Invent math (2013) 193:697–749
DOI 10.1007/s00222-012-0438-8

# The spin of prime ideals

**J.B. Friedlander · H. Iwaniec · B. Mazur · K. Rubin**

Received: 28 October 2011 / Accepted: 19 October 2012 /
Published online: 17 November 2012


**Abstract** Fixing a nontrivial automorphism of a number field $K$, we associate to ideals in $K$ an invariant (with values in $\{0, \pm 1\}$) which we call the *spin* and for which the associated $L$-function does not possess Euler products. We are nevertheless able, using the techniques of bilinear forms, to handle spin value distribution over primes, obtaining stronger results than the analogous ones which follow from the technology of $L$-functions in its current state. The initial application of our theorem is to the arithmetic statistics of Selmer groups of elliptic curves.

**Mathematics Subject Classification (2010)** Primary 11R44 · Secondary 11G05



J.B. Friedlander (✉)
Department of Mathematics, University of Toronto, Toronto, ON M5S 2E4, Canada
e-mail: frdlndr@math.toronto.edu

H. Iwaniec
Department of Mathematics, Rutgers University, New Brunswick, NJ 08903, USA
e-mail: iwaniec@math.rutgers.edu

B. Mazur
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
e-mail: mazur@math.harvard.edu

K. Rubin
Department of Mathematics, UC Irvine, Irvine, CA 92697, USA
e-mail: krubin@math.uci.edu

## 1 Introduction

A very attractive area where algebraic and analytic number theory meet is in the distribution of prime ideals. Such questions are typically studied by means of $L$-functions, starting with Dirichlet and continued by Dedekind, Hecke, Cebotarev, Artin, and many others. The key feature of such $L$-functions is the Euler product, which enables analytic arguments, particularly analytic continuation, functional equations and zero-free regions to be employed.

Given a number field $K$ and an automorphism $\sigma : K \to K$ we associate to ideals in $K$ an invariant for which the associated $L$-function does not possess Euler products; nevertheless we are able to handle the distribution of this invariant over primes. Actually, we obtain stronger results than the analogous ones which follow from $L$-function theory in its current state. We refer to our symbol as the "spin" of the ideal. The spin occurs most naturally if we confine ourselves to number fields with specific properties. A more thorough discussion of these is given in Sect. 3.

Let $K/\mathbb{Q}$ be a Galois extension of degree $n \geqslant 3$ with cyclic Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. For simplicity, we assume that $K$ is totally real and that the totally positive units are exactly the squares of units. At the end of Sect. 3 we give some examples which show that there is a plentiful supply of fields satisfying these conditions. One convenient feature of such fields is the coincidence of the ideal class groups: class equivalence is the same, whether defined in the narrow or the wide sense. Although we do not require the class number $h$ to be one, we shall assign spins only to principal ideals; for these it can be done most neatly.

For a given element $\sigma$ of $G$ and each odd principal ideal $\mathfrak{a}$ we define its spin by

$$\mathrm{spin}(\sigma, \mathfrak{a}) = \left(\frac{\alpha}{\mathfrak{a}^\sigma}\right), \tag{1.1}$$

where $\mathfrak{a} = (\alpha)$, $\alpha \succ 0$ (that is, $\alpha$ is totally positive) and $(\alpha/\mathfrak{b})$ stands for the quadratic residue symbol in $K$. For simplicity, we assume, apart from the final two sections of the paper, that $\sigma$ is a generator of $G$ and is fixed throughout so that we may denote the spin for brevity as $\mathrm{spin}(\mathfrak{a})$, keeping in mind that the spin depends on the choice of the generator $\sigma$. Note that $\mathrm{spin}(\mathfrak{a}) = \pm 1$ if $(\mathfrak{a}, \mathfrak{a}^\sigma) = 1$ and is zero otherwise.

An essential ingredient in our arguments is a bound for short sums of real Dirichlet characters; see Conjecture $C_n$ in Sect. 9.

**Theorem 1.1** *Let $n \geqslant 3$. Assume Conjecture $C_n$ with exponent $\delta \leqslant 2/n$. We have*

$$\sum_{\substack{\mathfrak{p} \text{ principal} \\ N\mathfrak{p} \leqslant x}} \mathrm{spin}(\mathfrak{p}) \ll x^{1-\nu+\varepsilon}, \tag{1.2}$$

*where* $\mathfrak{p}$ *runs over odd prime ideals and* $\nu = \nu(n) = \frac{\delta}{2n(12n+1)}$. *Here, the implied constant depends on* $\varepsilon$ *and the field* $K$.

It turns out that our Conjecture $C_3$ holds true with exponent $\delta(3) = 1/48$ due to a well-known result of D. Burgess [2]. Hence, the estimate (1.2) is unconditionally true for cubic fields with

$$\nu = \nu(3) = 1/10656. \tag{1.3}$$

The contribution to the sum in (1.2) coming from primes of degree greater than one is negligible and, for unramified primes of degree one, the spin takes the values $\pm 1$. Our theorem implies that, unconditionally for $n = 3$ and, dependent on Conjecture $C_n$ for $n \geqslant 4$, the spin takes these values asymptotically equally often. Hopefully, future progress with short character sums will make (1.2) unconditional for fields of higher degree.

For $n = 2$ the sign change of the spin of principal prime ideals of degree one is quite regular, so our method (for catching primes by bilinear forms techniques) fails (however, see further results on this in the final Sect. 12). In fact, if we restrict the primes to a fixed residue class of modulus $8\Delta$ where $\Delta$ is the field discriminant, then the spin is constant, so for such a restricted sum (1.2) is false. On the other hand, if $n \geqslant 3$ and $\sigma$ is a generator, then the spin turns quite randomly, so (1.2) can be established for sums twisted by many kinds of characters. For example, our arguments work with very little change when the spin is twisted by a Hecke Grössencharakter.

Note that the theorem saves a fixed power of $x$ when summing the prime spins. This is in contrast to the $L$-function theory which, in the absence of something approaching the Riemann Hypothesis, would not permit us to even count these primes with such a degree of accuracy. This observation suggests that the sets of primes of constant spin, although determined by a natural algebraic condition, seem very unlikely to be *Cebotarev classes* (that is, sets of primes distinguished by splitting properties in some fixed finite extension of $K$).

As it happens, there is little extra work involved in proving a more general result showing that cancellation occurs when summing the spin over primes in an arithmetic progression and this is of interest both on its own and for applications. Let $\mathfrak{M}$ be an integral ideal of $K$ with $2 \mid \mathfrak{M}$ and $\mu$ an integer of $K$ with $(\mu, \mathfrak{M}) = 1$. We shall take the progression $\mu (\mathrm{mod}\, \mathfrak{M})$ to be fixed throughout the paper.

**Theorem 1.2** *The bound* (1.2) *still holds when the sum is further restricted to principal prime ideals which have a totally positive generator* $\pi$ *satisfying* $\pi \equiv \mu (\mathrm{mod}\, \mathfrak{M})$.

Our results have implications for the distribution of the Selmer rank of elliptic curves. In fact, the question addressed in this paper first arose in trying to improve the results in [11] on Selmer ranks in families of quadratic twists. Let $E$ for example be the elliptic curve

$$y^2 = x^3 + x^2 - 16x - 29,$$

which has conductor $784 = 2^4 \cdot 7^2$. Let $K$ be the maximal real subfield of the field $\mathbb{Q}(\boldsymbol{\mu}_7)$ of 7-th roots of unity. Then, $K$ is a cyclic extension of $\mathbb{Q}$ of degree 3, and $K = \mathbb{Q}(E[2])$, the field generated by the coordinates of the points of order 2 on $E$.

Suppose $p$ is a rational prime congruent to $\pm 1 \pmod 7$, so $p$ splits into 3 distinct primes in $K$. Let $\mathfrak{p}$ be one of the primes above $p$. If $\mathfrak{p}$ has a totally positive generator that is congruent to $1 \pmod 8$, then the 2-Selmer group $\mathrm{Sel}_2(E^{(p)}/\mathbb{Q})$ of the quadratic twist of $E$ by $p$ has dimension

$$\dim_{\mathbf{F}_2} \mathrm{Sel}_2\big(E^{(p)}/\mathbb{Q}\big) = \begin{cases} 3 & \text{if } \mathrm{spin}(\mathfrak{p}) = 1, \\ 1 & \text{if } \mathrm{spin}(\mathfrak{p}) = -1. \end{cases}$$

The condition that $p$ have a generator congruent to 1 modulo 8 is equivalent to asking that $p$ split completely in the ray class field of $K$ modulo 8. Hence, the set of such $p$ has positive density. Moreover, $K$ has class number 1. Thus, Theorem 1.2 shows that, within that set of twists, the Selmer rank is equal to 1 half of the time and 3 half of the time. As one might expect, this holds more generally; see Sect. 10.

We conclude the introduction with a brief outline of the contents of the paper. In Sect. 2 we recall the law of quadratic reciprocity in the setting of a general number field and some related issues which we need for this work. In Sect. 3 we recall some basic facts about number fields; to some extent these are specialized to the type of fields we are considering. One of the technical problems we encounter is the difficulty in stepping smoothly between ideals and integers. This requires a good understanding of the geometrical shape of a convenient fundamental domain for the action of units on $\mathbb{R}^n$. In Sect. 4 we use the construction of T. Shintani [14] and we establish various properties which are needed for our applications.

Although the quadratic residue symbol has multiplicative properties, the spin does not behave in a purely multiplicative fashion. This feature rules out the possibility of using the techniques of $L$-functions but opens the possibility of using the well-known technique of transforming sums over primes to congruence sums and bilinear forms. In Sect. 5 we show how sums over primes are reduced to these latter shapes in a general context and then, in Sects. 6 and 7 respectively, we produce the required bounds for them. Section 8 quickly pieces together these ingredients to complete the proof of the theorems. In Sect. 9 we present the estimates for character sums which power the whole work. In particular, for cubic fields ($n = 3$), the bound we use was established by Burgess via an appeal to the Riemann Hypothesis for algebraic curves, which in this case have genus six.

In Sect. 10 we prove Theorem 10.1 which relates the spin to Selmer groups and justifies, in greater generality, the claims made for our example. In Sect. 11 we briefly discuss the relationships among the spins associated to different automorphisms and point out a few of the very interesting (to us) problems left open by this work. Then, in the final Sect. 12 we consider prime spins for an involutary automorphism, a problem which requires completely different tools.

## 2 Quadratic residues and reciprocity

We say that an integral ideal $\mathfrak{a}$ is odd if $(\mathfrak{a}, 2) = 1$, and is otherwise even. If $\mathfrak{p}$ is an odd prime ideal and $\alpha$ is an integer in $K$ with $\alpha \not\equiv 0 (\mathrm{mod}\, \mathfrak{p})$, then the quadratic residue symbol $(\alpha/\mathfrak{p})$ is defined by

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \alpha \equiv \xi^2 (\mathrm{mod}\, \mathfrak{p}), \\ -1 & \text{otherwise.} \end{cases}$$

We extend this to all $\alpha \in \mathcal{O}$, the ring of integers of $K$, by setting

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = 0 \quad \text{if } \alpha \equiv 0 (\mathrm{mod}\, \mathfrak{p}).$$

If $\mathfrak{q} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ is the product of odd prime ideals (not necessarily distinct) then

$$\left(\frac{\alpha}{\mathfrak{q}}\right) = \left(\frac{\alpha}{\mathfrak{p}_1}\right) \cdots \left(\frac{\alpha}{\mathfrak{p}_r}\right)$$

gives us a multiplicative extension of the definition. Given an odd ideal $\mathfrak{q}$, the symbol $(\alpha/\mathfrak{q})$ is periodic in $\alpha (\mathrm{mod}\, \mathfrak{q})$ and multiplicative in $\alpha$.

Have in mind that the quadratic residue symbol $(\alpha/\mathfrak{q})$ depends on the field $K$ although this fact is not displayed in our notation. Observe that, for $p$ a rational prime not dividing the rational integer $a$, the symbol $(a/p)$ does not agree with the Legendre symbol in $\mathbb{Q}$. To see this, take a prime $p$ which splits completely in $K$. Suppose $K/\mathbb{Q}$ is Galois of even degree. Then we can write $p = \mathfrak{q}\mathfrak{q}^\sigma$ where $\sigma$ is an involution in $G = \mathrm{Gal}(K/\mathbb{Q})$. Hence,

$$\left(\frac{a}{p}\right) = \left(\frac{a}{\mathfrak{q}}\right)\left(\frac{a}{\mathfrak{q}^\sigma}\right) = \left(\frac{a}{\mathfrak{q}}\right)^2 = 1,$$

while the Legendre symbol sometimes changes values.

If $\beta \in \mathcal{O}$, we say that $\beta$ is odd or even according as $(\beta)$ is, where $(\beta)$ is the principal ideal generated by $\beta$, and for $\beta$ odd, we define the symbol $(\alpha/\beta) = (\alpha/(\beta))$. Note that $(\alpha/\beta)$ does not change if $\beta$ is replaced by an associate; however, it may vary if $\alpha$ is changed by a unit which is not a square.

The famous law of quadratic reciprocity extends to arbitrary number fields. A nice treatment of this is given in Chap. 8 of Hecke [7]. See also Chap. 6, Sect. 8 of J. Neukirch [12]. To state this in the most convenient way, we first require the Hilbert symbols.

