathrm{spin}(\sigma, \mathfrak{p})$ governs the splitting of $\mathfrak{p}$ in $K(\alpha)$, i.e., $\mathrm{spin}(\sigma, \mathfrak{p}) = 1$ (resp., $-1$, $0$) if $\mathfrak{p}$ is split (resp., inert, ramified) in $K(\alpha)/K$. In [24], under the assumptions that $\sigma$ generates $\mathrm{Gal}(K/\mathbb{Q})$, that $n \geq 3$, and that the technical Conjecture $C_n$ (see Section 6.2.5) holds true, Friedlander et al. prove that the natural density of $\mathfrak{p}$ that are split (resp., inert) in $K(\sqrt{\alpha})/K$ is $\frac{1}{2}$ (resp., $\frac{1}{2}$), just as would be the case were $\alpha$ not to vary with $\mathfrak{p}$.

More generally, suppose $S$ is a subset of $\mathrm{Gal}(K/\mathbb{Q})$ and consider the *joint spin*

$$s_{\mathfrak{p}} = \prod_{\sigma \in S} \mathrm{spin}(\sigma, \mathfrak{p}),$$

defined for principal prime ideals $\mathfrak{p} = \pi\mathcal{O}_K$. If we let $\alpha^2 = \prod_{\sigma \in S} \sigma^{-1}(\pi)$, then $s_{\mathfrak{p}}$ is equal to 1 (resp., $-1$, 0) if $\mathfrak{p}$ is split (resp., inert, ramified) in $K(\alpha)/K$. If $\sigma^{-1} \in S$ for some $\sigma \in S$, then the factor $\mathrm{spin}(\sigma, \mathfrak{p})\mathrm{spin}(\sigma^{-1}, \mathfrak{p})$ falls under the purview of the usual Chebotarev Density Theorem as suggested in [24, p. 744] and studied precisely by McMeekin [56]. We therefore focus on the case that $\sigma \notin S$ whenever $\sigma^{-1} \in S$ and prove the following equidistribution theorem concerning the joint spin $s_{\mathfrak{p}}$, defined in full generality, also for totally complex fields, in Section 6.2.3.

**Theorem 6.1.1.** *Let $K/\mathbb{Q}$ be a Galois extension of degree $n$. If $K$ is totally real, we further assume that every totally positive unit in $\mathcal{O}_K$ is a square. Suppose that $S$ is a non-empty subset of* $\mathrm{Gal}(K/\mathbb{Q})$ *such that $\sigma \in S$ implies $\sigma^{-1} \notin S$. Foe each non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, define $s_{\mathfrak{a}}$ as in (6.6). Assume Conjecture $C_{|S|n}$ holds true with $\delta = \delta(|S|n) > 0$ (see Section 6.2.5). Let $\epsilon > 0$ be a real number. Then for all $X \geq 2$, we have*

$$\sum_{\substack{\mathrm{N}(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ prime}}} s_{\mathfrak{p}} \ll X^{1 - \frac{\delta}{54|S|^2 n(12n+1)} + \epsilon},$$

*where the implied constant depends only on $\epsilon$ and $K$.*

It may be possible to weaken our condition on $S$ and instead require only that there exists $\sigma \in S$ with $\sigma^{-1} \notin S$.

The main theorem in [24] is the special case of Theorem 6.1.1 where $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$, $n \geq 3$, and $S = \{\sigma\}$. After establishing their equidistribution result, Friedlander et al. [24, p. 744] raise the question of the joint distribution of spins, and in particular the case of $\mathrm{spin}(\sigma, \mathfrak{p})$ and $\mathrm{spin}(\sigma^2, \mathfrak{p})$ where again $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$, but $S = \{\sigma, \sigma^2\}$ and $n \geq 5$. The following corollary of Theorem 6.1.1 applied to the set $S = \{\sigma, \sigma^2\}$ answers their question.

**Theorem 6.1.2.** *Let $K/\mathbb{Q}$ be a totally real Galois extension of degree $n$ such that every totally positive unit in $\mathcal{O}_K$ is a square. Suppose that $S = \{\sigma_1, \ldots, \sigma_t\}$ is a non-empty subset of $\mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma \in S$ implies $\sigma^{-1} \notin S$. Assume Conjecture $C_{tn}$ holds true (see Section 6.2.5). Let $= (e_1, \ldots, e_t) \in \mathbb{F}_2^t$. Then, as $X \to \infty$, we have*

$$\frac{|\{\mathfrak{p} \textit{ principal prime ideal in } \mathcal{O}_K : \ \mathrm{N}(\mathfrak{p}) \leq X, \ \mathrm{spin}(\sigma_i, \mathfrak{p}) = (-1)^{e_i} \textit{ for } 1 \leq i \leq t\}|}{|\{\mathfrak{p} \textit{ principal prime ideal in } \mathcal{O}_K : \ \mathrm{N}(\mathfrak{p}) \leq X\}|} \sim \frac{1}{2^t}.$$

We expect that Theorem 6.1.1 has several algebraic applications; see for example the original work of Friedlander et al. [24], but also [41], [43], and [58]. Here we give one such application by giving a negative answer to a conjecture of Cohn and Lagarias [11]. Given an integer $k \geq 1$ and a finite abelian group $A$, we define the $2^k$-rank of $A$ as

$$\mathrm{rk}_{2^k} A = \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA.$$

Cohn and Lagarias [11] considered the one-prime-parameter families of quadratic number fields $\{\mathbb{Q}(\sqrt{dp})\}_p$, where $d$ is a fixed integer $\not\equiv 2 \bmod 4$ and $p$ varies over primes such that $dp$ is a fundamental discriminant. Bolstered by ample numerical evidence as well as theoretical examples [11], they conjectured that for every $k \geq 1$ and $d \not\equiv 2 \bmod 4$, there exists a governing field $M_{d,k}$ for the $2^k$-rank of the narrow class group $\mathcal{C}\ell(\mathbb{Q}(\sqrt{dp}))$ of $\mathbb{Q}(\sqrt{dp})$, i.e., there exists a finite normal extension $M_{d,k}/\mathbb{Q}$ and a class function

$$\phi_{d,k} : \ \mathrm{Gal}(M_{d,k}/\mathbb{Q}) \to \mathbb{Z}_{\geq 0}$$

such that

$$\phi_{d,k}(\mathrm{Art}_{M_{d,k}/\mathbb{Q}}(p)) = \mathrm{rk}_{2^k}\mathcal{C}\ell(\mathbb{Q}(\sqrt{dp})), \tag{6.2}$$

where $\mathrm{Art}_{M_{d,k}/\mathbb{Q}}(p)$ is the Artin conjugacy class of $p$ in $\mathrm{Gal}(M_{d,k}/\mathbb{Q})$. This conjecture was proven for all $k \leq 3$ by Stevenhagen [70], but no governing field has been found for any value of $d$ if $k \geq 4$. Interestingly enough, Smith [69] recently introduced the notion of relative governing fields and used them to deal with distributional questions for $\mathcal{C}\ell(K)[2^\infty]$ for imaginary quadratic fields $K$. Our next theorem, which we will prove in Section 6.5, is a relatively straightforward consequence of Theorem 6.1.1.

**Theorem 6.1.3.** *Assume conjecture $C_n$ for all $n$. Then there is no governing field for the 16-rank of $\mathbb{Q}(\sqrt{-4p})$; in other words, there does not exist a field $M_{-4,4}$ and class function $\phi_{-4,4}$ satisfying (6.2).*

## Acknowledgments

The authors are very grateful to Carlo Pagano for useful discussions. We would also like to thank Peter Sarnak for making us aware of the useful reference [4].

## 6.2 Prerequisites

Here we collect certain facts about quadratic residue symbols and unit groups in number fields that are necessary to give a rigorous definition of spins of ideals and that are useful in our subsequent arguments.

Throughout this section, let $K$ be a number field which is Galois of degree $n$ over $\mathbb{Q}$. Then either $K$ is totally real, as in [24], or $K$ is totally complex, in which case $n$ is even. An element $\alpha \in K$ is called *totally positive* if $\iota(\alpha) > 0$ for all real embeddings $\iota : K \hookrightarrow \mathbb{R}$; if this is the case, we will write $\alpha \succ 0$. If $K$ is totally complex, there are no real embeddings of $K$ into $\mathbb{R}$, and so $\alpha \succ 0$ for every $\alpha \in K$ vacuously. Let $\mathcal{O}_K$ denote the ring of integers of $K$. If $K$ is totally real, we assume that

$$(\mathcal{O}_K^\times)^2 = \left\{u^2 : u \in \mathcal{O}_K^\times\right\} = \left\{u \in \mathcal{O}_K^\times : u \succ 0\right\} = (\mathcal{O}_K^\times)_+, \tag{6.3}$$

where the first and last equalities are definitions and the middle equality is the assumption. This assumption, present in [24], implies that the narrow and the ordinary class groups of $K$ coincide, and hence that every non-zero principal ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written as $\mathfrak{a} = \alpha\mathcal{O}_K$ for some $\alpha \succ 0$. If $K$ is totally complex, then the narrow and the ordinary class groups of $K$ coincide vacuously. In either case, we will let $\mathcal{C}\ell = \mathcal{C}\ell(K)$ and $h = h(K)$ denote the (narrow) class group and the (narrow) class number of $K$.

### 6.2.1 Quadratic residue symbols and quadratic reciprocity

We define the quadratic residue symbol in $K$ in the standard way. That is, given an odd prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ (i.e., a prime ideal having odd absolute norm), and an element $\alpha \in \mathcal{O}_K$, define $\left(\frac{\alpha}{\mathfrak{p}}\right)_{K,2}$ as the unique element in $\{-1, 0, 1\}$ such that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{K,2} \equiv \alpha^{\frac{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})-1}{2}} \bmod \mathfrak{p}.$$

Given an odd ideal $\mathfrak{b}$ of $\mathcal{O}_K$ with prime ideal factorization $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$, define

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_{K,2} = \prod_{\mathfrak{p}} \left(\frac{\alpha}{\mathfrak{p}}\right)_{K,2}^{e_{\mathfrak{p}}}.$$

Finally, given an element $\beta \in \mathcal{O}_K$, let $(\beta)$ denote the principal ideal in $\mathcal{O}_K$ generated by $\beta$. We say that $\beta$ is odd if $(\beta)$ is odd and we define

$$\left(\frac{\alpha}{\beta}\right)_{K,2} = \left(\frac{\alpha}{(\beta)}\right)_{K,2}.$$

We will suppress the subscripts $K, 2$ when there is no risk of ambiguity. Although [24] focuses on a special type of totally real Galois number fields, the version of quadratic reciprocity stated in [24, Section 3] holds and was proved for a general number field. We recall it here. For a place $v$ of $K$, finite or infinite, let $K_v$ denote the completion of $K$ with respect to $v$. Let $(\cdot,\cdot)_v$ denote the Hilbert symbol at $v$, i.e., given $\alpha,\beta\in K$, we let $(\alpha,\beta)_v\in\{-1,1\}$ with $(\alpha,\beta)_v=1$ if and only if there exists $(x,y,z)\in K_v^3\setminus\{(0,0,0)\}$ such that $x^2-\alpha y^2-\beta z^2=0$. As in [24, Section 3], define

$$\mu_2(\alpha,\beta)=\prod_{v|2}(\alpha,\beta)_v \quad \text{and} \quad \mu_\infty(\alpha,\beta)=\prod_{v|\infty}(\alpha,\beta)_v.$$

The following lemma is a consequence of the Hilbert reciprocity law and local considerations at places above 2; see [24, Lemma 2.1, Proposition 2.2, and Lemma 2.3].