For any $\alpha, \beta \in K$ and any $\mathfrak{p}$, the Hilbert symbol

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \pm 1,$$

takes the value 1 if the quadratic form $\alpha x^2 + \beta y^2 - z^2$ represents zero non-trivially in the local field $K_{\mathfrak{p}}$ and takes the value $-1$ otherwise. We have the following properties for any $\alpha, \beta, \gamma \in K$ and any place $\mathfrak{p}$ (see Proposition 3.2 of [12]):

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \left(\frac{\beta, \alpha}{\mathfrak{p}}\right), \qquad \left(\frac{\alpha, \beta\gamma}{\mathfrak{p}}\right) = \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)\left(\frac{\alpha, \gamma}{\mathfrak{p}}\right),$$
$$\left(\frac{\alpha, -\alpha}{\mathfrak{p}}\right) = 1, \qquad \left(\frac{\alpha, 1-\alpha}{\mathfrak{p}}\right) = 1, \qquad \left(\frac{\alpha, \beta^2}{\mathfrak{p}}\right) = 1.$$

We next define, for any $\alpha, \beta, \in \mathcal{O}$

$$\mu_2(\alpha, \beta) = \prod_{\mathfrak{p}|2} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right), \qquad \mu_\infty(\alpha, \beta) = \prod_{\mathfrak{p}|\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right),$$

and

$$\mu(\alpha, \beta) = \mu_2(\alpha, \beta)\mu_\infty(\alpha, \beta).$$

For any $\alpha, \beta \in \mathcal{O}$, $\beta$ odd, we introduce the *completed* quadratic residue symbol

$$\left|\frac{\alpha}{\beta}\right| = \mu_\infty(\alpha, \beta)\left(\frac{\alpha}{\beta}\right). \tag{2.1}$$

Note that, if $\alpha$ or $\beta$ is totally positive, then $|\alpha/\beta| = (\alpha/\beta)$.

Now, we can state:

**Lemma 2.1** (Law of Quadratic Reciprocity) *For two odd integers* $\alpha, \beta \in \mathcal{O}$, *we have*

$$\left(\frac{\alpha}{\beta}\right) = \mu(\alpha, \beta)\left(\frac{\beta}{\alpha}\right), \tag{2.2}$$

*or equivalently,*

$$\left|\frac{\alpha}{\beta}\right| = \mu(\alpha, \beta)\left|\frac{\beta}{\alpha}\right| = \mu_2(\alpha, \beta)\left(\frac{\beta}{\alpha}\right). \tag{2.3}$$

Even in the rational field, the reciprocity law finds problems with the prime 2 and in number fields that situation is further complicated. We shall need to circumvent some of those problems with the symbol $(\alpha/\beta)$ in the situation where the upper entry may not be odd and we could not find in the literature a treatment which completely fulfilled our needs.

We shall show that the symbol $|\alpha/\beta|$, as a function of $\beta$ is periodic of period $(8\alpha)$. Actually, this does what we require with room to spare; all we need is that, for $(\alpha, \beta) = 1$ the symbol $(\alpha/\beta) = \pm 1$ depends on $\alpha$ but only on the residue class of $\beta$ modulo $(2^\ell \alpha)$, for some $\ell$ which could even depend on the field $K$. See the use of this property in Sect. 6.

Our goal in the remainder of this section is:

**Proposition 2.2** *Fix any nonzero* $\alpha \in \mathcal{O}$. *The symbol* $|\alpha/\beta|$, *for odd integers* $\beta$, *depends only on the residue class of* $\beta$ *modulo* $(8\alpha)$. *The same is true for the symbol* $(\alpha/\beta)$ *for odd totally positive integers* $\beta$.

We begin the argument with the following result.

**Lemma 2.3** *Let* $\alpha, \beta \in \mathcal{O}$ *be odd. Then,* $\mu_2(\alpha, \beta)$ *depends only on the residue classes of* $\alpha, \beta$ *modulo* 8.

*Proof* Using the multiplicativity property of the Hilbert symbol, we see that it suffices to prove that any $\eta \equiv 1 \pmod 8$ is a square in $K_\mathfrak{p}$ for any $\mathfrak{p}|2$. This follows by Hensel's lemma, but actually, it is seen explicitly from the identity

$$\sqrt{1+8x} = 1 + \sum_{\ell \geqslant 1} c_\ell \frac{(4x)^\ell}{\ell!}, \quad \text{where } c_\ell = \prod_{0 \leqslant k < \ell} (1-2k).$$

Since $2^\ell$ does not divide $\ell!$, the series converges $\mathfrak{p}$-adically. This completes the proof of the lemma. □

Combining the lemma with the reciprocity law, we obtain

**Corollary 2.4** *Proposition 2.2 is true in case* $\alpha$ *is odd.*

So, as expected, the main problem occurs when $\alpha$ is even. Were we to have a reasonable definition for our symbol when the lower entry is even and an accompanying version of the reciprocity law, then this case would probably also be straight-forward. As it is, we manoeuvre to reduce to the situation of the upper entry being odd by using properties of the symbol, in particular, its already known periodicity.

We next consider a further supplement to the Legendre symbol for which the period is even smaller. We define, for $\alpha, \beta \in \mathcal{O}$, $\beta$ odd,

$$\left[\frac{\alpha}{\beta}\right] = \mu_2(\alpha,\beta)\left|\frac{\alpha}{\beta}\right| = \mu(\alpha,\beta)\left(\frac{\alpha}{\beta}\right). \tag{2.4}$$

**Lemma 2.5** *Fix $\alpha \in \mathcal{O}$ such that $1+\alpha$ is odd. Then*

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\delta}\right] \quad \text{if } \beta \equiv \delta\big(\mathrm{mod}(2\alpha)\big). \tag{2.5}$$

*Proof* We can assume $(\alpha, \beta\delta) = 1$ since otherwise (2.5) trivially holds. Fix $\gamma \in \mathcal{O}$ such that $\beta\gamma \equiv 1+\alpha(\mathrm{mod}(2\alpha))$. Note that $\gamma$ is odd. It suffices to show that

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\gamma}\right].$$

To this end, consider the number

$$\lambda = \frac{\beta\gamma - 1}{\alpha}, \quad \text{so } \beta\gamma = \alpha\lambda + 1.$$

Obviously $\lambda \in \mathcal{O}$, $\lambda \equiv 1(\mathrm{mod}\, 2)$ and $(\lambda, \beta\gamma) = 1$. We write

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)\left(\frac{\lambda}{\beta}\right)^2 = \left(\frac{\alpha\lambda}{\beta}\right)\left(\frac{\lambda}{\beta}\right) = \left(\frac{-1}{\beta}\right)\left(\frac{\lambda}{\beta}\right) = \left(\frac{-\lambda}{\beta}\right) \\ = \left(\frac{\beta}{\lambda}\right)\prod_{\mathfrak{p}|2\infty}\left(\frac{\beta, -\lambda}{\mathfrak{p}}\right),\end{aligned}$$

by the reciprocity law. Next, we write

$$\left(\frac{\beta}{\lambda}\right) = \left(\frac{\gamma}{\lambda}\right) = \left(\frac{\lambda}{\gamma}\right)\prod_{\mathfrak{p}|2\infty}\left(\frac{\gamma, \lambda}{\mathfrak{p}}\right).$$

Here, we have

$$\left(\frac{\lambda}{\gamma}\right) = \left(\frac{\alpha}{\gamma}\right)\left(\frac{\alpha\lambda}{\gamma}\right) = \left(\frac{\alpha}{\gamma}\right)\left(\frac{-1}{\gamma}\right) = \left(\frac{\alpha}{\gamma}\right)\prod_{\mathfrak{p}|2\infty}\left(\frac{\gamma, -1}{\mathfrak{p}}\right).$$

Collecting the above results, we arrive at

$$\left(\frac{\alpha}{\beta}\right)=\left(\frac{\alpha}{\gamma}\right)\prod_{\mathfrak{p}|2\infty}\mu(\mathfrak{p}),$$

with

$$\begin{aligned}\mu(\mathfrak{p})&=\left(\frac{\beta,-\lambda}{\mathfrak{p}}\right)\left(\frac{\gamma,\lambda}{\mathfrak{p}}\right)\left(\frac{\gamma,-1}{\mathfrak{p}}\right)=\left(\frac{\beta\gamma,-\lambda}{\mathfrak{p}}\right)\\&=\left(\frac{\beta\gamma,-\alpha\lambda}{\mathfrak{p}}\right)\left(\frac{\beta\gamma,\alpha}{\mathfrak{p}}\right)=\left(\frac{\beta\gamma,1-\beta\gamma}{\mathfrak{p}}\right)\left(\frac{\beta\gamma,\alpha}{\mathfrak{p}}\right)\\&=\left(\frac{\beta\gamma,\alpha}{\mathfrak{p}}\right)=\left(\frac{\beta,\alpha}{\mathfrak{p}}\right)\left(\frac{\gamma,\alpha}{\mathfrak{p}}\right).\end{aligned}$$

This completes the proof of (2.5) and the lemma. □

We are now ready to complete the proof of Proposition 2.2. As particular cases of the previous lemma we get $[2/\beta]=[2/\delta]$ if $\beta\equiv\delta(\bmod 4)$ and, for any $\alpha\neq 0$, $[2\alpha/\beta]=[2\alpha/\delta]$ if $\beta\equiv\delta(\bmod(4\alpha))$. Multiplying the last two equations we find (because 4 is a square)

$$\left[\frac{\alpha}{\beta}\right]=\left[\frac{\alpha}{\delta}\right]\quad\text{if } \beta\equiv\delta\big(\bmod(4\alpha)\big).$$

Here, if we have the stronger congruence condition $\beta\equiv\delta(\bmod(8\alpha))$, the Hilbert symbol at any $\mathfrak{p}|2$ can be omitted by Lemma 2.3. This completes the proof of the proposition.

## 3 Number field preliminaries

Let $K$ be a totally real number field of degree $n=[K:\mathbb{Q}]$ so $K$ has $n$ embeddings into $\mathbb{R}$. For $\alpha\in K$ we denote its conjugates by $\alpha^{(1)},\dots,\alpha^{(n)}$. They are all real and

$$N\alpha=\alpha^{(1)}\cdots\alpha^{(n)},\qquad T\alpha=\alpha^{(1)}+\cdots+\alpha^{(n)}$$

are the norm and the trace of $\alpha$. We say that $\alpha\in K$ is totally positive if all its conjugates are positive, in which case we write $\alpha\succ 0$. We embed $K$ into $\mathbb{R}^n$ by the mapping

$$\alpha\to\big(\alpha^{(1)},\dots,\alpha^{(n)}\big)\tag{3.1}$$

with addition and multiplication performed componentwise. With a slight abuse of notation, for $\mathcal{D}$ a subset of $\mathbb{R}^n$ we shall write briefly $\alpha \in \mathcal{D}$ meaning $(\alpha^{(1)}, \dots, \alpha^{(n)}) \in \mathcal{D}$.

Let $\mathcal{U}$ denote the group of units, $\mathcal{U}^+$ the subgroup of totally positive units and $\mathcal{U}^2$ the subgroup of squares of units, so $\mathcal{U}^2 \subset \mathcal{U}^+ \subset \mathcal{U}$. Note that we have $[\mathcal{U} : \mathcal{U}^2] = 2^n$ because, by the Dirichlet unit theorem, every $u \in \mathcal{U}$ has a unique representation

$$u = \pm \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}, \quad r = n - 1, \tag{3.2}$$

where $\varepsilon_1, \dots, \varepsilon_r$ is a system of fixed fundamental units and $m_1, \dots, m_r \in \mathbb{Z}$. Hence $u$ is a square exactly when it has positive sign and the exponents $m_1, \dots, m_r$ are even. Assume the homomorphism $\mathcal{U} \to \{\pm 1\} \times \cdots \times \{\pm 1\}$ given by

$$u \to \left( \frac{u^{(1)}}{|u^{(1)}|}, \dots, \frac{u^{(n)}}{|u^{(n)}|} \right)$$

is surjective. Equivalently, this means that $[\mathcal{U} : \mathcal{U}^+] = 2^n$, hence $\mathcal{U}^+ = \mathcal{U}^2$ and also that ideal class equivalence is the same, whether defined in the wide or the narrow sense.

Note that for $u \in \mathcal{U}^+$, $u \neq 1$ we have

$$u^{(1)} + \cdots + u^{(n)} > n \tag{3.3}$$

and equality holds for $u = 1$. This follows from the arithmetic–geometric mean inequality.

We are now going to define the spin of odd principal ideals. Throughout, we assume that $K/\mathbb{Q}$ is a totally real Galois cyclic extension of degree $n \geqslant 3$ and $\mathcal{U}^+ = \mathcal{U}^2$. Fix a generator of $G = \mathrm{Gal}(K/\mathbb{Q})$, say $\sigma$. Then, if $\mathfrak{a}$ is an odd principal ideal, we define

$$\mathrm{spin}(\mathfrak{a}) = \left( \frac{\alpha}{\mathfrak{a}^\sigma} \right), \tag{3.4}$$

where $\alpha$ is chosen as a totally positive generator of $\mathfrak{a}$. Such an $\alpha$ is uniquely determined up to the square of a unit so $\mathrm{spin}(\mathfrak{a})$ is well-defined.[1]

Although the definition (3.4) makes sense for any $\sigma \in G$, we decided to choose $\sigma$ from the generators of $G$ because it will be convenient for our arguments. Having fixed $\sigma$, for notational convenience we shall write, for any

[1]For Gaussian primes, the name “spin” was used in [6], but for a symbol which is only superficially reminiscent of our $\mathrm{spin}(\mathfrak{p})$ for prime ideals. Writing $\pi = r + is \in \mathbb{Z}[i]$ uniquely with $r, s > 0, r$ odd, the spin of $p = \pi\bar{\pi}$ was defined to be the (usual) Jacobi symbol $\sigma_p = (s/r) = \pm 1$.

ideal $\mathfrak{a}$

$$\mathfrak{a}^{\sigma} = \mathfrak{a}', \qquad \mathfrak{a}^{\sigma^{-1}} = \mathfrak{a}^{-},$$

and for any $\alpha \in K$,

$$\alpha^{\sigma} = \alpha', \qquad \alpha^{\sigma^{-1}} = \alpha^{-}.$$

In this notation (3.4) becomes

$$\operatorname{spin}(\mathfrak{a}) = \left(\frac{\alpha}{\alpha'}\right) = \left(\frac{\alpha^{-}}{\alpha}\right).$$

Note that $\operatorname{spin}(\mathfrak{a}) = \pm 1$ if $(\mathfrak{a}, \mathfrak{a}') = 1$ and $\operatorname{spin}(\mathfrak{a}) = 0$ otherwise.

We shall need to understand the spin of the product of two odd ideals which may not be principal even though their product is. To this end we fix a collection $\mathcal{C}\ell = \{\mathfrak{A}, \mathfrak{B}, \ldots\}$ of odd ideals, a set of representatives of the ideal class group, choosing two from each class. Put

$$\mathfrak{f} = \prod_{\mathfrak{C} \in \mathcal{C}\ell} \mathfrak{C}. \tag{3.5}$$

We can assume, for purely technical convenience, that $\mathfrak{f}$ is a square-free ideal and of course $\mathfrak{f}$ is principal. Actually, we can assume even more, that

$$f = N\mathfrak{f} \quad \text{is square-free.} \tag{3.6}$$

Note that this implies that the ideals in our collection, together with their conjugates, are pairwise co-prime and odd. The reason for taking, in the collection $\mathcal{C}\ell$, two representatives from each ideal class is that sometimes we pick up one representative and find we need to do it again. For convenience, it is nice to have the second choice co-prime with the first.

Now, let $\mathfrak{a}\mathfrak{b}$ be a principal ideal co-prime with $2f$. We have

$$\begin{aligned} \mathfrak{a}\mathfrak{A} &= (\alpha), \quad \alpha \succ 0, \\ \mathfrak{b}\mathfrak{B} &= (\beta), \quad \beta \succ 0, \end{aligned} \tag{3.7}$$

for some $\mathfrak{A}, \mathfrak{B} \in \mathcal{C}\ell$, $\mathfrak{A} \neq \mathfrak{B}$. Note that $(\mathfrak{A}, \mathfrak{B}) = 1$ and $\mathfrak{A}\mathfrak{B}$ is co-prime with $\mathfrak{A}'\mathfrak{B}'$. Since $\mathfrak{a}\mathfrak{b}$ is principal so is $\mathfrak{A}\mathfrak{B}$, say $\mathfrak{A}\mathfrak{B} = (\gamma)$, $\gamma \succ 0$. Then $\mathfrak{a}\mathfrak{b}(\gamma) =$

$(\alpha\beta)$ and

$$\begin{aligned}\mathrm{spin}(\mathfrak{a}\mathfrak{b}) &= \left(\frac{\alpha\beta\gamma}{\mathfrak{a}'\mathfrak{b}'}\right) = \left(\frac{\alpha}{\mathfrak{b}'}\right)\left(\frac{\beta}{\mathfrak{a}'}\right)\left(\frac{\alpha}{\mathfrak{a}'}\right)\left(\frac{\beta}{\mathfrak{b}'}\right)\left(\frac{\gamma}{\mathfrak{a}'\mathfrak{b}'}\right)\\ &= \left(\frac{\alpha}{\beta'}\right)\left(\frac{\beta}{\alpha'}\right)\left(\frac{\alpha}{\mathfrak{a}'\mathfrak{B}'}\right)\left(\frac{\beta}{\mathfrak{b}'\mathfrak{A}'}\right)\left(\frac{\gamma}{\mathfrak{a}'\mathfrak{b}'}\right)\\ &= \left(\frac{\alpha}{\beta'}\right)\left(\frac{\beta}{\alpha'}\right)\left(\frac{\alpha\gamma}{\mathfrak{a}'\mathfrak{B}'}\right)\left(\frac{\beta\gamma}{\mathfrak{b}'\mathfrak{A}'}\right)\left(\frac{\gamma}{\gamma'}\right).\end{aligned}$$

Next, by the reciprocity law we write

$$\left(\frac{\beta}{\alpha'}\right) = \left(\frac{\beta^-}{\alpha}\right) = \pm\left(\frac{\alpha}{\beta^-}\right),$$

where the sign depends only on the residue classes of $\alpha$, $\beta$ modulo 8. Hence, we conclude the following factorization rule for the spin:

$$\mathrm{spin}(\mathfrak{a}\mathfrak{b}) = \pm\left(\frac{\alpha}{\beta'\beta^-}\right)\left(\frac{\alpha\gamma}{\mathfrak{a}'\mathfrak{B}'}\right)\left(\frac{\beta\gamma}{\mathfrak{b}'\mathfrak{A}'}\right)\mathrm{spin}(\gamma). \tag{3.8}$$

The two middle symbols separate $\mathfrak{a}$ from $\mathfrak{b}$ and hence do not play a role in the estimation of general bilinear forms. However, the leading symbol

$$\left(\frac{\alpha}{\beta'\beta^-}\right) = \left(\frac{\alpha}{\mathfrak{b}'\mathfrak{b}^-}\right)\left(\frac{\alpha}{\mathfrak{B}'\mathfrak{B}^-}\right) \tag{3.9}$$

is vital for this. Note that, if we had chosen $\sigma$ in (3.4) to be an involution, then $\beta' = \beta^-$ and the leading symbol in (3.9) would be constant, in other words the spin symbol would be essentially multiplicative. In such a case there is no way to get cancellation in general bilinear forms. This is the reason why our arguments fail for quadratic fields.

If $\mathfrak{p}$ is an odd prime ideal then

$$\sum_{\alpha\,(\mathrm{mod}\,\mathfrak{p})}\left(\frac{\alpha}{\mathfrak{p}}\right) = 0$$

which means that the number of quadratic residue classes $(\mathrm{mod}\,\mathfrak{p})$ is equal to the number of quadratic non-residue classes $(\mathrm{mod}\,\mathfrak{p})$. More generally, if the odd ideal $\mathfrak{q}$ is not the square of an ideal, then

$$\sum_{\alpha\,(\mathrm{mod}\,\mathfrak{q})}\left(\frac{\alpha}{\mathfrak{q}}\right) = 0. \tag{3.10}$$

We say that the positive rational integer $q$ is squarefull if $p|q$ implies $p^2|q$.

**Lemma 3.1** *Let $\mathfrak{q}$ be an odd ideal whose norm $q = N\mathfrak{q}$ is not squarefull. Then*

$$\sum_{\alpha (\operatorname{mod} \mathfrak{q}'\mathfrak{q}^-)} \left(\frac{\alpha}{\mathfrak{q}'\mathfrak{q}^-}\right) = 0. \tag{3.11}$$

*Proof* Let $p$ be a prime divisor of $q$ whose square does not divide $q$. Hence, $p = N\mathfrak{p}$ for some $\mathfrak{p}|\mathfrak{q}$ and $\mathfrak{q} = \mathfrak{p}\mathfrak{c}$ with $(\mathfrak{c}, p) = 1$. In particular, $(\mathfrak{c}'\mathfrak{c}^-, \mathfrak{p}'\mathfrak{p}^-) = 1$ so $\mathfrak{q}'\mathfrak{q}^- = \mathfrak{p}'\mathfrak{p}^-\mathfrak{c}'\mathfrak{c}^-$ is not the square of an ideal because $\mathfrak{p}' \neq \mathfrak{p}^-$. Hence (3.11) follows from (3.10). □

In many situations we shall employ an integral basis of $K$, say $\omega_1, \dots, \omega_n$. For convenience we can take $\omega_1 = 1$, so

$$\mathcal{O} = \omega_1\mathbb{Z} + \cdots + \omega_n\mathbb{Z} = \mathbb{Z} + \mathbb{M}$$

where $\mathbb{M} = \omega_2\mathbb{Z} + \cdots + \omega_n\mathbb{Z}$ is a submodule of $\mathcal{O}$ of rank $n-1$. We shall also consider the submodule $\mathbb{L} = \eta_2\mathbb{Z} + \cdots + \eta_n\mathbb{Z}$ with

$$\eta_2 = \omega_2 - \omega_2', \dots, \eta_n = \omega_n - \omega_n'. \tag{3.12}$$

**Lemma 3.2** *The map $\mathbb{M} \to \mathcal{O}$ given by $\beta \to \beta - \beta'$ is an injection; its image is the module $\mathbb{L}$.*

*Proof* Since the map $\xi \to \xi'$ generates the Galois group, it follows that, if $\beta' - \beta = 0$ then $\beta$ must be rational, hence contained in $\mathbb{Z} \cap \mathbb{M}$. However, $\mathbb{Z} \cap \mathbb{M} = 0$. □

**Corollary 3.3** *The numbers $\eta_2, \dots, \eta_n$ are linearly independent over $\mathbb{Q}$, so $\mathbb{L}$ has rank $n-1$.*

It would be nice to have an integral basis $1, \omega_2, \dots, \omega_n$ of $K$ for which all the conjugates of $\theta = \eta_2/\eta_3$ are distinct, so

$$W = \prod_{\tau \neq \mathrm{id}} \left(\eta_2\eta_3^\tau - \eta_2^\tau\eta_3\right) \neq 0. \tag{3.13}$$

In other words, we wish to have a basis such that $K = \mathbb{Q}(\theta)$. If $n$ is a prime number, then any basis gives $W \neq 0$. Indeed, if $\theta = \theta^\tau$ for some $\tau \neq \mathrm{id}$ then all the conjugates of $\theta$ are equal, because any $\tau \neq \mathrm{id}$ is a generator of the whole Galois group $G$. Therefore, $\theta$ is rational, contradicting the fact that $\eta_2, \eta_3$ are linearly independent over $\mathbb{Q}$. However, we can work with any basis and any $n \geqslant 3$ due to the following properties.

**Lemma 3.4** *Let* $\tau \in G$, $\tau \neq \mathrm{id}$. *Then, at least two of the numbers*

$$\eta_k^\tau / \eta_k, \quad 2 \leqslant k \leqslant n, \tag{3.14}$$

*are distinct.*

*Proof* Suppose all the numbers (3.14) are equal, so $(\eta_k/\eta_2)^\tau = \eta_k/\eta_2$ for $2 \leqslant k \leqslant n$. This shows that all the $n-1$ numbers $\eta_k/\eta_2$ are in a proper subfield of $K$ of degree $\leqslant n/2 < n-1$ so these numbers must be linearly dependent over $\mathbb{Q}$, which contradicts Corollary 3.3. □

Let $\mathfrak{h}(\tau)$ be the ideal generated by the numbers

$$\eta_k^\tau \eta_\ell - \eta_k \eta_\ell^\tau, \quad 2 \leqslant k \neq \ell \leqslant n. \tag{3.15}$$

Thus, Lemma 3.4 says that $\mathfrak{h}(\tau)$ is a non-zero ideal. We denote

$$\mathfrak{h} = \mathfrak{D} \prod_{\tau \neq \mathrm{id}} \mathfrak{h}(\tau), \tag{3.16}$$

where $\mathfrak{D}$ is the *different* of the field $K$.

For $\alpha = a_1\omega_1 + \cdots + a_n\omega_n \in \mathcal{O}$ the basis coefficients $a_1, \ldots, a_n$ are linear combinations of the conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ and vice-versa. Therefore, the system of estimates $\alpha^{(1)}, \ldots, \alpha^{(n)} \ll y$ is equivalent to the system of estimates $a_1, \ldots, a_n \ll y$, of course with possibly different implied constants depending on the field $K$ and the basis.

We are going to estimate sums of a quadratic character in $\mathcal{O}$ by using bounds for sums of a quadratic character in $\mathbb{Z}$. The following simple result plays a crucial role in this reduction.

**Lemma 3.5** *Let $K$ be any number field and $n$ its degree. If the integral ideal $\mathfrak{f}$ of $K$ has square-free norm, then every residue class* $(\bmod\, \mathfrak{f})$ *is represented by a rational integer.*

*Proof* Let $f = N\mathfrak{f}$. Then, the number of residue classes $\bmod\, \mathfrak{f}$ is, by definition, just $f$ and, to show the result, it suffices to show that the numbers $1, 2, \ldots, f$ are incongruent modulo $\mathfrak{f}$. Now, suppose two such rational integers $a$ and $b$ are congruent $\bmod\, \mathfrak{f}$. Then, by the complete multiplicativity of the norm, $N\mathfrak{f} = f$ divides $N(a-b) = (a-b)^n$. But these are rational integers and $f$ is square-free so $f$ must divide the square-free kernel of $(a-b)^n$, which in turn divides $a-b$. (Alternatively, $\mathcal{O}/\mathfrak{f}$ is the direct product of prime fields $\mathbb{F}_p$ for distinct primes $p$ and so, by the Chinese Remainder Theorem, is isomorphic to $\mathbb{Z}/f\mathbb{Z}$.) □

Let $\mathfrak{q}$ be an odd ideal. Consider the symbol

$$\chi_{\mathfrak{q}}(\ell) = \left(\frac{\ell}{\mathfrak{q}}\right) \quad \text{for } \ell \in \mathbb{Z}. \tag{3.17}$$

This is multiplicative in $\ell$ and periodic of period $q = N\mathfrak{q}$ so, as a function on $\mathbb{Z}$, $\chi_{\mathfrak{q}}$ is a real Dirichlet character of modulus $q$. We need to know when $\chi_{\mathfrak{q}}$ can be the principal character.

**Lemma 3.6** *For an odd ideal $\mathfrak{q}$, if $q = N\mathfrak{q}$ is not squarefull then the Dirichlet character $\chi_{\mathfrak{q}}$ is not principal.*

*Proof* Suppose $q$ is not squarefull. That means there is a prime $p$ dividing $q$ whose square does not divide $q$. Since $q = N\mathfrak{q}$, there is a prime ideal $\mathfrak{p}$ lying above $p$ and dividing $\mathfrak{q}$. Take $\ell$ which is a non-square modulo $p$ and $\ell \equiv 1 (\bmod\, q/p)$. Such an $\ell$ exists by the Chinese Remainder Theorem. Now, $\chi_{\mathfrak{q}}(\ell) = \chi_{\mathfrak{p}}(\ell)\chi_{\mathfrak{q}/\mathfrak{p}}(\ell) = -1$ so the character is not principal. □

In the following sections we shall often appeal to some estimates for the units in $\mathcal{U}^+$ which we are now going to present. These are not new (see for example, Cassels [4], Lang [9], for different arguments) but we include brief proofs for completeness.