**Lemma 6.2.1.** *Let $\alpha,\beta\in\mathcal{O}_K$ with $\beta$ odd. Then $\mu_\infty(\alpha,\beta)\left(\frac{\alpha}{\beta}\right)$ depends only on the congruence class of $\beta$ modulo $8\alpha$. Moreover, if $\alpha$ is also odd, then*

$$\left(\frac{\alpha}{\beta}\right)=\mu_2(\alpha,\beta)\mu_\infty(\alpha,\beta)\left(\frac{\beta}{\alpha}\right).$$

*The factor $\mu_2(\alpha,\beta)$ depends only on the congruence classes of $\alpha$ and $\beta$ modulo 8.*

We remark that if $K$ is totally complex, then $(\alpha,\beta)_\infty=1$ for all $\alpha,\beta\in K$. Also, if $K$ is a totally real Galois number field and $\beta\in K$ is totally positive, then again $(\alpha,\beta)_\infty=1$ for all $\alpha\in K$.

### 6.2.2 Class group representatives

As in [24, p. 707], we define a set of ideals $\mathcal{C}\ell$ and an ideal $\mathfrak{f}$ of $\mathcal{O}_K$ as follows. Let $C_i$, $1\le i\le h$, denote the $h$ ideal classes. For each $i\in\{1,\dots,h\}$, we choose two distinct odd ideals belonging to $C_i$, say $\mathfrak{A}_i$ and $\mathfrak{B}_i$, so as to ensure that, upon setting

$$\mathcal{C}\ell_a=\{\mathfrak{A}_1,\dots,\mathfrak{A}_h\},\quad \mathcal{C}\ell_b=\{\mathfrak{B}_1,\dots,\mathfrak{B}_h\},\quad \mathcal{C}\ell=\mathcal{C}\ell_a\cup\mathcal{C}\ell_b,$$

and

$$\mathfrak{f}=\prod_{\mathfrak{c}\in\mathcal{C}\ell}\mathfrak{c}=\prod_{i=1}^{h}\mathfrak{A}_i\mathfrak{B}_i,$$

the norm

$$f=\mathrm{N}(\mathfrak{f})$$

is squarefree. We define

$$F:=2^{2h+3}fD_K, \tag{6.4}$$

where $D_K$ is the discriminant of $K$.

### 6.2.3 Definition of joint spin

We define a sequence $\{s_\mathfrak{a}\}_\mathfrak{a}$ of complex numbers indexed by non-zero ideals $\mathfrak{a}\subset\mathcal{O}_K$ as follows. Let $S$ be a non-empty subset of $\mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma\notin S$ whenever $\sigma^{-1}\in S$.

We define $r(\mathfrak{a})$ to be the indicator function of an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ to be odd and principal, i.e.,

$$r(\mathfrak{a}) = \begin{cases} 1 & \text{if there exists an odd } \alpha \in \mathcal{O}_K \text{ such that } \mathfrak{a} = \alpha\mathcal{O}_K \\ 0 & \text{otherwise.} \end{cases}$$

Define $r_+(\alpha)$ to be the indicator function of an element $\alpha \in K$ to be totally positive, i.e.,

$$r_+(\alpha) = \begin{cases} 1 & \text{if } \alpha \succ 0 \\ 0 & \text{otherwise.} \end{cases}$$

Note that if $K$ is a totally complex number field, then vacuously $r_+(\alpha) = 1$ for all $\alpha$ in $K$. If $\alpha \in K$ is odd and $r_+(\alpha) = 1$, then we define

$$\operatorname{spin}(\sigma, \alpha) = \left(\frac{\alpha}{\sigma(\alpha)}\right).$$

Fix a decomposition $\mathcal{O}_K^\times = T_K \times V_K$, where $T_K \subset \mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$ of finite order and $V_K \subset \mathcal{O}_K^\times$ is a free abelian group of rank $r_K$ (i.e., $r_K = n - 1$ if $K$ is totally real and $r_K = \frac{n}{2} - 1$ if $K$ is totally complex). With $F$ as in (6.4), suppose that

$$\psi : (\mathcal{O}_K/F\mathcal{O}_K)^\times \to \mathbb{C} \tag{6.5}$$

is a map such that $\psi(\alpha \bmod F) = \psi(\alpha u^2 \bmod F)$ for all $\alpha \in \mathcal{O}_K$ coprime to $F$ and all $u \in \mathcal{O}_K^\times$. We define

$$s_\mathfrak{a} = r(\mathfrak{a}) \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} r_+(tv\alpha)\psi(tv\alpha \bmod F) \prod_{\sigma \in S} \operatorname{spin}(\sigma, tv\alpha), \tag{6.6}$$

where $\alpha$ is any generator of the ideal $\mathfrak{a}$ satisfying $r(\mathfrak{a}) = 1$. The averaging over $V_K/V_K^2$ makes the *spin* $s_\mathfrak{a}$ a well-defined function of $\mathfrak{a}$ since, for any unit $u \in \mathcal{O}_K^\times$, any totally positive $\alpha \in \mathcal{O}_K$ of odd absolute norm, and any $\sigma \in S$, we have

$$\operatorname{spin}(\sigma, u^2\alpha) = \left(\frac{u^2\alpha}{\sigma(u^2\alpha)}\right) = \left(\frac{u^2\alpha}{\sigma(\alpha)}\right) = \left(\frac{\alpha}{\sigma(\alpha)}\right) = \operatorname{spin}(\sigma, \alpha).$$

If $K$ is a totally real (in which case we assume that $K$ satisfies (6.3)), then, for an ideal $\mathfrak{a} = \alpha\mathcal{O}_K$, there is one and only one choice of $t \in T_K$ and $v \in V_K/V_K^2$ such that $r_+(tv\alpha) = 1$. Hence in this case

$$s_\mathfrak{a} = r(\mathfrak{a})\psi(\alpha \bmod F) \prod_{\sigma \in S} \operatorname{spin}(\sigma, \alpha),$$

where $\alpha$ is any totally positive generator of $\mathfrak{a}$. If in addition $n \geq 3$, $\operatorname{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$, and $S = \{\sigma\}$, then $s_\mathfrak{a}$ coincides with $\operatorname{spin}(\sigma, \mathfrak{a})$ in [24, (3.4), p. 706]. If we take instead $S = \{\sigma, \sigma^2\}$ and assume $n \geq 5$, then the distribution of $s_\mathfrak{a}$ has implications for [24, Problem, p. 744].

If $K$ is totally complex, then vacuously $r_+(tv\alpha) = 1$ for all $t \in T_K$ and $v \in V_K/V_K^2$, so the definition of $s_\mathfrak{a}$ specializes to

$$s_\mathfrak{a} = r(\mathfrak{a}) \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} \psi(tv\alpha \bmod F) \prod_{\sigma \in S} \operatorname{spin}(\sigma, tv\alpha).$$

### 6.2.4 Fundamental domains

We will need a suitable fundamental domain $\mathcal{D}$ for the action of the units on elements in $\mathcal{O}_K$.

In case that $K$ is totally real and satisfies (6.3), we take $\mathcal{D} \subset \mathbb{R}^n_+$ to be the same as in [24, (4.2), p. 713]. We fix a numbering of the $n$ real embeddings $\iota_1, \dots, \iota_n : K \hookrightarrow \mathbb{R}$, and we say that $\alpha \in \mathcal{D}$ if and only if $(\iota_1(\alpha), \dots, \iota_n(\alpha)) \in \mathcal{D}$. Hence every non-zero $\alpha \in \mathcal{D}$ is totally positive. Because of the assumption (6.3), every non-zero principal ideal in $\mathcal{O}_K$ has a totally positive generator, and $\mathcal{D}$ is a fundamental domain for the action of $(\mathcal{O}_K)^\times_+$ on the totally positive elements in $\mathcal{O}_K$, in the sense of [24, Lemma 4.3, p. 715].

In case that $K$ is totally complex, we take $\mathcal{D} \subset \mathbb{R}^n$ to be the same as in [41, Lemma 3.5, p. 10]. In this case, we fix an integral basis $\{\eta_1, \dots, \eta_n\}$ for $\mathcal{O}_K$. For an element $\alpha = a_1\eta_1 + \cdots + a_n\eta_n \in K$ with $a_1, \dots, a_n \in \mathbb{Q}$ we say that $\alpha \in \mathcal{D}$ if and only if $(a_1, \dots, a_n) \in \mathcal{D}$. Every non-zero principal ideal $\mathfrak{a}$ in $\mathcal{O}_K$ has exactly $|T_K|$ generators in $\mathcal{D}$; moreover, if one of the generators of $\mathfrak{a}$ in $\mathcal{D}$ is $\alpha$, say, then the set of generators of $\mathfrak{a}$ in $\mathcal{D}$ is $\{t\alpha : t \in T_K\}$.

The main properties of $\mathcal{D}$ are listed in [24, Lemma 4.3, Lemma 4.4, Corollary 4.5] and [43, Lemma 3.5]. We will often use the property that if an element $\alpha \in \mathcal{D} \cap \mathcal{O}_K$ of norm $\mathrm{N}(\alpha) \leq X$ is written in an integral basis $\eta = \{\eta_1, \dots, \eta_n\}$ as $\alpha = a_1\eta_1 + \cdots + a_n\eta_n \in \mathcal{O}_K$, $a_1, \dots, a_n \in \mathbb{Z}$, then

$$|a_i| \ll X^{\frac{1}{n}}$$

for $1 \leq i \leq n$ where the implied constant depends only on $\eta$.

### 6.2.5 Short character sums

The following is a conjecture on short character sums appearing in [24]. It is essential for the estimates for sums of type I.