**Lemma 3.7** *There exists a unit $u \in \mathcal{U}^+$ such that all but one of its conjugates are $\leqslant \frac{1}{2}$.*

*Proof* Let $-1, \varepsilon_1, \dots, \varepsilon_r$ be generators of $\mathcal{U}$ with $\varepsilon_\ell > 0$ for $1 \leqslant \ell \leqslant r = n-1$. Take

$$u = \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r},$$

so

$$u^{(k)} = \varepsilon_1^{(k)a_1} \cdots \varepsilon_r^{(k)a_r}.$$

We need integers $a_1, \dots, a_r$ such that all the linear forms

$$L_k = a_1 \log \varepsilon_1^{(k)} + \cdots + a_r \log \varepsilon_r^{(k)}, \quad 1 \leqslant k \leqslant r$$

are negative. Because the determinant (the regulator) of

$$\mathcal{R} = \left(\log \varepsilon_\ell^{(k)}\right), \quad 1 \leqslant \ell, k \leqslant r$$

does not vanish, there are real numbers $a_1, \dots, a_r$ with $L_k = -1$ for all $1 \leqslant k \leqslant r$. Approximate these by rationals and then clear the denominators getting a unit $u \in \mathcal{U}$ with $u^{(1)}, \ldots, u^{(r)} < 1$. Raising $u$ to a sufficiently large even power, we get a unit with the required property. □

**Lemma 3.8** *Let $B \geqslant 1$. The number of integers $\alpha \in \mathcal{O}_K$ all of whose conjugates satisfy $|\alpha^{(k)}| \leqslant B$ is finite. Those of the integers which are units $u \in \mathcal{U}^+$ also satisfy $u^{(k)} \geqslant B^{-r}$.*

*Proof* The number of possible irreducible polynomials these integers can satisfy is finite since the degree and coefficients of the latter are bounded. This gives the upper bound. The lower bound in case of $u \in \mathcal{U}^+$ follows because $Nu = 1$. □

Finally, we want to give examples of some fields having the properties we have been assuming. The following result is handy for this purpose.

**Lemma 3.9** *Suppose $n$ is an odd prime, and 2 is a primitive root modulo $n$. If $\mathcal{U}$ contains a unit that is neither totally positive nor totally negative, then $\mathcal{U}^+ = \mathcal{U}^2$.*

*Proof* Let $H = \{\pm 1\}^n$, and consider the map $\varphi : \mathcal{U}/\mathcal{U}^2 \to H$ defined by

$$u \mapsto \bigl(\operatorname{sign}\bigl(u^{(1)}\bigr), \ldots, \operatorname{sign}\bigl(u^{(n)}\bigr)\bigr).$$

The Galois group $G$ acts naturally on $H$ by permuting the real embeddings of $K$. With this action $H$ is a free $\mathbb{F}_2[G]$-module of rank one, and $\varphi$ is an $\mathbb{F}_2[G]$-homomorphism. If $n$ is an odd prime, then $\mathbb{F}_2[G]$ decomposes

$$\mathbb{F}_2[G] \cong \mathbb{F}_2[x]/\bigl(x^n - 1\bigr) \cong \mathbb{F}_2[x]/(x-1) \oplus \mathbb{F}_2[x]/\bigl(\Phi_n(x)\bigr),$$

where $\Phi_n(x) = (x^n - 1)/(x - 1)$ is the $n$-th cyclotomic polynomial. If 2 is a primitive root modulo $n$, then $\Phi_n(x)$ is irreducible in $\mathbb{F}_2[x]$, and we conclude that $H$ is the direct sum of two irreducible $\mathbb{F}_2[G]$-modules, the one-dimensional trivial representation and an irreducible $(n-1)$-dimensional complement. The image $\varphi(\mathcal{U})$ is an $\mathbb{F}_2[G]$-submodule of $H$ containing the trivial subspace $\{\varphi(1), \varphi(-1)\}$, so if $\mathcal{U}$ contains any unit of mixed signs then $\varphi(\mathcal{U})$ must be all of $H$, i.e., $\varphi$ is surjective.

By (3.2) we have $[\mathcal{U} : \mathcal{U}^2] = 2^n = |H|$, so $\varphi$ is an isomorphism. Since $\mathcal{U}^+/\mathcal{U}^2$ is in the kernel of $\varphi$, we conclude that $\mathcal{U}^+ = \mathcal{U}^2$. □

*Examples* Suppose $n = 3$. There is a nice family of cyclic cubic fields, introduced by Shanks [13], which provides examples of number fields satisfying $\mathcal{U}^+ = \mathcal{U}^2$.

For integers $m$, let $\alpha_m$ be a root of the polynomial

$$f_m(x) = x^3 + mx^2 + (m-3)x - 1.$$

Note that the only rational roots $f_m$ can have are $\pm 1$, but $f_m(1) = 2m - 3$ and $f_m(-1) = 1$, so $f_m$ is irreducible for every $m$. The discriminant of $f_m$ is $(m^2 - 3m + 9)^2$, so $K_m = \mathbb{Q}(\alpha_m)$ is a cyclic cubic field for every $m$.

Next, we note that for every $m$, Descartes' "Rule of Signs" shows that the polynomial $f_m(x)$ has exactly one positive real root. Therefore $\alpha_m$ has both positive and negative real embeddings, so Lemma 3.9 shows that $\mathcal{U}^+ = \mathcal{U}^2$ for every integer $m$.

Similarly, when $n = 5$ there is a family of cyclic quintic fields constructed by Lehmer [10]. For every integer $m$ let

$$g_m(x) = x^5 + m^2x^4 - 2\big(m^3 + 3m^2 + 5m + 5\big)x^3 + \big(m^4 + 5m^3 + 11m^2 + 15m + 5\big)x^2 + \big(m^3 + 4m^2 + 10m + 10\big)x + 1,$$

and let $\beta_m$ be a root of $g_m$. The field $L_m = \mathbb{Q}(\beta_m)$ is a cyclic quintic extension of $\mathbb{Q}$, and $\beta_m$ is a unit of $L_m$ of norm $-1$. Thus $\beta_m$ has at least one negative real embedding. If all the real embeddings of $\beta_m$ were negative, then all coefficients of $g_m$ would be positive. It is simple to check that $-2(m^3 + 3m^2 + 5m + 5)$ and $m^3 + 4m^2 + 10m + 10$ are not simultaneously positive for any integer $m$, so $\beta_m$ has at least one positive real embedding. Since 2 is a primitive root modulo 5, we conclude from Lemma 3.9 that $\mathcal{U}^+ = \mathcal{U}^2$ for every integer $m$.

## 4 A fundamental domain

In order to have a convenient unique representation of a principal ideal by one of its generators, we look for a specific fundamental domain of the group $\mathcal{U}^+$ acting on $\mathbb{R}^n_+$ by

$$u \circ x = \big(u^{(1)}x_1, \dots, u^{(n)}x_n\big). \tag{4.1}$$

For notational simplicity, we write $x \succ 0$, meaning that all the co-ordinates of $x = (x_1, \dots, x_n)$ are positive. Similarly, $x \succ C$ or $x \prec C$ means that all the co-ordinates are greater than $C$, or smaller than $C$, respectively. For $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ in $\mathbb{R}^n$ the scalar product is defined by

$$x \cdot y = x_1y_1 + \cdots + x_ny_n.$$

We begin with a somewhat general consideration. Let $U$ be a collection of $n$-dimensional positive vectors which does not contain $e = (1, \dots, 1)$. Put

$$\mathcal{D} = \big\{x \in \mathbb{R}^n_+;\ x \succ 0,\ u \cdot x > e \cdot x \text{ for all } u \in U\big\}. \tag{4.2}$$

Suppose there is a matrix $(c_{k\ell})$, $1 \leqslant k, \ell \leqslant n$ whose rows are in $U$, with its diagonal entries $c_{kk} > 1$ for $1 \leqslant k \leqslant n$ and its off-diagonal entries satisfying

$0 < c_{k\ell} < 1$ for $1 \leqslant k \neq \ell \leqslant n$. Put

$$C = 1 + \max_{k \neq \ell} \frac{c_{kk} - 1}{1 - c_{k\ell}}. \tag{4.3}$$

Note that all the entries of $(c_{k\ell})$ satisfy $0 < c_{k\ell} < C$. Define

$$\mathcal{D}(C) = \left\{x \in \mathbb{R}_+^n;\ x \succ 0,\ v \cdot x > e \cdot x \text{ for all } v \in U, v \prec C\right\}. \tag{4.4}$$

**Lemma 4.1** *We have*

$$\mathcal{D}(C) = \mathcal{D}. \tag{4.5}$$

*Proof* Obviously, $\mathcal{D} \subset \mathcal{D}(C)$. Suppose there exists $x \in \mathcal{D}(C) \setminus \mathcal{D}$. Because $x \notin \mathcal{D}$ there exists $u \in U$ such that $u \cdot x \leqslant e \cdot x$. Hence, $u$ is not bounded by $C$ because $x \in \mathcal{D}(C)$. This means that $u = (u_1, \dots, u_n)$ has $u_k \geqslant C$ for some $1 \leqslant k \leqslant n$. We write the inequality $u \cdot x \leqslant e \cdot x$ for $x = (x_1, \dots, x_n)$ in the following form:

$$(u_k - 1)x_k \leqslant \sum_{\ell \neq k} (1 - u_\ell)x_\ell.$$

Hence,

$$(C - 1)x_k < \sum_{\ell \neq k} x_\ell.$$

But

$$(C - 1) \geqslant (c_{kk} - 1)/\min_{\ell \neq k}(1 - c_{k\ell})$$

and hence

$$(c_{kk} - 1)x_k < \sum_{\ell \neq k} (1 - c_{k\ell})x_\ell.$$

Since the vector $v = (c_{k1}, \dots, c_{kn})$ belongs to $U$ and its entries are bounded by $C$, the last inequality contradicts the assumption that $x \in \mathcal{D}(C)$. □

We are going to apply Lemma 4.1 to the collection of vectors

$$U = \left\{\left(u^{(1)}, \dots, u^{(n)}\right); u \in \mathcal{U}^+, u \neq 1\right\}.$$

By Lemma 3.7 there exists a unit $u \in \mathcal{U}^+$ such that $u^{(1)}, \dots, u^{(n-1)} < 1$ and hence $u^{(n)} > 1$. This unit $u$ and its conjugates form the matrix $(c_{k\ell})$ whose existence was used in the proof of Lemma 4.1. We obtain:

**Lemma 4.2** *There exists a constant* $C > 1$ *such that the sets*

$$\mathcal{D} = \{x \succ 0; u \cdot x > e \cdot x \text{ for all } u \in \mathcal{U}^+, u \neq 1\}, \tag{4.6}$$

$$\mathcal{D}(C) = \{x \succ 0; u \cdot x > e \cdot x \text{ for all } u \in \mathcal{U}^+, u \neq 1, u \prec C\}, \tag{4.7}$$

*are the same set.*

Note that, by Lemma 3.8, the collection of units $u \neq 1, u \prec C$ which are used in $\mathcal{D}(C)$ is finite. We fix such a $C$ and denote

$$\tilde{\mathcal{U}} = \{u \in \mathcal{U}^+; u \neq 1, u \prec C\}. \tag{4.8}$$

Note that the closure $\bar{\mathcal{D}}$ consists of those $x$ for which all of the signs $>$ in $u \cdot x > e \cdot x$ are replaced by $\geqslant$ and the boundary consists of those elements of the closure for which we have equality with at least one unit $u \neq 1$.

Now, we are ready to prove the fundamental properties of the set (4.6).

**Lemma 4.3** *For any* $u \in \mathcal{U}^+, u \neq 1$ *we have*

$$(u \circ \mathcal{D}) \cap \mathcal{D} = \varnothing. \tag{4.9}$$

*For every* $x > 0$ *there exists* $u \in \mathcal{U}^+$ *which sends* $x$ *to the closure of* $\mathcal{D}$, *that is*

$$u \circ x \in \bar{\mathcal{D}}. \tag{4.10}$$

*Proof* Suppose $x \in \mathcal{D}$ and $x \in u \circ \mathcal{D}$. Then, $y = u^{-1} \circ x \in \mathcal{D}$, so $u^{-1} \cdot x > e \cdot x$ and $u \cdot y > e \cdot y$. The second inequality reads as

$$e \cdot x = u \cdot (u^{-1} \circ x) > e \cdot (u^{-1} \circ x) = u^{-1} \cdot x,$$

which contradicts the first inequality. This proves the first property (4.9). The second property (4.10) follows by choosing $u \in \mathcal{U}^+$ for which $u \cdot x$ is minimal. The minimum is attained since it is over a finite set, which is seen to be the case because $\mathcal{D} = \mathcal{D}(C)$. Suppose this $u$ did not have the property (4.10). This means that there is a $v \in \mathcal{U}^+$, $v \neq \mathrm{id}$, such that $v \cdot (u \circ x) < u \cdot x$. Hence $vu \in \mathcal{U}^+$ gives a smaller value than the minimum and proves (4.10). □

The above argument is essentially our interpretation of an argument of Shintani [14] who gave a complete description of the fundamental domain, say $\mathcal{D}^*$, of the action of $\mathcal{U}^+$ on $\mathbb{R}^n_+$. Lemma 4.3 shows that one can choose $\mathcal{D}^*$ with

$$\mathcal{D} \subset \mathcal{D}^* \subset \bar{\mathcal{D}}. \tag{4.11}$$

For our applications we do not need to see the boundary of $\mathcal{D}^*$ and that simplifies things a lot. Note that, if $\alpha \in \mathcal{O}$ then $\alpha \in \mathcal{D}$ means that $\alpha \succ 0$ and it has the smallest trace amongst its positive associates $u\alpha$, $u \in \mathcal{U}^+$. There are several features of this particular domain $\mathcal{D}^*$, such as convexity, which help to control the transition from ideals to integers. We present a few of these here; the others will be introduced as they are exploited in Sect. 6.

**Lemma 4.4** *Every $\alpha \in \mathcal{D}$ has all its conjugates in $\mathcal{D}$ and all of them have essentially the same size, that is*

$$\alpha^{(k)} \asymp T(\alpha) \asymp (N\alpha)^{\frac{1}{n}}, \quad 1 \leqslant k \leqslant n. \tag{4.12}$$

*Proof* Choose $u \in \mathcal{U}^+$ such that $u^{(\ell)} \leqslant \frac{1}{2}$ for all $\ell \neq k$, as in Lemma 3.7. Then, we see in turn,

$$u^{(1)}\alpha^{(1)} + \cdots + u^{(n)}\alpha^{(n)} > \alpha^{(1)} + \cdots + \alpha^{(n)},$$

$$u^{(k)}\alpha^{(k)} > \frac{1}{2}\big(\alpha^{(1)} + \cdots + \alpha^{(n)}\big),$$

$$\alpha^{(k)} \gg T\alpha, \quad k = 1, 2, \ldots, n.$$

Now, take $u \in \mathcal{U}^+$ to be the reciprocal of the previous choice, giving $\alpha^{(k)} \ll T\alpha$. This completes the proof. □

**Corollary 4.5** *If $\alpha = a_1\omega_1 + \cdots + a_n\omega_n \in \mathcal{D}$ then*

$$a_k \ll (N\alpha)^{\frac{1}{n}} \quad \textit{for } k = 1, \ldots, n. \tag{4.13}$$

Denote by $\mathcal{N}(x)$ the number of integers $\alpha \in \bar{\mathcal{D}}$ with $N\alpha \leqslant x$. Thus

$$\mathcal{N}(x) \asymp x, \tag{4.14}$$

but we do not need an asymptotic formula for $\mathcal{N}(x)$. More important to us is to have a precise comparison of $\mathcal{N}(x)$ with the number of these integers which are in a given residue class.

$$\mathcal{N}(x; \mathfrak{m}, \nu) = \sum_{\substack{\alpha \in \bar{\mathcal{D}}, N\alpha \leqslant x \\ \alpha \equiv \nu (\mathrm{mod}\, \mathfrak{m})}} 1. \tag{4.15}$$

**Lemma 4.6** *For any integral ideal* $\mathfrak{m}$ *and any* $\nu (\mathrm{mod}\, \mathfrak{m})$ *we have*

$$\mathcal{N}(x; \mathfrak{m}, \nu) = \frac{\mathcal{N}(x)}{N\mathfrak{m}} + O\big(x^{1-\frac{1}{n}}\big), \tag{4.16}$$

*where the implied constant depends only on the field $K$ (and so, not on* $\mathfrak{m}$*).*

*Proof* Fix an integral basis of $\mathcal{O}$ and choose one of its elements, say $\omega$. Write $\alpha = a\omega + \beta$ where $a \in \mathbb{Z}$ and $\beta$ is a linear combination of the other basis elements. Given $\beta$, we are going to evaluate the number of rational integers $a$ such that

$$a\omega + \beta \in \bar{\mathcal{D}}, \quad P(a) \leqslant x, \tag{4.17}$$

where $P(X) = (X\omega^{(1)} + \beta^{(1)}) \cdots (X\omega^{(n)} + \beta^{(n)})$, and

$$a\omega + \beta \equiv \nu (\bmod \mathfrak{m}). \tag{4.18}$$

The first condition in (4.17) means that $a$ satisfies a finite system of linear inequalities which also means exactly that $a$ is in a single interval whose end-points depend on $\omega, \beta$ and $K$. The second condition in (4.17) can be expressed as saying that $a$ runs over $n$ intervals, each of length $\ll x^{1/n}$, whose end-points depend on $\omega$, $\beta$ and $x$. Together, the two conditions in (4.17) are equivalent to saying that $a$ is in one of $n$ intervals of length $\ll x^{1/n}$ whose end-points depend on $\omega$, $\beta$, $K$ and $x$.

Next, the congruence condition (4.18), if solvable, means that we have $a \equiv a_0 (\bmod m)$ where $m$ is a positive rational number which depends on $\omega$, $\mathfrak{m}$ and $a_0$ is a rational residue class modulo $m$ which depends on $\omega$, $\nu$, $\beta$ and $\mathfrak{m}$. (We can take $m$ to be the smallest positive rational integer divisible by the ideal $\mathfrak{m}/(\omega, \mathfrak{m})$.) Changing $\nu$ to $\nu' = \nu + c\omega$ with $c \in \mathbb{Z}$ translates the class $a_0$ to $a_0 + c$. This operation can change the number of $a$'s in a given segment (of an arithmetic progression) by at most one. Such a bounded error term is then amplified by the number of segments and by the number of $\beta$ with $N\beta \ll x$ which is $O(x^{1-1/n})$. This proves that

$$\mathcal{N}(x; \mathfrak{m}, \nu) = \mathcal{N}\big(x; \mathfrak{m}, \nu'\big) + O\big(x^{1-\frac{1}{n}}\big), \quad \text{if } \nu' \in \nu + \omega\mathbb{Z},$$

where the implied constant depends only on the field $K$. Repeating these arguments with every element of the basis we derive the result for every $\nu' (\bmod \mathfrak{m})$. Then, averaging this relation over all classes $\nu' (\bmod \mathfrak{m})$, we complete the proof of (4.16). □

## 5 Sums over prime ideals

We begin with a few formulas of a combinatorial nature. Let $K$ be a number field. For any non-zero integral ideal $\mathfrak{n}$ we set

$$\Lambda(\mathfrak{n}) = \log N\mathfrak{p}, \qquad \text{if } \mathfrak{n} = \mathfrak{p}^{\ell},\ \ell = 1, 2, \ldots,$$

and $\Lambda(\mathfrak{n}) = 0$ otherwise. Hence it is easy to see that

$$\sum_{\mathfrak{b} | \mathfrak{a}} \Lambda(\mathfrak{b}) = \log N\mathfrak{a}.$$

Next, we introduce the Möbius function

$$\mu(\mathfrak{m}) = (-1)^t$$

if $\mathfrak{m}$ is the product of $t$ distinct prime ideals and $\mu(\mathfrak{m}) = 0$ otherwise. Note that for $\mathfrak{m} = (1)$ we have $t = 0$ and $\mu((1)) = 1$. Hence, we deduce

$$\sum_{\mathfrak{m}|\mathfrak{a}} \mu(\mathfrak{m}) = \begin{cases} 1 & \text{if } \mathfrak{a} = (1), \\ 0 & \text{otherwise.} \end{cases}$$

Using this, one can check the formulas

$$\Lambda(\mathfrak{n}) = -\sum_{\mathfrak{m}|\mathfrak{n}} \mu(\mathfrak{m}) \log N\mathfrak{m} = \sum_{\mathfrak{m}|\mathfrak{n}} \mu(\mathfrak{m}) \log \frac{N\mathfrak{n}}{N\mathfrak{m}}.$$

Let $\mathcal{A} = (a_{\mathfrak{n}})$ be an arbitrary sequence of complex numbers, enumerated by integral ideals and ordered by the norm. We are interested in estimating the sum

$$S(x) = \sum_{N\mathfrak{n}\leqslant x} a_{\mathfrak{n}} \Lambda(\mathfrak{n}). \tag{5.1}$$

We are thinking of the $a_{\mathfrak{n}}$ as changing argument randomly and expect considerable cancellation in the sum $S(x)$. Having this in mind, we are going to write a fairly general inequality which offers a bound for $S(x)$ in terms of other sums which we know how to manage. The idea goes by adding more terms in the spirit of the Eratosthenes–Legendre sieve until reaching two kinds of sums. The first kind are the congruence sums

$$A_{\mathfrak{d}}(x) = \sum_{\substack{N\mathfrak{n}\leqslant x \\ \mathfrak{n}\equiv 0 (\mathrm{mod}\, \mathfrak{d})}} a_{\mathfrak{n}}. \tag{5.2}$$

These will appear for $\mathfrak{d}$ with $d = N\mathfrak{d}$ relatively small, so the problem of estimating $A_{\mathfrak{d}}(x)$ really belongs to the harmonic analysis of $\mathcal{A} = (a_{\mathfrak{n}})$.

The second kind of sums are the bilinear forms

$$\mathcal{B}(M, N) = \sum_{N\mathfrak{m}\leqslant M} \sum_{N\mathfrak{n}\leqslant N} v_{\mathfrak{m}} w_{\mathfrak{n}} a_{\mathfrak{m}\mathfrak{n}}. \tag{5.3}$$

These will appear for $M, N$ neither of which is very small so that $\mathcal{B}(M, N)$ is a genuine bilinear form. Here the point is that $(v_{\mathfrak{m}})$, $(w_{\mathfrak{n}})$ are independent sequences; they do not see each other so they cannot conspire to annihilate the change of arguments of $a_{\mathfrak{m}\mathfrak{n}}$. Well, except for a sequence $\mathcal{A}$ whose terms are multiplicative; for example, if $a_{\mathfrak{mn}} = c_{\mathfrak{m}} c_{\mathfrak{n}}$ then the bilinear form (5.3) factors into linear forms

$$\mathcal{B}(M, N) = \Big( \sum_{N\mathfrak{m} \leqslant M} v_{\mathfrak{m}} c_{\mathfrak{m}} \Big) \Big( \sum_{N\mathfrak{n} \leqslant N} w_{\mathfrak{n}} c_{\mathfrak{n}} \Big)$$

and we can obtain a bias by choosing $v_{\mathfrak{m}} = \bar{c}_{\mathfrak{m}}$ and $w_{\mathfrak{n}} = \bar{c}_{\mathfrak{n}}$. Therefore, it is important that the sequence $\mathcal{A} = (a_{\mathfrak{n}})$ not be multiplicative in $\mathfrak{n}$. Our target sequence $a_{\mathfrak{n}} = \mathrm{spin}(\mathfrak{n})$ is qualified for treatment by our method, due to the twisted factorization property (3.8).

We shall see that the required bilinear forms $\mathcal{B}(M, N)$ have specific coefficients $v_{\mathfrak{m}}, w_{\mathfrak{n}}$, but in practice we are unable to take advantage of their intrinsic properties, so there is no point to describe these. Our estimates for $\mathcal{B}(M, N)$ will depend only on the upper bound for their coefficients. Specifically, we shall use the bilinear form with

$$|v_{\mathfrak{m}}| \leqslant \Lambda(\mathfrak{m}), \qquad |w_{\mathfrak{n}}| \leqslant \tau(\mathfrak{n}), \tag{5.4}$$

where $\tau$ is the usual divisor function, but of ideals in the ring $\mathcal{O}$.

**Proposition 5.1** *Let $x = yz$ with $z \geqslant y \geqslant 2$. We have*

$$\big|S(x)\big| \leqslant (3 \log x) \sum_{N\mathfrak{d} \leqslant y^2} \big|A_{\mathfrak{d}}\big(x'\big)\big| + (2 \log x)^2 \big|\mathcal{B}(M, N)\big| + \big|S(z)\big|, \tag{5.5}$$

*for some $x' \leqslant x$, some $M, N \leqslant z$, $MN = 2x$ and some complex coefficients $v_{\mathfrak{m}}, w_{\mathfrak{n}}$ in $\mathcal{B}(M, N)$ satisfying (5.4).*

*Proof* We begin by decomposing the convolution $\Lambda = \mu * \log$ as follows:

$$\Lambda(\mathfrak{n}) = \sum_{\mathfrak{am} = \mathfrak{n}} \mu(\mathfrak{m}) \log N\mathfrak{a} = \sum_{\substack{\mathfrak{am} = \mathfrak{n} \\ N\mathfrak{m} \leqslant y}} \mu(\mathfrak{m}) \log N\mathfrak{a} + \sum_{\substack{\mathfrak{lam} = \mathfrak{n} \\ N\mathfrak{m} > y}} \mu(\mathfrak{m}) \Lambda(\mathfrak{a}).$$

Suppose $\mathfrak{n}$ has norm $N\mathfrak{n} \leqslant x = yz$ with $z \geqslant y \geqslant 2$. Then, in the last sum we have $N\mathfrak{a} \leqslant z$. Having recorded this information, we now write

$$\sum_{\substack{\mathfrak{lam} = \mathfrak{n} \\ N\mathfrak{a} \leqslant z, N\mathfrak{m} > y}} \mu(\mathfrak{m}) \Lambda(\mathfrak{a}) = \sum_{\substack{\mathfrak{lam} = \mathfrak{n} \\ N\mathfrak{a} \leqslant z}} \mu(\mathfrak{m}) \Lambda(\mathfrak{a}) \quad - \sum_{\substack{\mathfrak{lam} = \mathfrak{n} \\ N\mathfrak{a} \leqslant z, N\mathfrak{m} \leqslant y}} \mu(\mathfrak{m}) \Lambda(\mathfrak{a}).$$

If, in the first sum on the right, we fix $\mathfrak{a}$, the inner *complete* sum over $\mathfrak{lm}$ vanishes unless $\mathfrak{lm} = (1)$ in which case $\mathfrak{a} = \mathfrak{n}$. Hence, we get the following identity:

$$\bigl(1-\delta(\mathfrak{n},z)\bigr)\Lambda(\mathfrak{n})=\sum_{\substack{\mathfrak{a}\mathfrak{m}=\mathfrak{n}\\ N\mathfrak{m}\leqslant y}}\sum\mu(\mathfrak{m})\log N\mathfrak{a}-\sum_{\substack{\mathfrak{l}\mathfrak{a}\mathfrak{m}=\mathfrak{n}\\ N\mathfrak{a}\leqslant z,N\mathfrak{m}\leqslant y}}\sum\sum\mu(\mathfrak{m})\Lambda(\mathfrak{a}),$$

where $\delta(\mathfrak{n},z)=1$ if $N\mathfrak{n}\leqslant z$ and is zero elsewhere. We split the sum over $\mathfrak{l}\mathfrak{a}\mathfrak{m}=\mathfrak{n}$ into two sums having $N\mathfrak{a}\leqslant y$ or not. Accordingly, $S(x)-S(z)$ splits into three sums

$$S(x)-S(z)=S_1(x)-S_2(x)-S_3(x),$$

where

$$S_1(x)=\sum_{N\mathfrak{m}\leqslant y}\mu(\mathfrak{m})\sum_{\substack{N\mathfrak{n}\leqslant x\\ \mathfrak{n}\equiv 0(\operatorname{mod}\mathfrak{m})}}a_{\mathfrak{n}}\log N\left(\frac{\mathfrak{n}}{\mathfrak{m}}\right),$$

$$S_2(x)=\sum_{\mathfrak{d}}\Biggl(\sum_{\substack{\mathfrak{a}\mathfrak{m}=\mathfrak{d}\\ N\mathfrak{a}\leqslant y,N\mathfrak{m}\leqslant y}}\mu(\mathfrak{m})\Lambda(\mathfrak{a})\Biggr)A_{\mathfrak{d}}(x)$$

and

$$S_3(x)=\sum_{\substack{N(\mathfrak{l}\mathfrak{a}\mathfrak{m})\leqslant x\\ y<N\mathfrak{a}\leqslant z,N\mathfrak{m}\leqslant y}}\sum\sum\mu(\mathfrak{m})\Lambda(\mathfrak{a})a_{\mathfrak{l}\mathfrak{a}\mathfrak{m}}.$$