**Conjecture 6.2.2.** *For all integers $n \geq 3$ there exists $\delta(n) > 0$ such that for all $\epsilon > 0$ there exists a constant $C(n, \epsilon) > 0$ with the property that for all integers $M$, all integers $Q \geq 3$, all integers $N \leq Q^{\frac{1}{n}}$ and all real non-principal characters $\chi$ of modulus $q \leq Q$ we have*

$$\left| \sum_{M < m \leq M+N} \chi(m) \right| \leq C(n, \epsilon) Q^{\frac{1-\delta(n)}{n} + \epsilon}.$$

Instead of working directly with Conjecture $C_n$, we need a version of it for arithmetic progressions. If $q$ is odd and squarefree, we let $\chi_q$ be the real Dirichlet character $\left(\frac{\cdot}{q}\right)$.

**Corollary 6.2.3.** *Assume Conjecture $C_n$. Then for all integers $n \geq 3$ there exists $\delta(n) > 0$ such that for all $\epsilon > 0$ there exists a constant $C(n, \epsilon) > 0$ with the property that for all odd squarefree integers $q > 1$, all integers $N \leq q^{\frac{1}{n}}$, all integers $M$, $l$ and $k$*

*with $q \nmid k$, we have*

$$\left| \sum_{\substack{M<m\leq M+N \\ n\equiv l \bmod k}} \chi_q(m) \right| \leq C(n,\epsilon) q^{\frac{1-\delta(n)}{n}}.$$

*Proof.* This is an easy generalization of Corollary 7 in [41]. □

### 6.2.6 The sieve

We will prove the following oscillation results for the sequence $\{s_{\mathfrak{a}}\}_{\mathfrak{a}}$. First, for any non-zero ideal $\mathfrak{m} \subset \mathcal{O}_K$ and any $\epsilon > 0$, we have

$$\sum_{\substack{\mathrm{N}(\mathfrak{a})\leq X \\ \mathfrak{a}\equiv 0 \bmod \mathfrak{m}}} s_{\mathfrak{a}} \ll_\epsilon X^{1-\frac{\delta}{54n|S|^2}+\epsilon}, \tag{6.7}$$

where $\delta$ is as in Conjecture $C_n$. Second, for any $\epsilon > 0$, we have

$$\sum_{\mathrm{N}(\mathfrak{a})\leq x} \sum_{\mathrm{N}(\mathfrak{b})\leq y} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}} \ll_\epsilon \left(x^{-\frac{1}{6n}} + y^{-\frac{1}{6n}}\right)(xy)^{1+\epsilon}, \tag{6.8}$$

for any pair of bounded sequences of complex numbers $\{v_{\mathfrak{m}}\}$ and $\{w_{\mathfrak{n}}\}$ indexed by non-zero ideals in $\mathcal{O}_K$. Then [24, Proposition 5.2, p. 722] implies that for any $\epsilon > 0$, we have

$$\sum_{\substack{\mathrm{N}(\mathfrak{p})\leq X \\ \mathfrak{p} \text{ prime ideal}}} s_{\mathfrak{p}} \ll_\epsilon X^{1-\theta+\epsilon},$$

where

$$\theta := \frac{\delta(|S|n)}{54|S|^2 n(12n+1)}.$$

Hence, in order to prove Theorem 6.1.1, it suffices to prove the estimates (6.7) and (6.8). We will deal with (6.7) in Section 6.3 and with (6.8) in Section 6.4.

## 6.3 Linear sums

We first treat the case that $K$ is totally real. Let $\mathfrak{m}$ be an ideal coprime with $F$ and $\sigma(\mathfrak{m})$ for all $\sigma \in S$. Following [24] we will bound

$$A(x) = \sum_{\substack{\mathrm{N}\mathfrak{a}\leq x \\ (\mathfrak{a},F)=1, \mathfrak{m}|\mathfrak{a}}} r(\mathfrak{a}) \psi(\alpha \bmod F) \prod_{\sigma\in S} \mathrm{spin}(\sigma,\alpha), \tag{6.9}$$

where $\alpha$ is any totally positive generator of $\mathfrak{a}$. We pick for each ideal $\mathfrak{a}$ with $r(\mathfrak{a}) = 1$ its unique generator $\alpha$ satisfying $\mathfrak{a} = (\alpha)$ and $\alpha \in \mathcal{D}^*$, where $\mathcal{D}^*$ is the fundamental domain from Friedlander et al. [24]. After splitting (6.9) in residue classes modulo $F$ we obtain

$$A(x) = \sum_{\substack{\rho \bmod F \\ (\rho,F)=1}} \psi(\rho) A(x;\rho) + \partial A(x),$$

where by definition

$$A(x;\rho) := \sum_{\substack{\alpha\in\mathcal{D}, \mathrm{N}\alpha\le x \\ \alpha\equiv\rho \bmod F \\ \alpha\equiv 0 \bmod \mathfrak{m}}} \prod_{\sigma\in S} \mathrm{spin}(\sigma,\alpha). \tag{6.10}$$

The boundary term $\partial A(x)$ can be dealt with using the argument in [24, p. 724], which gives $\partial A(x) \ll x^{1-\frac{1}{n}}$. Here and in the rest of our arguments the implied constant depends only on $K$ unless otherwise indicated. We will now estimate $A(x;\rho)$ for each $\rho \bmod F$, $(\rho, F) = 1$. Let $1, \omega_2, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$ and define

$$\mathbb{M} := \omega_2\mathbb{Z} + \cdots + \omega_n\mathbb{Z}.$$

Then, just as in [24, p. 725], we can decompose $\alpha$ uniquely as

$$\alpha = a + \beta, \qquad \text{with } a \in \mathbb{Z}, \beta \in \mathbb{M}.$$

Hence the summation conditions in (6.10) can be rewritten as

$$a+\beta \in \mathcal{D}, \quad \mathrm{N}(a+\beta) \le x, \quad a+\beta \equiv \rho \bmod F, \quad a+\beta \equiv 0 \bmod \mathfrak{m}. \tag{$*$}$$

From now on we think of $a$ as a variable satisfying $(*)$ while $\beta$ is inactive. We have the following formula

$$\mathrm{spin}(\sigma,\alpha) = \left(\frac{\alpha}{\sigma(\alpha)}\right) = \left(\frac{a+\beta}{a+\sigma(\beta)}\right) = \left(\frac{\beta-\sigma(\beta)}{a+\sigma(\beta)}\right).$$

If $\beta = \sigma(\beta)$ for some $\sigma \in S$ we get no contribution. So from now on we can assume $\beta \ne \sigma(\beta)$ for all $\sigma \in S$. Define $\mathfrak{c}(\sigma,\beta)$ to be the part of the ideal $(\beta - \sigma(\beta))$ coprime to $F$. Then, as explained on [24, p. 726], quadratic reciprocity gives

$$A(x;\rho) = \sum_{\beta\in\mathbb{M}} \pm T(x;\rho,\beta),$$

where $T(x;\rho,\beta)$ is given by

$$\begin{aligned} T(x;\rho,\beta) &:= \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. } (*)}} \prod_{\sigma\in S} \left(\frac{a+\sigma(\beta)}{\mathfrak{c}(\sigma,\beta)}\right) = \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. } (*)}} \prod_{\sigma\in S} \left(\frac{a+\beta}{\mathfrak{c}(\sigma,\beta)}\right) \\ &= \sum_{\substack{a\in\mathbb{Z} \\ a+\beta \text{ sat. } (*)}} \left(\frac{a+\beta}{\prod_{\sigma\in S}\mathfrak{c}(\sigma,\beta)}\right). \end{aligned} \tag{6.11}$$

Define $\mathfrak{c} := \prod_{\sigma \in S} \mathfrak{c}(\sigma, \beta)$ and factor $\mathfrak{c}$ as

$$\mathfrak{c} = \mathfrak{g}\mathfrak{q}, \tag{6.12}$$

where by definition $\mathfrak{g}$ consists of those prime ideals $\mathfrak{p}$ dividing $\mathfrak{c}$ that satisfy one of the following three properties

- $\mathfrak{p}$ has degree greater than one;
- $\mathfrak{p}$ is unramified of degree one and some non-trivial conjugate of $\mathfrak{p}$ also divides $\mathfrak{c}$;
- $\mathfrak{p}$ is unramified of degree one and $\mathfrak{p}^2$ divides $\mathfrak{c}$.

Note that there are no ramified primes dividing $\mathfrak{c}$, since $\mathfrak{c}$ is coprime to the discriminant by construction of $F$. Putting all the remaining prime ideals in $\mathfrak{q}$, we note that $q := \mathrm{N}\mathfrak{q}$ is a squarefree number and $g := \mathrm{N}\mathfrak{g}$ is a squarefull number coprime with $q$. The Chinese Remainder Theorem implies that there exists a rational integer $b$ with $b \equiv \beta \bmod \mathfrak{q}$. We stress that $\mathfrak{c}$, $\mathfrak{g}$, $\mathfrak{q}$, $g$, $q$ and $b$ depend only on $\beta$. Define $g_0$ to be the radical of $g$. Then the quadratic residue symbol $(\alpha/\mathfrak{g})$ is periodic in $\alpha$ modulo $g_0$. Hence the symbol $((a+\beta)/\mathfrak{g})$ as a function of $a$ is periodic of period $g_0$. Splitting the sum (6.11) in residue classes modulo $g_0$ we obtain

$$|T(x; \rho, \beta)| \leq \sum_{a_0 \bmod g_0} \left| \sum_{\substack{a \equiv a_0 \bmod g_0 \\ a+\beta \text{ sat. } (*)}} \left(\frac{a+b}{\mathfrak{q}}\right) \right|. \tag{6.13}$$

Following the argument on [24, p. 728], we see that (6.13) can be written as $n$ incomplete character sums of length $\ll x^{\frac{1}{n}}$ and modulus $q \ll x^{|S|}$. Furthermore, the conditions $(*)$ and $a \equiv a_0 \bmod g_0$ imply that $a$ runs over a certain arithmetic progression of modulus $k$ dividing $g_0 F m$, where $m := \mathrm{N}\mathfrak{m}$. So if $q \nmid k$, Corollary 6.2.3 yields

$$T(x; \rho, \beta) \ll_\epsilon g_0 x^{\frac{1-\delta}{n} + \epsilon} \tag{6.14}$$

with $\delta := \delta(|S| n) > 0$. Since $q \mid k$ implies $q \mid m$, we see that (6.14) holds if $q \nmid m$. Recalling (6.12) we conclude that (6.14) holds unless

$$p \mid \prod_{\sigma \in S} \mathrm{N}(\beta - \sigma(\beta)) \Rightarrow p^2 \mid mF \prod_{\sigma \in S} \mathrm{N}(\beta - \sigma(\beta)). \tag{6.15}$$

Our next goal is to count the number of $\beta \in \mathbb{M}$ satisfying both $(*)$ for some $a \in \mathbb{Z}$ and (6.15). For $\beta$ an algebraic integer of degree $n$, we denote by $\beta^{(1)}, \ldots, \beta^{(n)}$ the conjugates of $\beta$. Now if $\beta$ satisfies $(*)$ for some $a \in \mathbb{Z}$, we have $|\beta^{(i)}| \ll x^{\frac{1}{n}}$. So to achieve our goal, it suffices to estimate the number of $\beta \in \mathbb{M}$ satisfying $|\beta^{(i)}| \leq x^{\frac{1}{n}}$ and (6.15).