Note that, in the sum $S_2(x)$, we have $N\mathfrak{d}\leqslant y^2$ and the coefficient in front of the congruence sum $A_{\mathfrak{d}}(x)$ is bounded by

$$\sum_{\mathfrak{a}\mathfrak{m}=\mathfrak{d}}\Lambda(\mathfrak{a})=\log N\mathfrak{d}.$$

Similarly, we treat the first sum $S_1(x)$. Here, the presence of $\log N(\mathfrak{n}/\mathfrak{m})$ is somewhat inconvenient so we replace it by

$$\log N\left(\frac{\mathfrak{n}}{\mathfrak{m}}\right)=\int_{N\mathfrak{m}}^{N\mathfrak{n}}t^{-1}\,dt$$

and then, inverting the order of summation and integration, we arrange $S_1(x)$ into

$$\begin{aligned}S_1(x)&=\sum_{N\mathfrak{m}\leqslant y}\mu(\mathfrak{m})\int_{N\mathfrak{m}}^{x}\bigl(A_{\mathfrak{m}}(x)-A_{\mathfrak{m}}(t)\bigr)t^{-1}\,dt\\ &=\int_1^x\sum_{N\mathfrak{m}\leqslant\min(y,t)}\mu(\mathfrak{m})\bigl(A_{\mathfrak{m}}(x)-A_{\mathfrak{m}}(t)\bigr)t^{-1}\,dt.\end{aligned}$$

Now, we bound the inner sum by

$$\max_t \left| \sum_{N\mathfrak{m} \leqslant \min(y,t)} \mu(\mathfrak{m}) \big( A_{\mathfrak{m}}(x) - A_{\mathfrak{m}}(t) \big) \right|$$

and pull it outside the integral. We deduce that

$$\left|S_1(x)\right| \leqslant 2 \sum_{N\mathfrak{m} \leqslant y} \left|A_{\mathfrak{m}}\big(x'\big)\right| \log x,$$

for some $x' \leqslant x$. Adding the bound for $S_2(x)$ we get

$$\left|S_1(x)\right| + \left|S_2(x)\right| \leqslant 3(\log x) \sum_{N\mathfrak{d} \leqslant y^2} \left|A_{\mathfrak{d}}\big(x'\big)\right|$$

for some $x' \leqslant x$.

We consider the triple sum $S_3(x)$ as a double sum with $\mathfrak{a}$ being one variable and $\mathfrak{b} = \mathfrak{l}\mathfrak{m}$ as the second variable. These variables are weighted by $v_{\mathfrak{a}} = \Lambda(\mathfrak{a})$ and

$$w_{\mathfrak{b}} = \sum_{\mathfrak{m}|\mathfrak{b}, N\mathfrak{m} \leqslant y} \mu(\mathfrak{m}), \quad \text{so } |w_{\mathfrak{b}}| \leqslant \tau(\mathfrak{b}).$$

The variables are restricted by $y < N\mathfrak{a} \leqslant z$ and $N\mathfrak{a}\mathfrak{b} \leqslant x$. Hence, $N\mathfrak{b} \leqslant xy^{-1} = z$. Now we would like to relax the condition $N\mathfrak{a}\mathfrak{b} \leqslant x$ because it ties the two variables together, but still we should be able to recover a slightly weaker condition $N\mathfrak{a}\mathfrak{b} \leqslant 2x$. To this end, we subdivide the range for $N\mathfrak{a}$ into dyadic segments $\frac{1}{2}M < N\mathfrak{a} \leqslant M$ starting with $M = z$. The number of such intervals is no more than $\log z / \log 2$. When $a = N\mathfrak{a}$ is in such an interval then $b = N\mathfrak{b} \leqslant x/a < 2x/M = N$, say. Having recorded that $a \leqslant M, b \leqslant N$ with $M, N \leqslant z$, $MN = 2x$, we remove the condition $ab \leqslant x$ by a standard technique of separation of variables. Lemma 9 of [5] provides us with a function $h(t)$ which satisfies $\int_{-\infty}^{\infty} |h(t)|\, dt \leqslant \log 6x$ and also, for positive integers $k$,

$$\int_{-\infty}^{\infty} h(t) k^{it} dt = \begin{cases} 1 & \text{if } 1 \leqslant k \leqslant x, \\ 0 & \text{if } k > x. \end{cases}$$

We insert this integral, with $k = ab$, as a factor in the summation, allowing us to, in effect, separate the variables $a$ and $b$. We then interchange summation and integration. In this inner summation the coefficients of $\mathfrak{a}$ and $\mathfrak{b}$ are now contaminated by the twists $a^{it}$ and $b^{it}$ for a real $t$. These contaminating factors have absolute value one, hence do not change the bounds for the coefficients $v_{\mathfrak{a}}, w_{\mathfrak{b}}$. The summation now depends on $t$, but we majorize by choosing that $t$ which maximizes the absolute value of the whole sum. Having rendered it independent of $t$, we now pull this absolute value outside the integral, then integrate. The integration costs us a factor $\log 6x$ and, in total, the above operations cost us a loss in the bounds for the coefficients by a factor $(\log z/\log 2)\log 6x \leqslant (\log x/\log 2)\log 6x \leqslant (2\log x)^2$. This completes the proof of (5.5). □

One can show that (5.5) holds with the congruence sums $A_{\mathfrak{d}}(x)$ restricted by $N\mathfrak{d} \leqslant y$. This little improvement can be achieved along the above lines by more careful partitions, however, such a result would have no significance in our applications.

**Proposition 5.2** *Suppose we have fixed numbers* $0 < \vartheta, \theta < 1$ *such that the sequence* $\mathcal{A} = (a_{\mathfrak{n}})$ *with* $|a_{\mathfrak{n}}| \leqslant 1$ *allows the following estimations*:

$$A_{\mathfrak{d}}(x) \ll x^{1-\vartheta+\varepsilon}, \tag{5.6}$$

*for any ideal* $\mathfrak{d}$ *and any* $x \geqslant 2$, *and*

$$\mathcal{B}(M,N) \ll (M+N)^{\theta}(MN)^{1-\theta+\varepsilon}, \tag{5.7}$$

*for any* $M, N \geqslant 2$. *Here* $\varepsilon$ *is any positive number and the implied constants depend only on* $\varepsilon$ *and the field* $K$. *Then, for any* $x \geqslant 2$, *we have*

$$S(x) \ll x^{1-\frac{\vartheta\theta}{2+\theta}+\varepsilon} \tag{5.8}$$

*with any* $\varepsilon > 0$, *the implied constant depending on* $\varepsilon$ *and the field* $K$.

*Proof* Use the bounds $S(z) \ll z = xy^{-1}$, $|\{\mathfrak{d};\, N\mathfrak{d} \leqslant y^2\}| \ll y^2$ and apply (5.5) for $y = x^{\vartheta/(2+\theta)}$. □

We shall verify that (5.6) holds for our sequence of spins in Sect. 6 and (5.7) in Sect. 7.

## 6 Congruence sums in the spin

Recall that $\mathfrak{M}$ is the modulus occurring in the statement of Theorem 1.2. Since we are targeting ideals in a progression modulo $\mathfrak{M}$ it is convenient to introduce the characteristic function on these. We define the function $r(\mathfrak{a}) = r(\mathfrak{a}; \mathfrak{M}, \mu)$, on all integral ideals $\mathfrak{a}$ of $K$ by setting $r(\mathfrak{a}) = 1$ if there exists an integer $\alpha$ of $K$ such that $\mathfrak{a} = (\alpha)$, $\alpha \succ 0$, $\alpha \equiv \mu (\bmod\, \mathfrak{M})$ and we put $r(\mathfrak{a}) = 0$ otherwise. Keep in mind that $r(\mathfrak{a})$ is supported on ideals co-prime with $\mathfrak{M}$, so on odd ideals. Our final goal is to sum the spin of those primes in the support of $r$.

Let $F$ be a fixed positive rational integer which is a multiple of $\mathfrak{M}$ and of $2^{2h+3}f$, where $f$ is given by (3.6) and $h$ is the class number. Let $\mathfrak{m}$ be an ideal, co-prime with its Galois conjugate $\mathfrak{m}'$ and with $F$. We consider

$$A(x) = \sum_{\substack{N\mathfrak{a}\leqslant x \\ (\mathfrak{a},F)=1,\mathfrak{m}|\mathfrak{a}}} r(\mathfrak{a})\,\text{spin}(\mathfrak{a}). \tag{6.1}$$

We suppress, in the notation, the dependence of the congruence sum $A(x)$ on $\mathfrak{M}$, $\mu$, $F$ and $\mathfrak{m}$; however, in the estimations we shall pay attention to uniformity in terms of $\mathfrak{m}$, but not on the other three which are fixed for us. Obviously, $A(x)$ is bounded by the number of all ideals divisible by $\mathfrak{m}$ and having norm $\leqslant x$ so that

$$A(x) \ll \frac{x}{N\mathfrak{m}}. \tag{6.2}$$

Our goal in this section is to prove a much stronger bound for small $N\mathfrak{m}$, by exploiting the cancellation due to the sign change of the spin.

**Proposition 6.1** *Assume Conjecture $C_n$ (see(9.4)). Then, for any $\mathfrak{m}$ with $(\mathfrak{m},\mathfrak{m}'F)=1$ and any $x\geqslant 2$ we have*

$$A(x) \ll x^{1-\frac{\delta}{2n}+\varepsilon}, \tag{6.3}$$

*where the implied constant depends on $\varepsilon$ and the field $K$. The bound (6.3) with exponent $\delta = 1/48$ holds unconditionally for cubic fields.*

We remark that the latter statement follows from the former because, for $n=3$ the conjecture $C_3$ holds true by Burgess' theorem, with exponent $\delta = 1/48$; see Corollary 9.1.

We begin the proof by picking the unique generator of $\mathfrak{a}$, say $\mathfrak{a}=(\alpha)$, with $\alpha \in \mathcal{D}^*$. Recall that, according to our convention, $\alpha \in \mathcal{D}^*$ means

$$\left(\alpha^{(1)},\dots,\alpha^{(n)}\right) \in \mathcal{D}^*. \tag{6.4}$$

Here $\mathcal{D}^*$ denotes the fundamental domain of the group of totally positive units $\mathcal{U}^+ = \mathcal{U}^2$ acting on $\mathbb{R}^n_+$ as in Sect. 4. We do not need to know exactly what the boundary $\mathcal{D}^*\setminus\mathcal{D}$ looks like because the contribution of $\alpha\in\mathcal{D}^*\setminus\mathcal{D}$ is negligible for our purpose. This unique generator $\alpha$ may not be the same as the one equivalent to $\mu$ modulo $\mathfrak{M}$ whose existence is implied by the support of $r(\mathfrak{a})$, so we claim only that $\alpha\equiv\mu u$ for some $u\in\mathcal{U}^+$. Obviously, $u$ is determined up to the units in

$$\mathcal{U}^+_{\mathfrak{M}} = \left\{v\in\mathcal{U}^+;\, v\equiv 1 (\operatorname{mod}\mathfrak{M})\right\}.$$

We split the sum (6.1) over $\alpha \in \mathcal{D}$ into residue classes modulo $F$ getting

$$A(x) = \sideset{}{^\wedge}\sum_{\substack{\rho (\mathrm{mod}\, F)\\ (\rho, F)=1}} A(x;\rho) + \partial A(x), \tag{6.5}$$

where the superscript $\wedge$ restricts the summation to classes $\rho (\mathrm{mod}\, F)$, $\rho \equiv \mu u (\mathrm{mod}\, \mathfrak{M})$ for some $u \in \mathcal{U}^+$,

$$A(x;\rho) = \sum_{\substack{\alpha \in \mathcal{D}, N\alpha \leqslant x\\ \alpha \equiv \rho (\mathrm{mod}\, F)\\ \alpha \equiv 0 (\mathrm{mod}\, \mathfrak{m})}} \mathrm{spin}(\mathfrak{a}), \tag{6.6}$$

and $\partial A(x)$ denotes the contribution of the boundary terms, so

$$\left|\partial A(x)\right| \leqslant \left|\{\alpha \in \bar{\mathcal{D}} \setminus \mathcal{D};\, N\alpha \leqslant x\}\right|.$$

It is easy to estimate $\partial A(x)$ so we do it now. The condition $\alpha \in \bar{\mathcal{D}} \setminus \mathcal{D}$ implies that there is a unit $u \neq 1$ in the finite set $\tilde{\mathcal{U}} \subset \mathcal{U}^+$ defined in (4.8), such that

$$u^{(1)}\alpha^{(1)} + \cdots + u^{(n)}\alpha^{(n)} = \alpha^{(1)} + \cdots + \alpha^{(n)}\,;$$

see (4.8) and the remarks following it.

Returning to the notation of Sect. 3, we consider the fixed integral basis 1, $\omega_2, \ldots, \omega_n$ of $\mathcal{O} \subset K$. Writing $\alpha = a_1 + a_2\omega_2 + \cdots + a_n\omega_n$ in terms of that basis, the above equation becomes

$$\left(u^{(1)} + \cdots + u^{(n)} - n\right)a_1 = \lambda_2 a_2 + \cdots + \lambda_n a_n$$

for certain explicit $\lambda_i \in \mathcal{O}$, independent of $\alpha$. Since the factor in front of $a_1$ is positive (see (3.3)) for $u \neq 1$, the coordinate $a_1$ is determined by the other coordinates $a_2, \ldots, a_n$. However, all the basis co-ordinates are $\ll x^{1/n}$ (see (4.13)), so

$$\partial A(x) \ll x^{1-\frac{1}{n}}, \tag{6.7}$$

where the implied constant depends only on the field $K$. Note that we have abandoned the condition $\alpha \equiv 0 (\mathrm{mod}\, \mathfrak{m})$ losing something in the bound (6.7). This is not a serious issue because the estimates to come will be much weaker than (6.7), anyway.