To do this, we will need two lemmas. So far we have followed [24] rather closely, but we will have to significantly improve their estimates for the various error terms given on [24, p. 729-733]. One of the most important tasks ahead is to count squarefull norms in a certain $\mathbb{Z}$-submodule of $\mathcal{O}_K$. This problem is solved in [24] by simply counting squarefull norms in the full ring of integers. For our application this loss is unacceptable. In our first lemma we directly count squarefull norms in this submodule, a problem described in [24, p. 729] as potentially "very difficult".

**Lemma 6.3.1.** *Factor $\mathfrak{c}(\sigma, \beta)$ as*

$$\mathfrak{c}(\sigma, \beta) = \mathfrak{g}(\sigma, \beta)\mathfrak{q}(\sigma, \beta)$$

*just as in (6.12). Let $K^\sigma$ be the subfield of $K$ fixed by $\sigma$ and let $\mathcal{O}_{K^\sigma}$ be its ring of integers. Decompose $\mathcal{O}_K$ as*

$$\mathcal{O}_K = \mathcal{O}_{K^\sigma} \oplus \mathbb{M}'.$$

*Let $ord(\sigma)$ be the order of $\sigma$ in $\mathrm{Gal}(K/\mathbb{Q})$. If $g_0(\sigma, \beta)$ is the radical of $\mathrm{N}\mathfrak{g}(\sigma, \beta)$, then we have for all $\epsilon > 0$*

$$|\{\beta \in \mathbb{M}' : |\beta^{(i)}| \leq x^{\frac{1}{n}}, g_0(\sigma, \beta) > Z\}| \ll_\epsilon x^{1-\frac{1}{ord(\sigma)}+\epsilon} Z^{-1+\frac{2}{ord(\sigma)}}.$$

*Proof.* The argument given here is a generalization of [41, p. 17-18]. We start with the simple estimate

$$|\{\beta \in \mathbb{M}' : |\beta^{(i)}| \leq x^{\frac{1}{n}}, g_0(\sigma, \beta) > Z\}| \leq \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} A_{\mathfrak{g}}, \tag{6.16}$$

where

$$A_{\mathfrak{g}} := |\{\beta \in \mathbb{M}' : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \beta - \sigma(\beta) \equiv 0 \bmod \mathfrak{g}\}|.$$

Let $\mathbb{M}''$ be the image of $\mathbb{M}'$ under the map $\beta \mapsto \beta - \sigma(\beta)$ and fix a $\mathbb{Z}$-basis $\eta_1, \ldots, \eta_r$ of $\mathbb{M}''$. We remark that $r = n\left(1 - \frac{1}{\mathrm{ord}(\sigma)}\right)$, which will be important later on. Because $|\beta^{(i)}| \leq x^{\frac{1}{n}}$, we can write $\beta - \sigma(\beta)$ as $\beta - \sigma(\beta) = \sum_{i=1}^r a_i \eta_i$ with $|a_i| \leq C_K x^{\frac{1}{n}}$, where $C_K$ is a constant depending only on $K$. Hence we have

$$A_{\mathfrak{g}} \leq |\Lambda_{\mathfrak{g}} \cap S_x|,$$

where by definition

$$\Lambda_{\mathfrak{g}} := \{\gamma \in \mathbb{M}'' : \gamma \equiv 0 \bmod \mathfrak{g}\}$$
$$S_x := \{\gamma \in \mathbb{M}'' : \gamma = \sum_{i=1}^r a_i \eta_i, |a_i| \leq C_K x^{\frac{1}{n}}\}.$$

Using our fixed $\mathbb{Z}$-basis $\eta_1, \ldots, \eta_r$ we can view $\mathbb{M}''$ as a subset of $\mathbb{R}^r$ via the map $\eta_i \mapsto e_i$, where $e_i$ is the $i$-th standard basis vector. Under this identification $\mathbb{M}''$ becomes $\mathbb{Z}^r$ and $\Lambda_{\mathfrak{g}}$ becomes a sublattice of $\mathbb{Z}^r$. We have

$$A_{\mathfrak{g}} \leq |\Lambda_{\mathfrak{g}} \cap T_x|, \tag{6.17}$$

where

$$T_x := \{(a_1, \ldots, a_r) \in \mathbb{R}^r : |a_i| \leq C_K x^{\frac{1}{n}}\}.$$

Let us now parametrize the boundary of $T_x$. We start off by observing that $T_x = x^{\frac{1}{n}} T_1$, which implies that $\mathrm{Vol}(T_x) = x^{\frac{r}{n}} \mathrm{Vol}(T_1)$. Because $T_1$ is an $r$-dimensional hypercube, we conclude that its boundary $\partial T_1$ can be parametrized by Lipschitz functions with Lipschitz constant $L$ depending only on $K$. Therefore $\partial T_x$ can also be parametrized by Lipschitz functions with Lipschitz constant $x^{\frac{1}{n}} L$. Theorem 5.4 of [79] gives

$$\left| |\Lambda_{\mathfrak{g}} \cap T_x| - \frac{\mathrm{Vol}(T_x)}{\det \Lambda_{\mathfrak{g}}} \right| \ll_L \max_{0 \leq i < r} \frac{x^{\frac{i}{n}}}{\lambda_{\mathfrak{g},1} \cdot \ldots \cdot \lambda_{\mathfrak{g},i}}, \tag{6.18}$$

where $\lambda_{\mathfrak{g},1}, \ldots, \lambda_{\mathfrak{g},r}$ are the successive minima of $\Lambda_{\mathfrak{g}}$. Since $L$ depends only on $K$, it follows that the implied constant in (6.18) depends only on $K$, so we may simply write $\ll$ by our earlier conventions.

Our next goal is to give a lower bound for $\lambda_{\mathfrak{g},1}$. So let $\gamma \in \Lambda_{\mathfrak{g}}$ be non-zero. By definition of $\Lambda_{\mathfrak{g}}$ we have $\mathfrak{g} \mid \gamma$ and hence $g \mid \mathrm{N}\gamma$. Write

$$\gamma = \sum_{i=1}^{r} a_i \eta_i.$$

If $a_1, \ldots, a_r \leq C'_K g^{\frac{1}{n}}$ for a sufficiently small constant $C'_K$, we find that $\mathrm{N}\gamma < g$. But this is impossible, since $g \mid \mathrm{N}\gamma$ and $\mathrm{N}\gamma \neq 0$. So there is an $i$ with $a_i > C'_K g^{\frac{1}{n}}$. If we equip $\mathbb{R}^r$ with the standard Euclidean norm, we conclude that the length of $\gamma$ satisfies $||\gamma|| \gg g^{\frac{1}{n}}$ and hence

$$\lambda_{\mathfrak{g},1} \gg g^{\frac{1}{n}}. \tag{6.19}$$

Minkowski's second theorem and (6.19) imply that

$$\det \Lambda_{\mathfrak{g}} \gg g^{\frac{r}{n}}. \tag{6.20}$$

Combining (6.18), (6.19), (6.20) and $g \leq x$ gives

$$|\Lambda_{\mathfrak{g}} \cap T_x| \ll \frac{x^{\frac{r}{n}}}{g^{\frac{r}{n}}} + \frac{x^{\frac{r-1}{n}}}{g^{\frac{r-1}{n}}} \ll \frac{x^{\frac{r}{n}}}{g^{\frac{r}{n}}}. \tag{6.21}$$

Plugging (6.17) and (6.21) back in (6.16) yields

$$|\{\beta \in \mathbb{M}' : |\beta^{(i)}| \leq x^{\frac{1}{n}}, g_0(\sigma, \beta) > Z\}| \leq \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} A_{\mathfrak{g}} \leq \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} |\Lambda_{\mathfrak{g}} \cap T_x| \ll \sum_{\substack{\mathfrak{g} \\ g_0 > Z}} \frac{x^{\frac{r}{n}}}{g^{\frac{r}{n}}}.$$

If we define $\tau_K(g)$ to be the number of ideals of $K$ of norm $g$, we can bound the last sum as follows

$$\begin{aligned}\sum_{\substack{\mathfrak{g}\\ g_0>Z}} \frac{x^{\frac{r}{n}}}{g^{\frac{r}{n}}} &= x^{\frac{r}{n}} \sum_{\substack{g\leq x\\ g \text{ squarefull}\\ g_0>Z}} \frac{\tau_K(g)}{g^{\frac{r}{n}}} \ll_\epsilon x^{\frac{r}{n}+\epsilon} \sum_{\substack{g\leq x\\ g \text{ squarefull}\\ g_0>Z}} \frac{1}{g^{\frac{r}{n}}}\\ &= x^{\frac{r}{n}+\epsilon} \sum_{\substack{g\leq x\\ g \text{ squarefull}\\ g_0>Z}} g^{\frac{1}{2}-\frac{r}{n}} \frac{1}{g^{\frac{1}{2}}} \leq x^{\frac{r}{n}+\epsilon} Z^{1-\frac{2r}{n}} \sum_{\substack{g\leq x\\ g \text{ squarefull}\\ g_0>Z}} \frac{1}{g^{\frac{1}{2}}}\\ &\leq x^{\frac{r}{n}+\epsilon} Z^{1-\frac{2r}{n}} \sum_{\substack{g\leq x\\ g \text{ squarefull}}} \frac{1}{g^{\frac{1}{2}}} \ll_\epsilon x^{\frac{r}{n}+\epsilon} Z^{1-\frac{2r}{n}}.\end{aligned}$$

Recalling that $r = n\left(1 - \frac{1}{\operatorname{ord}(\sigma)}\right)$ completes the proof of Lemma 6.3.1. □

**Lemma 6.3.2.** *Let $\sigma, \tau \in S$ be distinct. Recall that*

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{M}.$$

*Fix an integral basis $\omega_2, \ldots, \omega_n$ of $\mathbb{M}$ and define the polynomials $f_1, f_2 \in \mathbb{Z}[x_2, \ldots, x_n]$ by*

$$f_1(x_2, \ldots, x_n) = \mathrm{N}\left(\sum_{i=2}^n x_i(\sigma(\omega_i) - \omega_i)\right)$$
$$f_2(x_2, \ldots, x_n) = \mathrm{N}\left(\sum_{i=2}^n x_i(\tau(\omega_i) - \omega_i)\right).$$

*For $\beta \in \mathbb{M}$ with $\beta = \sum_{i=2}^n a_i\omega_i$ we define $f_1(\beta) := f_1(a_2, \ldots, a_n) = \mathrm{N}(\sigma(\beta) - \beta)$ and similarly for $f_2(\beta)$. Then*

$$|\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \gcd(f_1(\beta), f_2(\beta)) > Z\}| \ll_\epsilon x^{\frac{n-1}{n}+\epsilon} Z^{-\frac{1}{18}} + x^{\frac{n-2}{n}} + Z^{\frac{2n-4}{3}}.$$

*Proof.* Let $Y$ be the closed subscheme of $\mathbb{A}^{n-1}_{\mathbb{Z}}$ defined by $f_1 = f_2 = 0$. We claim that $Y$ has codimension 2, i.e. $f_1$ and $f_2$ are relatively prime polynomials. Suppose not. Note that $f_1$ and $f_2$ factor in $K[x_2, \ldots, x_n]$ as

$$f_1(x_2, \ldots, x_n) = \prod_{\sigma' \in \mathrm{Gal}(K/\mathbb{Q})} \left(\sum_{i=2}^n x_i(\sigma'\sigma(\omega_i) - \sigma'(\omega_i))\right)$$
$$f_2(x_2, \ldots, x_n) = \prod_{\tau' \in \mathrm{Gal}(K/\mathbb{Q})} \left(\sum_{i=2}^n x_i(\tau'\tau(\omega_i) - \tau'(\omega_i))\right).$$

Hence if $f_1$ and $f_2$ are not relatively prime, there are $\sigma', \tau' \in \mathrm{Gal}(K/\mathbb{Q})$ and $\kappa \in K^*$ such that

$$\sum_{i=2}^n x_i(\sigma'\sigma(\omega_i) - \sigma'(\omega_i)) = \kappa \sum_{i=2}^n x_i(\tau'\tau(\omega_i) - \tau'(\omega_i))$$

for all $x_2, \dots, x_n \in \mathbb{Z}$. Put $\beta = \sum_{i=2}^n x_i\omega_i$. Then we can rewrite this as

$$\sigma'\sigma(\beta) - \sigma'(\beta) = \kappa(\tau'\tau(\beta) - \tau'(\beta)) \tag{6.22}$$

for all $\beta \in \mathbb{M}$. But this implies that (6.22) holds for all $\beta \in K$. Now we apply the Artin-Dedekind Lemma, which gives a contradiction in all cases due to our assumptions $\sigma, \tau \in S$ and $\sigma \neq \tau$.

Having established our claim, we are in position to apply Theorem 3.3 of [4]. We embed $\mathbb{M}$ in $\mathbb{R}^{n-1}$ by sending $\omega_i$ to $e_i$, the $i$-th standard basis vector. Note that the image under this embedding is $\mathbb{Z}^{n-1}$. Write $\beta = \sum_{i=2}^n a_i\omega_i$. Since $|\beta^{(i)}| \leq x^{\frac{1}{n}}$, it follows that $|a_i| \leq C_K x^{\frac{1}{n}}$ for some constant $C_K$ depending only on $K$. Let $B$ be the compact region in $\mathbb{R}^{n-1}$ given by $B := \{(a_2, \dots, a_n) : |a_i| \leq C_K\}$. Theorem 3.3 of [4] with our $B$, $Y$ and $r = x^{\frac{1}{n}}$ gives

$$|\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, p \mid \gcd(f_1(\beta), f_2(\beta)), p > M\}| \ll \frac{x^{\frac{n-1}{n}}}{M \log M} + x^{\frac{n-2}{n}}, \tag{6.23}$$

where $M$ is any positive real number. Factor

$$f_1(\beta) := g_1q_1, \quad (g_1, q_1) = 1, \quad g_1 \text{ squarefull}, \quad q_1 \text{ squarefree}$$
$$f_2(\beta) := g_2q_2, \quad (g_2, q_2) = 1, \quad g_2 \text{ squarefull}, \quad q_2 \text{ squarefree}.$$

By Lemma 6.3.1 we conclude that for all $A > 0$ and $\epsilon > 0$

$$|\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, g_1 > A\}| \ll_\epsilon x^{\frac{n-1}{n}+\epsilon} A^{-\frac{1}{2}+\frac{1}{\mathrm{ord}(\sigma)}}.$$

With the same argument applied to $\tau$ we obtain

$$|\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, g_1 > A \text{ or } g_2 > A\}| \ll_\epsilon x^{\frac{n-1}{n}+\epsilon} A^{-\frac{1}{2}+\frac{1}{\mathrm{ord}(\sigma)}} + x^{\frac{n-1}{n}+\epsilon} A^{-\frac{1}{2}+\frac{1}{\mathrm{ord}(\tau)}}. \tag{6.24}$$

We discard those $\beta$ that satisfy (6.23) or (6.24). From (6.24) we deduce that the remaining $\beta$ certainly satisfy $\gcd(q_1, q_2) > \frac{Z}{A^2}$. Furthermore, by discarding those $\beta$ satisfying (6.23), we see that $\gcd(q_1, q_2)$ has no prime divisors greater than $M$. This implies that $\gcd(q_1, q_2)$ is divisible by a squarefree number between $\frac{Z}{A^2}$ and $\frac{ZM}{A^2}$. So we must still give an upper bound for

$$\left|\left\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, r \mid \gcd(q_1, q_2), \frac{Z}{A^2} < r \leq \frac{ZM}{A^2}\right\}\right|. \tag{6.25}$$

Let $r$ be a squarefree integer and let $\mathfrak{r}_1, \mathfrak{r}_2$ be two ideals of $K$ with norm $r$. Define

$$E_{\mathfrak{r}_1, \mathfrak{r}_2} := \left|\left\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \mathfrak{r}_1 \mid \sigma(\beta) - \beta, \mathfrak{r}_2 \mid \tau(\beta) - \beta\right\}\right|.$$

We will give an upper bound for $E_{\mathfrak{r}_1, \mathfrak{r}_2}$ following [24, p. 731-733]. Write $\beta = \sum_{i=2}^n a_i\omega_i$. Then $|\beta^{(i)}| \leq x^{\frac{1}{n}}$ implies $a_i \ll x^{\frac{1}{n}}$ and

$$\sum_{i=2}^n a_i(\sigma(\omega_i) - \omega_i) \equiv 0 \bmod \mathfrak{r}_1 \tag{6.26}$$

$$\sum_{i=2}^n a_i(\tau(\omega_i) - \omega_i) \equiv 0 \bmod \mathfrak{r}_2. \tag{6.27}$$

We split the coefficients $a_2, \dots, a_n$ according to their residue classes modulo $r$. Suppose that $p \mid r$ and let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be the unique prime ideals of degree one dividing $\mathfrak{r}_1$ and $\mathfrak{r}_2$ respectively. Then we get

$$\sum_{i=2}^{n} a_i(\sigma(\omega_i) - \omega_i) \equiv 0 \bmod \mathfrak{p}_1 \tag{6.28}$$

$$\sum_{i=2}^{n} a_i(\tau'\tau(\omega_i) - \tau'(\omega_i)) \equiv 0 \bmod \mathfrak{p}_1, \tag{6.29}$$

where $\tau'$ satisfies $\tau'^{-1}(\mathfrak{p}_1) = \mathfrak{p}_2$. If we further assume that $\mathfrak{p}_1$ is unramified, we claim that the above two equations are linearly independent over $\mathbb{F}_p$. Indeed, consider the isomorphism

$$\mathcal{O}_K/p \cong \mathbb{F}_p \times \cdots \times \mathbb{F}_p.$$

Note that $\tau'\tau \notin \{\mathrm{id}, \sigma\}$ or $\tau' \notin \{\mathrm{id}, \sigma\}$ due to our assumption that $\sigma$ and $\tau$ are distinct elements of $S$. Let us deal with the case $\tau'\tau \notin \{\mathrm{id}, \sigma\}$, the other case is dealt with similarly. Then there exists $\beta \in \mathcal{O}_K$ such that $\beta \equiv 1 \bmod \mathfrak{p}_1$, $\beta \equiv 1 \bmod \sigma^{-1}(\mathfrak{p}_1)$, $\beta \equiv 1 \bmod \tau'^{-1}(\mathfrak{p}_1)$ and $\beta$ is divisible by all other conjugates of $\mathfrak{p}_1$. By our assumption on $\tau'\tau$ it follows that $\beta \equiv 0 \bmod \tau^{-1}\tau'^{-1}(\mathfrak{p}_1)$. Hence we obtain

$$\sigma(\beta) - \beta \equiv 0 \bmod \mathfrak{p}_1, \quad \tau'\tau(\beta) - \tau'(\beta) \equiv -1 \bmod \mathfrak{p}_1.$$

However, for $\mathfrak{p}_1$ an unramified prime, we know that $\sigma(\beta) - \beta \equiv 0 \bmod \mathfrak{p}_1$ can not happen for all $\beta \in \mathcal{O}_K$, unless $\sigma$ is the identity. This proves our claim.

If we further split the coefficients $a_2, \dots, a_n$ according to their residue classes modulo $p$, our claim implies that there are $p^{n-3}$ solutions $a_2, \dots, a_n$ modulo $p$ satisfying (6.28) and (6.29), provided that $p$ is unramified. For ramified primes we can use the trivial upper bound $p^{n-1}$. Then we deduce from the Chinese Remainder Theorem that there are $\ll r^{n-3}$ solutions $a_2, \dots, a_n$ modulo $r$ satisfying (6.26) and (6.27). This yields

$$E_{\mathfrak{r}_1,\mathfrak{r}_2} \ll r^{n-3} \left( \frac{x^{\frac{1}{n}}}{r} + 1 \right)^{n-1} \ll x^{\frac{n-1}{n}} r^{-2} + r^{n-3}.$$

Therefore we have the following upper bound for (6.25)

$$\begin{aligned} \sum_{\frac{Z}{A^2} < r \leq \frac{ZM}{A^2}} \sum_{\substack{\mathfrak{r}_1,\mathfrak{r}_2 \\ \mathrm{N}\mathfrak{r}_1 = \mathrm{N}\mathfrak{r}_2 = r}} E_{\mathfrak{r}_1,\mathfrak{r}_2} &\ll \sum_{\frac{Z}{A^2} < r \leq \frac{ZM}{A^2}} \sum_{\substack{\mathfrak{r}_1,\mathfrak{r}_2 \\ \mathrm{N}\mathfrak{r}_1 = \mathrm{N}\mathfrak{r}_2 = r}} x^{\frac{n-1}{n}} r^{-2} + r^{n-3} \\ &\ll_\epsilon x^\epsilon \sum_{\frac{Z}{A^2} < r \leq \frac{ZM}{A^2}} x^{\frac{n-1}{n}} r^{-2} + r^{n-3} \\ &\ll_\epsilon x^\epsilon \left( x^{\frac{n-1}{n}} \frac{A^2}{Z} + \left( \frac{ZM}{A^2} \right)^{n-2} \right). \end{aligned}$$