Next, we are going to estimate every $A(x;\rho)$ separately for the residue classes $\rho (\mathrm{mod}\, F)$, $(\rho, F) = 1$. Returning again to the notation of Sect. 3, we consider the module

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

with rank $\mathbb{M} = n - 1$ and $\mathcal{O} = \mathbb{Z} + \mathbb{M}$. We now write $\alpha$ uniquely as

$$\alpha = a + \beta, \quad \text{with } a \in \mathbb{Z}, \beta \in \mathbb{M}, \tag{6.8}$$

so the summation conditions listed in (6.6) read as follows:

$$a + \beta \in \mathcal{D}, \qquad N(a + \beta) \leqslant x, \tag{6.9}$$

$$a + \beta \equiv \rho (\operatorname{mod} F), \qquad a + \beta \equiv 0 (\operatorname{mod} \mathfrak{m}). \tag{6.10}$$

The congruence conditions show that not every $\beta \in \mathbb{M}$ is admissible because the two residue classes $\beta - \rho (\operatorname{mod} F)$ and $\beta (\operatorname{mod} \mathfrak{m})$ must both be represented by rational integers. Since $(F, \mathfrak{m}) = 1$ we can choose one rational integer $\tilde{a}$ such that

$$\tilde{a} + \beta \equiv \rho (\operatorname{mod} F), \qquad \tilde{a} + \beta \equiv 0 (\operatorname{mod} \mathfrak{m}), \tag{6.11}$$

and we get a single congruence condition for the variable $a$:

$$a \equiv \tilde{a} (\operatorname{mod} F\mathfrak{m}). \tag{6.12}$$

We shall not exploit these properties in any substantial fashion, but rather keep them in mind for consistency in the forthcoming arguments. Moreover, it is also advisable to keep in mind that all the conjugates of $\beta$ satisfy

$$\beta^{(1)}, \ldots, \beta^{(n)} \ll x^{\frac{1}{n}}, \tag{6.13}$$

which follows from (6.9).

From now on we think of $a$ as a variable which satisfies the conditions (6.9) and the congruence (6.12) while $\beta$ is inactive. Therefore, the conditions for $a$ which will emerge from the forthcoming transformations must be articulated rather precisely, but we do not need to be very explicit about the resulting features which depend only on $\beta$. For example, the signs $\pm$ which will come out of various applications of the reciprocity law will be independent of $a$ because $a$ runs over the fixed residue class (6.12).

For $\mathfrak{a} = (\alpha)$ satisfying (6.8)–(6.12) we write

$$\operatorname{spin}(\mathfrak{a}) = \left(\frac{\alpha}{\alpha'}\right) = \left(\frac{a + \beta}{a + \beta'}\right) = \left(\frac{\beta - \beta'}{a + \beta'}\right)$$

by the periodicity. If $\beta = \beta'$ we get no contribution, so we can assume

$$\beta \neq \beta'. \tag{6.14}$$

Next, we are going to interchange the upper entry $\beta-\beta'$ and the lower entry $a+\beta'$ by the reciprocity law. To do so, we first pull out from the ideal $(\beta-\beta')$ all its prime factors in $F$. We can write

$$\big(\beta-\beta'\big)=\big(\eta^2\big)\mathfrak{c}_0\mathfrak{c}_1\mathfrak{c}, \tag{6.15}$$

with $(\mathfrak{c},F)=1$, $\mathfrak{c}_1|F^\infty$, $(\mathfrak{c}_1,2)=1$, $\mathfrak{c}_0|4^h$, where, as before, $h$ is the class number, $\eta\in\mathcal{O}$, $\eta|2^\infty$. (This factorization is not unique but any such choice will lead to the same result for $A(x;\rho)$.)

Let $\mathfrak{C}_0,\mathfrak{C}_1,\mathfrak{C}$ be three of the fixed ideals in $\mathcal{C}\ell$ which represent the inverse classes of $\mathfrak{c}_0,\mathfrak{c}_1,\mathfrak{c}$, respectively, see (3.5)–(3.6). Therefore, $\mathfrak{c}_0\mathfrak{C}_0=(\gamma_0)$, $\mathfrak{c}_1\mathfrak{C}_1=(\gamma_1)$ and $\mathfrak{c}\mathfrak{C}=(\gamma)$. Since $\mathfrak{c}_0\mathfrak{c}_1\mathfrak{c}$ is a principal ideal, so is $\mathfrak{C}_0\mathfrak{C}_1\mathfrak{C}=(\gamma_2)$, say. Choosing appropriate associates we have

$$\beta-\beta'=\eta^2\gamma_0\gamma_1\gamma\gamma_2^{-1}. \tag{6.16}$$

Hence,

$$\left(\frac{\beta-\beta'}{a+\beta'}\right)=\left(\frac{\gamma_0\gamma_1\gamma_2\gamma}{a+\beta'}\right)=\left(\frac{\gamma_0}{a+\beta'}\right)\left(\frac{\gamma_1\gamma_2\gamma}{a+\beta'}\right).$$

Since $(\gamma_0)=\mathfrak{c}_0\mathfrak{C}_0$ divides $F/8$ and $a$ runs over a fixed residue class modulo $F$, the first symbol $(\gamma_0/(a+\beta'))$ does not depend on $a$; see Corollary 2.2. For the second symbol we apply the reciprocity law and obtain

$$\left(\frac{\gamma_1\gamma_2\gamma}{a+\beta'}\right)=\pm\left(\frac{a+\beta'}{\gamma_1\gamma_2\gamma}\right),$$

where, for fixed $\beta$, the sign $\pm$ does not depend on $a$. (This is the case because $a+\beta'$ is in a fixed odd class modulo 8, which suffices to imply that the relevant Hilbert symbols at even places do not depend on $a$. Moreover, at the infinite places the Hilbert symbols are equal to 1 because, by (6.9), $a+\beta$ is totally positive.) Furthermore, we have

$$\left(\frac{a+\beta'}{\gamma_1\gamma_2\gamma}\right)=\left(\frac{a+\beta'}{\mathfrak{c}}\right)\left(\frac{a+\beta'}{\mathfrak{C}_0\mathfrak{c}_1}\right)=\left(\frac{a+\beta'}{\mathfrak{c}}\right)\left(\frac{\tilde{a}+\beta'}{\mathfrak{C}_0\mathfrak{c}_1}\right),$$

because $a\equiv\tilde{a}(\mathrm{mod}\,F)$ and $\mathfrak{C}_0\mathfrak{c}_1|F^\infty$. We conclude that

$$\mathrm{spin}(\mathfrak{a})=\pm\left(\frac{a+\beta'}{\mathfrak{c}}\right), \tag{6.17}$$

where the $\pm$ sign does not depend on $a$ and where $\mathfrak{c}$ denotes the part of the ideal $(\beta-\beta')$ free of divisors of $F$, that is

$$\mathfrak{c}=\mathfrak{c}(\beta)=\big(\beta-\beta'\big)/\big(\beta-\beta',F^\infty\big). \tag{6.18}$$

Hence, $A(x;\rho)$ splits as follows:

$$A(x;\rho)=\sum_{\beta\in\mathbb{M}}\pm T(x;\beta), \tag{6.19}$$

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

$$T(x;\beta)=\sum_{a}{}^{\flat}\left(\frac{a+\beta'}{\mathfrak{c}}\right). \tag{6.20}$$

Here, the symbol $\flat$ means that $a$ runs over the rational integers satisfying the conditions (6.9) and the congruence (6.12). Of course, these conditions impose some restrictions on $\beta\in\mathbb{M}$. For example, (6.11) and (6.13) must hold or else the summation (6.20) is void. At this point we do not need to be very specific about the exact conditions for $\beta$.

We proceed to the estimation of $T(x;\beta)$. Our intention is to replace $\beta'$ in the upper entry of the symbol by a rational integer modulo $\mathfrak{c}$. This however may not be possible if the ideal $\mathfrak{c}$ contains prime divisors of degree greater than one. For this reason, we factor $\mathfrak{c}$ into

$$\mathfrak{c}=\mathfrak{g}\mathfrak{q}, \tag{6.21}$$

where $\mathfrak{g}$ takes from $\mathfrak{c}$ all prime ideals of degree greater than one, all ramified primes, and all unramified primes of degree one for which some different conjugate is also a factor of $\mathfrak{c}$. For $\mathfrak{q}$ taking the rest, note that $q=N\mathfrak{q}$ is a square-free number and norm $g=N\mathfrak{g}$ is a squarefull number co-prime with $q$. Let $b$ be a rational integer with $b\equiv\beta'(\bmod q)$. This exists because $q=N\mathfrak{q}$ is square-free. Note that $b$ is a rational integer which depends on $\beta$ but not on $a$. We have

$$\left(\frac{a+\beta'}{\mathfrak{c}}\right)=\left(\frac{a+\beta'}{\mathfrak{g}}\right)\left(\frac{a+\beta'}{\mathfrak{q}}\right)=\left(\frac{a+\beta'}{\mathfrak{g}}\right)\left(\frac{a+b}{\mathfrak{q}}\right).$$

Let $g_0$ be the product of all distinct prime divisors of $g$,

$$g_0=\prod_{p\mid g}p. \tag{6.22}$$

The quadratic residue symbol $(\alpha/\mathfrak{g})$ is periodic in $\alpha$ modulo $\mathfrak{g}^*=\prod_{\mathfrak{p}\mid\mathfrak{g}}\mathfrak{p}$, hence it is periodic in $\alpha$ modulo $g_0$ because $\mathfrak{g}^*$ divides $g_0$. Therefore, the symbol $((a+\beta')/\mathfrak{g})$ as a function of $a$ is periodic of period $g_0$. Splitting the sum (6.20) into residue classes modulo $g_0$, we get

$$T(x;\beta)\leqslant\sum_{a_0(\bmod g_0)}\left|\sum_{a\equiv a_0(\bmod g_0)}{}^{\flat}\left(\frac{a+b}{\mathfrak{q}}\right)\right|. \tag{6.23}$$

Recall that the superscript $\flat$ indicates that the summation variable $a$ satisfies the conditions (6.9), (6.12). These conditions imply

$$a \ll x^{\frac{1}{n}}, \tag{6.24}$$

but we have to describe these conditions much more precisely. The first condition $\alpha = a + \beta \in \mathcal{D}$ is described by a system of linear inequalities $u \cdot \alpha > e \cdot \alpha$ for every $u \in \tilde{\mathcal{U}}$, where $\tilde{\mathcal{U}}$ is a finite subset of $\mathcal{U}^+$. Hence, this condition means that $a$ runs over a single open interval whose endpoints depend on $\beta$. Next, we observe that the polynomial $(X + \beta^{(1)}) \cdots (X + \beta^{(n)})$ has real coefficients, so the second condition $N(a + \beta) \leqslant x$ means that $a$ runs over a collection of $n$ segments whose endpoints depend on $\beta$ and $x$. Therefore, the simultaneous conditions in (6.9) can be expressed by saying that $a$ runs over a certain collection of $n$ intervals.

Finally, the congruence (6.12), together with $a \equiv a_0 (\operatorname{mod} g_0)$, means that $a$ runs over a certain arithmetic progression of modulus $k$ which divides $g_0 F N \mathfrak{m}$. We can assume that $m = N\mathfrak{m}$ and $q = N\mathfrak{q}$ are co-prime. If not, there is a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} | \mathfrak{m}'$ and $\mathfrak{p} | q$. Let $\mathfrak{p}^\tau$ be a conjugate of $\mathfrak{p}$ which divides the ideal $\mathfrak{q}$. Then, the quadratic residue symbol in (6.23) factors as follows:

$$\left(\frac{a+b}{\mathfrak{q}}\right) = \left(\frac{a+b}{\mathfrak{p}^\tau}\right) \cdots = \left(\frac{a+b}{\mathfrak{p}}\right) \cdots = \left(\frac{a+\beta'}{\mathfrak{p}}\right) \cdots = 0$$

because $b \equiv \beta' (\operatorname{mod} q)$ and $\tilde{a} + \beta' \equiv 0 (\operatorname{mod} \mathfrak{m}')$. Since $g_0, F$ are also co-prime with $q$, we have $(g_0 F m, q) = 1$ so $a$ in (6.23) runs over an arithmetic progression of modulus $k$ which is co-prime with $q$.

Having said these things, we see that the inner sum in (6.23) can be arranged as the sum of $n$ sums, each of which runs over a single segment of an arithmetic progression of length $\ll x^{1/n}$. Since $\chi_\mathfrak{q}(\ell) = (\ell/\mathfrak{q})$ is a real Dirichlet character of modulus $q = N\mathfrak{q}$ (see (3.17) and Lemma 3.6) we have here $n$ incomplete character sums of length $\ll x^{1/n}$ and the modulus $q \ll x$ of the character is co-prime to the modulus $k$ of the progression. Therefore, if $q$ is not squarefull, Conjecture $C_n$ applies, (or rather its consequence for arithmetic progressions as described at the end of Sect. 9), giving (see (9.4)),

$$T(x; \beta) \ll g_0 x^{\frac{1-\delta}{n} + \varepsilon}. \tag{6.25}$$

Here, the implied constant depends only on $\varepsilon$ and the field $K$ but not on $\beta$. Perhaps the reader is wondering why the implied constant in (6.25) does not depend on $\beta$, although many steps before we arrived there depend on $\beta$. The answer is that the estimate (9.4) in Conjecture $C_n$ holds for any incomplete character sum, regardless of the location of the segment where the summation takes place. This feature is really vital for our application because in (6.23) we have no idea where $b$, the rational representative of $\beta'$ modulo $\mathfrak{q}$, can be in relation to $q = N\mathfrak{q}$.