Note that $\sigma \in S$ implies $\mathrm{ord}(\sigma) \geq 3$. Now choose $A = M = Z^{\frac{1}{3}}$ to complete the proof of Lemma 6.3.2. $\square$

With Lemma 6.3.1 and Lemma 6.3.2 in hand we return to estimating the number of $\beta \in \mathbb{M}$ satisfying $|\beta^{(i)}| \leq x^{\frac{1}{n}}$ and (6.15). We choose a $\sigma \in S$ and we will consider it as fixed for the remainder of the proof. Note that any integer $n > 0$ can be factored uniquely as

$$n = q'g'r',$$

where $q'$ is a squarefree integer coprime to $mF$, $g'$ is a squarefull integer coprime to $mF$ and $r'$ is composed entirely of primes from $mF$. This allows us to define $\mathrm{sqf}(n, mF) := q'$. We start by giving an upper bound for

$$\left|\left\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\beta - \sigma(\beta)), mF) \leq Z\right\}\right|.$$

To do this, we need a slight generalization of the argument on [24, p. 729]. Recall that $K^\sigma$ is the subfield of $K$ fixed by $\sigma$ and $\mathcal{O}_{K^\sigma}$ its ring of integers. Decompose $\mathcal{O}_K$ as

$$\mathcal{O}_K = \mathcal{O}_{K^\sigma} \oplus \mathbb{M}'.$$

Then we have

$$\begin{aligned}&\left|\left\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\beta - \sigma(\beta)), mF) \leq Z\right\}\right| \\ &\qquad \ll x^{\frac{1}{\mathrm{ord}(\sigma)} - \frac{1}{n}} \left|\left\{\beta \in \mathbb{M}' : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\beta - \sigma(\beta)), mF) \leq Z\right\}\right|. \end{aligned} \tag{6.30}$$

The map $\mathbb{M}' \to \mathcal{O}_K$ given by $\beta \mapsto \beta - \sigma(\beta)$ is injective. Set $\gamma := \beta - \sigma(\beta)$. Furthermore, the conjugates of $\gamma$ satisfy $|\gamma^{(i)}| \leq 2x^{\frac{1}{n}}$, which gives

$$\begin{aligned}&\left|\left\{\beta \in \mathbb{M}' : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\beta - \sigma(\beta)), mF) \leq Z\right\}\right| \\ &\qquad \leq \left|\left\{\gamma \in \mathcal{O}_K : |\gamma^{(i)}| \leq 2x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\gamma), mF) \leq Z\right\}\right|. \end{aligned} \tag{6.31}$$

Instead of counting algebraic integers $\gamma$, we will count the principal ideals they generate, where each given ideal occurs no more than $\ll (\log x)^n$ times. This yields the bound

$$\begin{aligned}&\left|\left\{\gamma \in \mathcal{O}_K : |\gamma^{(i)}| \leq 2x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\gamma), mF) \leq Z\right\}\right| \\ &\qquad \ll (\log x)^n \left|\{\mathfrak{b} \subseteq \mathcal{O}_K : \mathrm{N}(\mathfrak{b}) \leq 2^n x, \mathrm{sqf}(\mathrm{N}(\mathfrak{b}), mF) \leq Z\}\right|.\end{aligned}$$

We conclude that

$$\left|\left\{\gamma \in \mathcal{O}_K : |\gamma^{(i)}| \leq 2x^{\frac{1}{n}}, \mathrm{sqf}(\mathrm{N}(\gamma), mF) \leq Z\right\}\right| \ll (\log x)^n \sum_{\substack{b \leq 2^n x \\ \mathrm{sqf}(b, mF) \leq Z}} \tau_K(b), \tag{6.32}$$

where we remind the reader that $\tau_K(b)$ denotes the number of ideals in $K$ of norm $b$.

Let us count the number of $b \leq 2^n x$ satisfying $\mathrm{sqf}(b, mF) \leq Z$. We do this by counting the number of possible $g', r' \leq 2^n x$ that can occur in the factorization $b = q'g'r'$. First of all, there are $\ll x^{\frac{1}{2}}$ squarefull integers $g'$ satisfying $g' \leq 2^n x$. To bound the number of $r' \leq 2^n x$, we observe that we may assume $m \leq x$, because otherwise the sum in (6.9) is empty. This implies that the number of integers $r' \leq 2^n x$ that are composed entirely of primes from $mF$ is $\ll_\epsilon x^\epsilon$. Obviously there are at most $Z$ squarefree integers $q'$ coprime to $mF$ satisfying $q' \leq Z$. We conclude that the number of $b \leq 2^n x$ satisfying $\operatorname{sqf}(b, mF) \leq Z$ is $\ll_\epsilon Zx^{\frac{1}{2}+\epsilon}$. Combined with the upper bound $\tau_K(b) \ll_\epsilon x^\epsilon$ we obtain

$$(\log x)^n \sum_{\substack{b \leq 2^n x \\ \operatorname{sqf}(b, mF) \leq Z}} \tau_K(b) \ll_\epsilon Zx^{\frac{1}{2}+\epsilon}. \tag{6.33}$$

Stringing together the inequalities (6.30), (6.31), (6.32) and (6.33) we conclude that

$$\left|\left\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \operatorname{sqf}(\mathrm{N}(\beta - \sigma(\beta)), mF) \leq Z\right\}\right| \ll_\epsilon Zx^{\frac{1}{2}+\frac{1}{\operatorname{ord}(\sigma)}-\frac{1}{n}+\epsilon}. \tag{6.34}$$

Now in order to give an upper bound for the number of $\beta$ satisfying $|\beta^{(i)}| \leq x^{\frac{1}{n}}$ and (6.15), that is

$$p \mid \prod_{\sigma \in S} \mathrm{N}(\beta - \sigma(\beta)) \Rightarrow p^2 \mid mF \prod_{\sigma \in S} \mathrm{N}(\beta - \sigma(\beta)),$$

we start by picking $Z = x^{\frac{1}{3n}}$ and discarding all $\beta$ satisfying (6.34) for the $\sigma \in S$ we fixed earlier. For this $\sigma \in S$ and varying $\tau \in S$ with $\tau \neq \sigma$ we apply Lemma 6.3.2 to obtain

$$|\{\beta \in \mathbb{M} : |\beta^{(i)}| \leq x^{\frac{1}{n}}, \gcd(\mathrm{N}(\beta - \sigma(\beta)), \mathrm{N}(\beta - \tau(\beta))) > x^{\frac{1}{3n|S|}}\}| \ll_\epsilon x^{\frac{n-1}{n}-\frac{1}{54n|S|}+\epsilon}. \tag{6.35}$$

We further discard all $\beta$ satisfying (6.35) for some $\tau \in S$ with $\tau \neq \sigma$. Now it is easily checked that the remaining $\beta$ do not satisfy (6.15). Hence we have completed our task of estimating the number of $\beta$ satisfying $|\beta^{(i)}| \leq x^{\frac{1}{n}}$ and (6.15).

Let $A_0(x;\rho)$ be the contribution to $A(x;\rho)$ of the terms $\alpha = a + \beta$ for which (6.15) does not hold and let $A_\square(x;\rho)$ be the contribution to $A(x;\rho)$ for which (6.15) holds. Then we have the obvious identity

$$A(x;\rho) = A_0(x;\rho) + A_\square(x;\rho).$$

Next we make a further partition

$$A_0(x;\rho) = A_1(x;\rho) + A_2(x;\rho),$$

where the components run over $\alpha = a + \beta$, $\beta \in \mathbb{M}$ with $\beta$ such that

$$\begin{aligned} g_0 &\leq Y \text{ in } A_1(x;\rho) \\ g_0 &> Y \text{ in } A_2(x;\rho). \end{aligned}$$

Here $Y$ is at our disposal and we choose it later. From (6.34) and (6.35) we deduce that

$$A_\square(x;\rho) \ll_\epsilon x^{1-\frac{1}{54n|S|}+\epsilon}.$$

To estimate $A_1(x;\rho)$ we apply 6.14 and sum over all $\beta \in \mathbb{M}$ satisfying $|\beta^{(i)}| \leq x^{\frac{1}{n}}$, ignoring all other restrictions on $\beta$, to obtain

$$A_1(x;\rho) \ll_\epsilon Y x^{1-\frac{\delta}{n}+\epsilon}.$$

We still have to bound $A_2(x;\rho)$. Recall that

$$\mathfrak{c} = \prod_{\sigma \in S} \mathfrak{c}(\sigma, \beta),$$

leading to the factorization $\mathfrak{c} = \mathfrak{g}\mathfrak{q}$ in (6.12). We further recall that $g_0$ is the radical of $N\mathfrak{g}$. Now factor each term $\mathfrak{c}(\sigma, \beta)$ as

$$\mathfrak{c}(\sigma, \beta) = \mathfrak{g}(\sigma, \beta)\mathfrak{q}(\sigma, \beta) \tag{6.36}$$

just as in (6.12). The point of (6.36) is that

$$\mathfrak{g} \mid \prod_{\sigma \in S} \mathfrak{g}(\sigma, \beta) \prod_{\substack{\sigma, \tau \in S \\ \sigma \neq \tau}} \gcd(\mathfrak{c}(\sigma, \beta), \mathfrak{c}(\tau, \beta))$$

and therefore

$$g_0 \mid \prod_{\sigma \in S} g_0(\sigma, \beta) \prod_{\substack{\sigma, \tau \in S \\ \sigma \neq \tau}} \gcd(\mathfrak{c}(\sigma, \beta), \mathfrak{c}(\tau, \beta)).$$

We use Lemma 6.3.1 to discard all $\beta$ satisfying $g_0(\sigma, \beta) > Y^{\frac{1}{|S|^2}}$. Similarly, we use Lemma 6.3.2 to discard all $\beta$ satisfying $\gcd(\mathfrak{c}(\sigma, \beta), \mathfrak{c}(\tau, \beta)) > Y^{\frac{1}{|S|^2}}$. Then the remaining $\beta$ satisfy $g_0 \leq Y$. Furthermore, we have removed

$$\ll_\epsilon x^{\frac{n-1}{n}+\epsilon} Y^{-\frac{1}{18|S|^2}} + x^{\frac{n-2}{n}} + Y^{\frac{2n-4}{3|S|^2}} + x^{\frac{n-1}{n}+\epsilon} Y^{-\frac{1}{3|S|^2}}$$

$\beta$ in total and hence

$$A_2(x;\rho) \ll_\epsilon x^{1+\epsilon} Y^{-\frac{1}{18|S|^2}} + x^{\frac{n-1}{n}} + x^{\frac{1}{n}} Y^{\frac{2n-4}{3|S|^2}} + x^{1+\epsilon} Y^{-\frac{1}{3|S|^2}}.$$

After picking $Y = x^{\frac{\delta}{2n}}$ we conclude that

$$A(x) \ll_\epsilon x^{1-\frac{\delta}{54n|S|^2}+\epsilon}.$$

We will now sketch how to modify this proof for totally complex $K$. We have to bound

$$A(x) = \sum_{\substack{N\mathfrak{a} \leq x \\ (\mathfrak{a}, F)=1, \mathfrak{m} \mid \mathfrak{a}}} r(\mathfrak{a}) \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} \psi(tv\alpha \bmod F) \prod_{\sigma \in S} \mathrm{spin}(\sigma, tv\alpha). \tag{6.37}$$

We use the fundamental domain constructed for totally complex fields form subsection 6.2.4 and we pick for each principal $\mathfrak{a}$ its generator in $\mathcal{D}$. Then equation (6.37) becomes

$$\begin{aligned} A(x) &= \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} \sum_{\substack{\alpha \in \mathcal{D}, \mathrm{N}\alpha \le x \\ \alpha \equiv \rho \bmod F \\ \alpha \equiv 0 \bmod \mathfrak{m}}} \psi(tv\alpha \bmod F) \prod_{\sigma \in S} \mathrm{spin}(\sigma, tv\alpha) \\ &= \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} \sum_{\substack{\alpha \in tv\mathcal{D}, \mathrm{N}\alpha \le x \\ \alpha \equiv \rho \bmod F \\ \alpha \equiv 0 \bmod \mathfrak{m}}} \psi(\alpha \bmod F) \prod_{\sigma \in S} \mathrm{spin}(\sigma, \alpha). \end{aligned}$$

We deal with each sum of the shape

$$\sum_{\substack{\alpha \in tv\mathcal{D}, \mathrm{N}\alpha \le x \\ \alpha \equiv \rho \bmod F \\ \alpha \equiv 0 \bmod \mathfrak{m}}} \psi(\alpha \bmod F) \prod_{\sigma \in S} \mathrm{spin}(\sigma, \alpha) \tag{6.38}$$

exactly in the same way as for real quadratic fields $K$, where it is important to note that the shifted fundamental domain $tv\mathcal{D}$ still has the essential properties we need. Combining our estimate for each sum in equation (6.38), we obtain the desired upper bound for $A(x)$.

## 6.4 Bilinear sums

Let $x, y > 0$ and let $\{v_{\mathfrak{a}}\}_{\mathfrak{a}}$ and $\{w_{\mathfrak{b}}\}_{\mathfrak{b}}$ be two sequences of complex numbers bounded in modulus by 1. Define

$$B(x, y) = \sum_{\mathrm{N}(\mathfrak{a}) \le x} \sum_{\mathrm{N}(\mathfrak{b}) \le y} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}}. \tag{6.39}$$

We wish to prove that for all $\epsilon > 0$, we have

$$B(x, y) \ll_\epsilon \left(x^{-\frac{1}{6n}} + y^{-\frac{1}{6n}}\right) (xy)^{1+\epsilon}, \tag{6.40}$$

where the implied constant is uniform in all choices of sequences $\{v_{\mathfrak{a}}\}_{\mathfrak{a}}$ and $\{w_{\mathfrak{b}}\}_{\mathfrak{b}}$ as above.

We split the sum $B(x, y)$ into $h^2$ sums according to which ideal classes $\mathfrak{a}$ and $\mathfrak{b}$ belong to. In fact, since $s_{\mathfrak{a}\mathfrak{b}}$ vanishes whenever $\mathfrak{a}\mathfrak{b}$ does not belong to the principal class, it suffices to split $B(x, y)$ into $h$ sums

$$B(x, y) = \sum_{i=1}^{h} B_i(x, y), \quad B_i(x, y) = \sum_{\substack{\mathrm{N}(\mathfrak{a}) \le x \\ \mathfrak{a} \in C_i}} \sum_{\substack{\mathrm{N}(\mathfrak{b}) \le y \\ \mathfrak{b} \in C_i^{-1}}} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}}.$$

We will prove the desired estimate for each of the sums $B_i(x, y)$. So fix an index $i \in \{1, \dots, h\}$, let $\mathfrak{A} \in \mathcal{C}\ell_a$ be the ideal belonging to the ideal class $C_i^{-1}$, and let

$\mathfrak{B} \in \mathcal{C}\ell_b$ be the ideal belonging to the ideal class $C_i$. The conditions on $\mathfrak{a}$ and $\mathfrak{b}$ above mean that

$$\mathfrak{a}\mathfrak{A} = (\alpha), \quad \alpha \succ 0$$

and

$$\mathfrak{b}\mathfrak{B} = (\beta), \quad \beta \succ 0.$$

Since $\mathfrak{A} \in C_i^{-1}$ and $\mathfrak{B} \in C_i$, there exists an element $\gamma \in \mathcal{O}_K$ such that

$$\mathfrak{A}\mathfrak{B} = (\gamma), \quad \gamma \succ 0.$$

We are now in a position to use the factorization formula for $\mathrm{spin}(\mathfrak{a}\mathfrak{b})$ appearing in [24, (3.8), p. 708], which in turn leads to a factorization formula for $s_{\mathfrak{a}\mathfrak{b}}$. We note that the formula [24, (3.8), p. 708] also holds in case $K$ is totally complex, with exactly the same proof. We have

$$\mathrm{spin}(\sigma, \alpha\beta/\gamma) = \mathrm{spin}(\sigma, \gamma)\delta(\sigma; \alpha, \beta) \left(\frac{\alpha\gamma}{\sigma(\mathfrak{a}\mathfrak{B})}\right) \left(\frac{\beta\gamma}{\sigma(\mathfrak{b}\mathfrak{A})}\right) \left(\frac{\alpha}{\sigma(\beta)\sigma^{-1}(\beta)}\right), \tag{6.41}$$

where $\delta(\sigma; \alpha, \beta) \in \{\pm 1\}$ is a factor which comes from an application of quadratic reciprocity and which depends only on $\sigma$ and the congruence classes of $\alpha$ and $\beta$ modulo 8.

If $K$ is real quadratic, then we set

$$v'_{\mathfrak{a}} = v_{\mathfrak{a}} \prod_{\sigma \in S} \left(\frac{\alpha\gamma}{\sigma(\mathfrak{a}\mathfrak{B})}\right), \quad w'_{\mathfrak{b}} = w_{\mathfrak{b}} \prod_{\sigma \in S} \left(\frac{\beta\gamma}{\sigma(\mathfrak{b}\mathfrak{A})}\right),$$

and

$$\delta(\alpha, \beta) = \psi(\alpha\beta \bmod F) \prod_{\sigma \in S} \delta(\sigma; \alpha, \beta), \quad s(\gamma) = \prod_{\sigma \in S} \mathrm{spin}(\sigma, \gamma),$$

so that we can rewrite the sum $B_i(x, y)$ as

$$B_i(x, y) = s(\gamma) \sum_{\substack{\alpha \in \mathcal{D} \\ \mathrm{N}(\alpha) \leq x\mathrm{N}(\mathfrak{A}) \\ \alpha \equiv 0 \bmod \mathfrak{A}}} \sum_{\substack{\beta \in \mathcal{D} \\ \mathrm{N}(\beta) \leq y\mathrm{N}(\mathfrak{B}) \\ \beta \equiv 0 \bmod \mathfrak{B}}} \delta(\alpha, \beta) v'_{(\alpha)/\mathfrak{A}} w'_{(\beta)/\mathfrak{B}} \prod_{\sigma \in S} \left(\frac{\alpha}{\sigma(\beta)\sigma^{-1}(\beta)}\right). \tag{6.42}$$

Now set

$$v_\alpha = \mathbf{1}(\alpha \equiv 0 \bmod \mathfrak{A}) \cdot v'_{(\alpha)/\mathfrak{A}}$$

and

$$w_\beta = \mathbf{1}(\beta \equiv 0 \bmod \mathfrak{B}) \cdot w'_{(\beta)/\mathfrak{B}},$$

where $\mathbf{1}(P)$ is the indicator function of a property $P$. Also, for $\alpha, \beta \in \mathcal{O}_K$ with $\beta$ odd, we define

$$\phi(\alpha, \beta) = \prod_{\sigma \in S} \left(\frac{\alpha}{\sigma(\beta)\sigma^{-1}(\beta)}\right).$$

Finally, we further split $B_i(x,y)$ according to the congruence classes of $\alpha$ and $\beta$ modulo $F$, so as to control the factor $\delta(\alpha,\beta)$, which now depends on congruence classes of $\alpha$ and $\beta$ modulo $F$ due to the presence of $\psi(\alpha\beta \bmod F)$. We have

$$B_i(x,y) = s(\gamma) \sum_{\alpha_0\in(\mathcal{O}_K/(F))^\times} \sum_{\beta_0\in(\mathcal{O}_K/(F))^\times} \delta(\alpha_0,\beta_0)B_i(x,y;\alpha_0,\beta_0),$$

where

$$B_i(x,y;\alpha_0,\beta_0) = \sum_{\substack{\alpha\in\mathcal{D}(x\mathrm{N}(\mathfrak{A}))\\ \alpha\equiv\alpha_0 \bmod F}} \sum_{\substack{\beta\in\mathcal{D}(y\mathrm{N}(\mathfrak{B}))\\ \beta\equiv\beta_0 \bmod F}} v_\alpha w_\beta \phi(\alpha,\beta).$$

To prove the bound (6.40), at least in the case that $K$ is totally real, it now suffices to prove, for each $\epsilon > 0$, the bound

$$B_i(x,y;\alpha_0,\beta_0) \ll_\epsilon \left(x^{-\frac{1}{6n}} + y^{-\frac{1}{6n}}\right)(xy)^{1+\epsilon}, \tag{6.43}$$

where the implied constant is uniform in all choices of uniformly bounded sequences of complex numbers $\{v_\alpha\}_\alpha$ and $\{w_\beta\}_\beta$ indexed by elements of $\mathcal{O}_K$. Each of the sums $B_i(x,y;\alpha_0,\beta_0)$ is of the same shape as $B(M,N;\omega,\zeta)$ in Chapter 4; in the notation of Chapter 4, $\mathfrak{f} = (F)$, $\alpha_w$ corresponds to $v_\alpha$, $\beta_z$ corresponds to $w_\beta$, and $\gamma(w,z)$ corresponds to $\phi(\alpha,\beta)$ (unfortunately with the arguments $\alpha$ and $\beta$ flipped). Our desired estimate for $B_i(x,y;\alpha_0,\beta_0)$, and hence also $B(x,y)$, would now follow from Proposition 4.3.6, provided that we can verify properties (P1)-(P3) for the function $\phi(\alpha,\beta)$.

We now verify (P1)-(P3), thereby proving the bound (6.43) and hence also the bound (6.40). Property (P1) follows from the law of quadratic reciprocity, since for odd $\alpha$ and $\beta$ we have

$$\begin{aligned}
\phi(\alpha,\beta) &= \prod_{\sigma\in S}\left(\frac{\alpha}{\sigma(\beta)}\right)\left(\frac{\alpha}{\sigma^{-1}(\beta)}\right) \\
&= \prod_{\sigma\in S}\mu(\sigma;\alpha,\beta)\left(\frac{\sigma(\beta)}{\alpha}\right)\left(\frac{\sigma^{-1}(\beta)}{\alpha}\right) \\
&= \left(\prod_{\sigma\in S}\mu(\sigma;\alpha,\beta)\right)\cdot\prod_{\sigma\in S}\left(\frac{\beta}{\sigma^{-1}(\alpha)}\right)\left(\frac{\beta}{\sigma(\alpha)}\right) \\
&= \left(\prod_{\sigma\in S}\mu(\sigma;\alpha,\beta)\right)\cdot\phi(\beta,\alpha),
\end{aligned}$$

where $\mu(\sigma;\alpha,\beta)$ depends only on $\sigma$ and the congruence classes of $\alpha$ and $\beta$ modulo 8. Property (P2) follows immediately from the multiplicativity of each argument of the quadratic residue symbol $(\cdot/\cdot)$. Finally, for property (P3), since $\sigma^{-1}\notin S$ whenever $\sigma\in S$, we see that

$$\varphi(\beta) = \prod_{\sigma\in S}\sigma(\beta)\sigma^{-1}(\beta)$$

divides $\mathrm{N}(\beta) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\beta)$; thus, the first part of (P3) indeed holds true. It now suffices to prove that

$$\sum_{\xi \bmod \mathrm{N}(\beta)} \left(\frac{\xi}{\varphi(\beta)}\right)$$

vanishes if $|\mathrm{N}(\beta)|$ is not squarefull. The sum above is a multiple of the sum

$$\sum_{\xi \bmod \varphi(\beta)} \left(\frac{\xi}{\varphi(\beta)}\right),$$

which vanishes if the principal ideal generated by $\varphi(\beta)$ is not the square of an ideal. The proof now proceeds as in [24, Lemma 3.1]. Supposing $|\mathrm{N}(\beta)|$ is not squarefull, we take a rational prime $p$ such that $p \mid \mathrm{N}(\beta)$ but $p^2 \nmid \mathrm{N}(\beta)$. This implies that there is a degree-one prime ideal divisor $\mathfrak{p}$ of $\beta$ such that $(\beta) = \mathfrak{p}\mathfrak{c}$ with $\mathfrak{c}$ coprime to $p$, i.e., coprime to all the conjugates of $\mathfrak{p}$. Hence $\varphi(\beta)$ factors as

$$(\varphi(\beta)) = \prod_{\sigma \in S} \sigma(\mathfrak{p})\sigma^{-1}(\mathfrak{p}) \prod_{\sigma \in S} \sigma(\mathfrak{c})\sigma^{-1}(\mathfrak{c}),$$

where the evidently non-square $\prod_{\sigma \in S} \sigma(\mathfrak{p})\sigma^{-1}(\mathfrak{p})$ is coprime to $\prod_{\sigma \in S} \sigma(\mathfrak{c})\sigma^{-1}(\mathfrak{c})$, hence proving that $(\varphi(\beta))$ is not a square. This proves that property (P3) holds true, and then Proposition 4.3.6 implies the estimate (6.43) and hence also (6.40), at least in the case that $K$ is totally real.

If $K$ is totally complex, fix $t \in T_K$ and $v \in V_K/V_K^2$. Then replacing $\alpha$ by $tv\alpha$ in (6.41), we get

$$\begin{aligned}\mathrm{spin}(\sigma, tv\alpha\beta/\gamma) = \mathrm{spin}(\sigma, \gamma)\delta(\sigma; tv\alpha, \beta)& \\ \left(\frac{tv\alpha\gamma}{\sigma(\mathfrak{a}\mathfrak{B})}\right)\left(\frac{\beta\gamma}{\sigma(\mathfrak{b}\mathfrak{A})}\right)&\left(\frac{tv}{\sigma(\beta)\sigma^{-1}(\beta)}\right)\left(\frac{\alpha}{\sigma(\beta)\sigma^{-1}(\beta)}\right),\end{aligned}$$

where now $\delta(\sigma; \alpha, \beta; t, v) = \delta(\sigma; tv\alpha, \beta)\left(\frac{tv}{\sigma(\beta)\sigma^{-1}(\beta)}\right) \in \{\pm 1\}$ depends only on $\sigma$, $t$, $v$, and the congruence classes of $\alpha$ and $\beta$ modulo 8. Then instead of (6.42), we have

$$\begin{aligned}B_i(x,y) = s(\gamma) \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} \sum_{\substack{\alpha \in \mathcal{D} \\ \mathrm{N}(\alpha) \le x\mathrm{N}(\mathfrak{A}) \\ \alpha \equiv 0 \bmod \mathfrak{A}}} \sum_{\substack{\beta \in \mathcal{D} \\ \mathrm{N}(\beta) \le y\mathrm{N}(\mathfrak{B}) \\ \beta \equiv 0 \bmod \mathfrak{B}}} \delta(\alpha, \beta; t, v)& \\ v(t,v)'_{(\alpha)/\mathfrak{A}} w'_{(\beta)/\mathfrak{B}} \prod_{\sigma \in S} \left(\frac{\alpha}{\sigma(\beta)\sigma^{-1}(\beta)}\right),&\end{aligned} \tag{6.44}$$

where now

$$v(t,v)'_{\mathfrak{a}} = v_{\mathfrak{a}} \prod_{\sigma \in S} \left(\frac{tv\alpha\gamma}{\sigma(\mathfrak{a}\mathfrak{B})}\right), \quad w'_{\mathfrak{b}} = w_{\mathfrak{b}} \prod_{\sigma \in S} \left(\frac{\beta\gamma}{\sigma(\mathfrak{b}\mathfrak{A})}\right),$$

and

$$\delta(\alpha, \beta; t, v) = \psi(tv\alpha\beta \bmod F) \prod_{\sigma \in S} \delta(\sigma; \alpha, \beta; t, v), \quad s(\gamma) = \prod_{\sigma \in S} \mathrm{spin}(\sigma, \gamma).$$

The rest of the proof now proceeds identically to the case when $K$ is totally real.

## 6.5 Governing fields

Let $E = \mathbb{Q}(\zeta_8, \sqrt{1+i})$ and let $h(-4p)$ be the class number of $\mathbb{Q}(\sqrt{-4p})$. It is well-known that $E$ is a governing field for the 8-rank of $\mathbb{Q}(\sqrt{-4p})$; in fact 8 divides $h(-4p)$ if and only if $p$ splits completely in $E$. We assume that $K$ is a hypothetical governing field for the 16-rank of $\mathbb{Q}(\sqrt{-4p})$ and derive a contradiction. If $K'$ is a normal field extension of $\mathbb{Q}$ containing $K$, then $K'$ is also a governing field. Therefore we can reduce to the case that $K$ contains $E$. In particular, $K$ is totally complex.

We have $\mathrm{Gal}(E/\mathbb{Q}) \cong D_4$ and we fix an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$ that we call $r$. Let $p$ be a rational prime that splits completely in $E$. Since $E$ is a PID, we can take $\pi$ to be a prime in $\mathcal{O}_E$ above $p$. It follows from Proposition 6.2 of [41], which is based on earlier work of Bruin and Hemenway [7], that there exists an integer $F$ and a function $\psi_0 : (\mathcal{O}_E/F\mathcal{O}_E)^\times \to \mathbb{C}$ such that for all $p$ with $(p, F) = 1$ we have

$$16 \mid h(-4p) \Leftrightarrow \psi_0(\pi \bmod F) \left(\frac{r(\pi)}{\pi}\right)_{E,2} = 1, \tag{6.45}$$

where $\psi_0(\alpha \bmod F) = \psi_0(\alpha u^2 \bmod F)$ for all $\alpha \in \mathcal{O}_K$ coprime to $F$ and all $u \in \mathcal{O}_K^\times$. We take $S$ equal to the inverse image of our fixed automorphism $r$ under the natural surjective map $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(E/\mathbb{Q})$. Then it is easily seen that $\sigma \in S$ implies $\sigma^{-1} \notin S$. If $\mathfrak{p}$ is a principal prime of $K$ with generator $w$ of norm $p$, we have

$$\begin{aligned}\prod_{\sigma \in S} \mathrm{spin}(\sigma, w) = \prod_{\sigma \in S} \left(\frac{w}{\sigma(w)}\right)_{K,2} &= \left(\frac{w}{r(\mathrm{N}_{K/E}(w))}\right)_{K,2} \\ = \psi_1(w \bmod 8) \left(\frac{r(\mathrm{N}_{K/E}(w))}{w}\right)_{K,2} &= \psi_1(w \bmod 8) \left(\frac{r(\mathrm{N}_{K/E}(w))}{\mathrm{N}_{K/E}(w)}\right)_{E,2}.\end{aligned}$$

We are now going to apply Theorem 6.1.1 to the number field $K$, the function

$$\psi(w \bmod F) := \psi_1(w \bmod 8)\psi_0\left(\mathrm{N}_{K/E}(w) \bmod F\right).$$

and $S$ as defined above. Then for a principal prime $\mathfrak{p}$ of $K$ with generator $w$ and norm $p$

$$\begin{aligned} s_{\mathfrak{p}} &= \sum_{t \in T_K} \sum_{v \in V_K/V_K^2} \psi\left(tvw \bmod F\right) \prod_{\sigma \in S} \mathrm{spin}(\sigma, tvw) \\ &= 2|T_K||V_K/V_K^2| \left(\mathbf{1}_{16|h(-p)} - \frac{1}{2}\right), \end{aligned} \tag{6.46}$$

since the equivalence in (6.45) does not depend on the choice of $\pi$. Theorem 6.1.1 shows oscillation of the sum

$$\sum_{\substack{\mathrm{N}(\mathfrak{p}) \le X \\ \mathfrak{p} \text{ principal}}} s_{\mathfrak{p}}.$$

The dominant contribution of this sum comes from prime ideals of degree 1 and for these primes equation (6.46) is valid. But if $K$ were to be a governing field, $s_{\mathfrak{p}}$ has to be constant on unramified prime ideals of degree 1, which is the desired contradiction.