Recall that (6.25) holds provided $q = N\mathfrak{q}$ is not squarefull. However, if $q$ is squarefull, then $q = 1$ and

$$F^2 N\big(\beta - \beta'\big) \quad \text{is squarefull.} \tag{6.26}$$

The condition (6.26) is satisfied very rarely, so we can count crudely. Denote by $A_\Box(x;\rho)$ the contribution to $A(x;\rho)$ of the terms for which (6.26) holds. We can afford to ignore the congruence conditions (6.10). We have

$$A_\Box(x;\rho) \leqslant \big|\big\{\alpha \in \mathcal{D};\, N\alpha \leqslant x,\, F^2 N\big(\beta - \beta'\big) \text{ squarefull}\big\}\big|.$$

Since $\alpha \in \mathcal{D}$, $N(\alpha) \leqslant x$ all the conjugates $\alpha^{(k)}$ are $\ll x^{1/n}$. Hence, $|a| \leqslant y$ and all the conjugates of $\gamma = \beta - \beta' = \alpha - \alpha'$ satisfy $|\gamma^{(k)}| \leqslant y$ for some $y \asymp x^{1/n}$. Recall that the map $\mathbb{M} \to \mathcal{O}$ given by $\beta \to \beta - \beta'$ is injective (see Lemma 3.2). Therefore, we have

$$A_\Box(x;\rho) \leqslant y\big|\big\{\gamma \in \mathcal{O};\, \big|\gamma^{(k)}\big| \leqslant y,\, F^2 N(\gamma) \text{ squarefull}\big\}\big|.$$

Here, we can replace the counting of integers $\gamma$ by the counting of the principal ideals they generate, each integer occurring with multiplicity $\ll (\log x)^n$ by Lemma 3.8. Hence

$$A_\Box(x;\rho) \ll x^{\frac{1}{n}} (\log x)^n \big|\big\{\mathfrak{b} \subset \mathcal{O};\, N\mathfrak{b} \leqslant X,\, F^2 N\mathfrak{b} \text{ squarefull}\big\}\big|,$$

where $X = y^n$ so $X \asymp x$. Note that we have moved from the integers in the submodule $\mathbb{L} \subset \mathcal{O}$ (see Sect. 3) to the ideals in $\mathcal{O}$ because detecting squarefull norms in a submodule of lower rank could be very difficult. Fortunately, we can afford the loss which results from this extension because $n \geqslant 3$. Now, we can exploit the multiplicative structure of the ideals in $\mathcal{O}$ which gives us the bound

$$A_\Box(x;\rho) \ll x^{\frac{1}{n}} (\log x)^n \sum_{\substack{b \leqslant X \\ F^2 b \text{ squarefull}}} \tau_n(b),$$

where $b$ runs over positive rational integers and $\tau_n(b)$ denotes the divisor function of degree $n$ so that $\tau_n(b) \ll b^\varepsilon$. Hence, we conclude

$$A_\Box(x;\rho) \ll x^{\frac{1}{2} + \frac{1}{n} + \varepsilon}, \tag{6.27}$$

where the implied constant depends on $\varepsilon$ and the field $K$.

Let $A_0(x;\rho)$ be the contribution to $A(x;\rho)$ of the terms $\alpha = a + \beta$ for which (6.26) does not hold. Therefore, we have the following partition:

$$A(x;\rho) = A_{\Box}(x;\rho) + A_0(x;\rho) \tag{6.28}$$

To estimate $A_0(x;\rho)$ we can use (6.25) for every relevant $\beta$, but the bound (6.25) is useless for $g_0$ too large. Therefore, we make the further partition

$$A_0(x;\rho) = A_1(x;\rho) + A_2(x;\rho) + A_3(x;\rho), \tag{6.29}$$

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

$$g_0 \leqslant Z \quad \text{in } A_1(x;\rho), \tag{6.30}$$

$$g_0 > Z, \qquad g \leqslant Y \quad \text{in } A_2(x;\rho), \tag{6.31}$$

$$g_0 > Z, \qquad g > Y \quad \text{in } A_3(x;\rho). \tag{6.32}$$

We shall choose $Z \leqslant Y$ later.

To estimate $A_1(x;\rho)$ we use (6.25) and then sum over $\beta \in \mathbb{M}$ satisfying (6.13), ignoring the other restrictions. This gives

$$A_1(x;\rho) \ll Z x^{1-\frac{\delta}{n}+\varepsilon}. \tag{6.33}$$

The estimation of $A_3(x;\rho)$ is also very quick. We treat $A_3(x;\rho)$ by arguments similar to those we applied to $A_{\Box}(x;\rho)$. The condition that $F^2N(\gamma)$ is squarefull is now replaced by $g|N(\gamma)$. Hence,

$$\begin{aligned} A_3(x;\rho) &\ll x^{\frac{1}{n}}(\log x)^n \sum_{\substack{g>Y \\ g \text{ squarefull}}} \sum_{\substack{b \leqslant X \\ g|b}} \tau_n(b) \\ &\ll x^{1+\frac{1}{n}+\varepsilon} \sum_{\substack{Y<g\leqslant x \\ g \text{ squarefull}}} g^{-1}. \end{aligned}$$

This last sum is estimated by

$$Y^{-\frac{1}{2}} \sum_{\substack{g\leqslant x \\ g \text{ squarefull}}} g^{-\frac{1}{2}} \leqslant Y^{-\frac{1}{2}} \prod_{p\leqslant x} \left(1 + \frac{1}{p}\left(1 - \frac{1}{\sqrt{p}}\right)^{-1}\right) \ll Y^{-\frac{1}{2}} \log x.$$

Hence, we conclude that

$$A_3(x;\rho) \ll Y^{-\frac{1}{2}} x^{1+\frac{1}{n}+\varepsilon}. \tag{6.34}$$

It remains to estimate $A_2(x;\rho)$ which is quite a difficult job. If, along the lines of the proof of (6.34), we had not wasted the information that $\beta-\beta'$ is in a submodule $\mathbb{L}\subset\mathcal{O}$ of rank $n-1$, then the factor $x^{1/n}$ in (6.34) would be saved, so the result would be useful for $Y>x^{\delta}$ and there would be no need to consider the sum $A_2(x;\rho)$ over the middle range (6.31). But, it is difficult to take this information into account when $g=N\mathfrak{g}$ is quite large. We are now going to exploit this information for the estimation of $A_2(x;\rho)$ but the arguments need to be more delicate.

We begin with the arguments that were applied to $A_3(x;\rho)$ but keep the condition $\gamma=\beta-\beta'\equiv 0(\operatorname{mod}\mathfrak{g})$ in place of $N(\gamma)\equiv 0(\operatorname{mod} g)$. We obtain

$$\left|A_2(x;\rho)\right|\leqslant y\sum_{\substack{\mathfrak{g}\\ g_0>Z,g\leqslant Y}}E_{\mathfrak{g}}(y),\tag{6.35}$$

where $y\asymp x^{1/n}$ and

$$E_{\mathfrak{g}}(y)=\left|\left\{\gamma\in\mathbb{L};\gamma\equiv 0(\operatorname{mod}\mathfrak{g}),\left|\gamma^{(k)}\right|\leqslant y\text{ for all }k\right\}\right|.$$

Recall that $\mathfrak{g}$ (see (6.21)) runs over ideals, all of whose prime factors have degree greater than one or, if of degree one, have another prime factor of the same norm, that $g=N\mathfrak{g}$ and $g_0$ is the product of all the distinct primes in $g$. Note that every prime ideal dividing $\mathfrak{g}$ also divides $g_0$.

For the estimation of $E_{\mathfrak{g}}(y)$ we express every $\gamma$ in terms of the basis $\eta_2,\dots,\eta_n$ of $\mathbb{L}$, getting $\gamma=a_2\eta_2+\cdots+a_n\eta_n$ with integer coefficients $a_2,\dots,a_n$ satisfying

$$a_2,\dots,a_n\ll y,\tag{6.36}$$

$$a_2\eta_2+\cdots+a_n\eta_n\equiv 0(\operatorname{mod}\mathfrak{g}).\tag{6.37}$$

Next, we split the coefficients $a_2,\dots,a_n$ according to their residue classes modulo $g_0$, say $r_2,\dots,r_n$. For each unramified prime $\mathfrak{p}|\mathfrak{g}$ of degree greater than one we take an automorphism $\tau\neq\mathrm{id}$ such that $\mathfrak{p}^{\tau}=\mathfrak{p}$. Such a $\tau$ exists (in the decomposition group of the prime $\mathfrak{p}$), because $\deg\mathfrak{p}=f>1$. Then, (6.37) yields two different congruences modulo $\mathfrak{p}$:

$$\begin{aligned}r_2\eta_2+\cdots+r_n\eta_n&\equiv 0(\operatorname{mod}\mathfrak{p}),\\ r_2\eta_2^{\tau}+\cdots+r_n\eta_n^{\tau}&\equiv 0(\operatorname{mod}\mathfrak{p}).\end{aligned}\tag{6.38}$$

For each unramified prime $\mathfrak{p}$ dividing $\mathfrak{g}$ of degree one there exists a companion $\mathfrak{p}^{\tau^{-1}}\neq\mathfrak{p}$ which also divides $\mathfrak{g}$. Then, (6.37) yields one congruence modulo $\mathfrak{p}\mathfrak{p}^{\tau^{-1}}$:

$$r_2\eta_2+\cdots+r_n\eta_n\equiv 0\big(\operatorname{mod}\mathfrak{p}\mathfrak{p}^{\tau^{-1}}\big).$$

This single congruence yields the same system (6.38).

By Lemma 3.4 we have $\eta_k\eta_\ell^\tau \neq \eta_k^\tau\eta_\ell$ for some $2 \leqslant k \neq \ell \leqslant n$. Hence, if $\mathfrak{p}$ does not divide $\mathfrak{h}$ (see the definition of the ideal $\mathfrak{h}$ in (3.16))

$$\eta_k\eta_\ell^\tau - \eta_k^\tau\eta_\ell \not\equiv 0 (\operatorname{mod} \mathfrak{p}),$$

so $r_k, r_\ell$ are determined uniquely modulo $\mathfrak{p}$ by the other residue classes. But $r_k, r_\ell$ are rational so they are determined uniquely modulo every prime ideal which is a conjugate of $\mathfrak{p}$. Hence, by the Chinese Remainder Theorem, $r_k, r_\ell$ are determined uniquely modulo $p$ for every $p|g_0$, $p$ co-prime with $h = N\mathfrak{h}$, because $p$ is the product of distinct conjugates of $\mathfrak{p}$. Thus,

$$\left|\left\{r_2, \dots, r_n (\operatorname{mod} p) \text{ admissible}\right\}\right| = p^{n-3}.$$

For the primes $p|h$ we use the trivial bound $p^{n-1}$, so the total number of admissible residue classes satisfies

$$\left|\left\{r_2, \dots, r_n (\operatorname{mod} g_0) \text{ admissible}\right\}\right| \ll g_0^{n-3}, \tag{6.39}$$

where the implied constant depends only on the field $K$. Hence, the number of coefficients $a_2, \dots, a_n$ satisfying (6.36) and (6.37) is bounded by

$$g_0^{n-3}\left(yg_0^{-1} + 1\right)^{n-1} \ll y^{n-1}g_0^{-2} + g_0^{n-3},$$

and so

$$E_{\mathfrak{g}}(y) \ll y^{n-1}g_0^{-2} + g_0^{n-3}. \tag{6.40}$$

Introducing (6.40) into (6.35) we obtain

$$\left|A_2(x;\rho)\right| \ll \sum_{\substack{\mathfrak{g} \\ g_0 > Z, g \leqslant Y}} \left(y^n g_0^{-2} + yg_0^{n-3}\right).$$

The number of ideals $\mathfrak{g}$ with $N\mathfrak{g} = g$ is bounded by $\tau(g) \ll Y^\varepsilon$. Hence,

$$\left|A_2(x;\rho)\right| \ll x^\varepsilon \sum_{\substack{g \text{ squarefull} \\ g_0 > Z, g \leqslant Y}} \left(xg_0^{-2} + x^{\frac{1}{n}}g_0^{n-3}\right),$$

where $g_0$ is the product of all distinct prime divisors of $g$.

We estimate the first sum as follows:

$$\sum_g g_0^{-2} \leqslant Z^{-1}\sum_g g_0^{-1} \leqslant Z^{-1}\prod\left(1 + \frac{1}{p}\left(1 - \frac{1}{p}\right)^{-1}\right) \ll Z^{-1}\log Y.$$

In the second sum we use the fact that $g_0^2|g$, so $g_0 \leqslant \sqrt{g} \leqslant \sqrt{Y}$, whence

$$\sum_g g_0^{n-3} \leqslant Y^{\frac{n-3}{2}} \sum_{\substack{g \text{ squarefull} \\ g \leqslant Y}} 1 \ll Y^{\frac{n}{2}-1}.$$

We conclude that

$$A_2(x;\rho) \ll Z^{-1}x^{1+\varepsilon} + Y^{\frac{n}{2}-1}x^{\frac{1}{n}+\varepsilon}, \tag{6.41}$$

where the implied constant depends on $\varepsilon$ and the field $K$.

Inserting the three estimates, (6.33), (6.34), (6.41), into (6.29), we deduce that

$$A_0(x;\rho) \ll x^{\varepsilon}\big(Zx^{1-\frac{\delta}{n}} + Y^{-\frac{1}{2}}x^{1+\frac{1}{n}} + Z^{-1}x + Y^{\frac{n}{2}-1}x^{\frac{1}{n}}\big),$$

where $Z \leqslant Y$ are at our disposal. We choose $Z = x^{\delta/2n}$ and $Y = x^{2/(n-1)}$, getting

$$A_0(x;\rho) \ll x^{1-\frac{\delta}{2n}+\varepsilon}. \tag{6.42}$$

Adding to (6.42) the bound (6.27), we find that (6.42) holds also for $A(x;\rho)$. Finally, summing this bound over the residue classes $\rho(\operatorname{mod} F)$ and adding the bound (6.7), we complete the proof of the bound (6.3), that is Proposition 6.1.

## 7 Bilinear forms with spin

Let $F$ be a fixed positive integer which is a multiple of $\mathfrak{M}$ and $\mathfrak{f}$ (see (3.6)). We consider a general bilinear form

$$\mathcal{B}(x,y) = \sum\sum_{\substack{(\mathfrak{a}\mathfrak{b},F)=1 \\ N\mathfrak{a}\leqslant x, N\mathfrak{b}\leqslant y}} v_{\mathfrak{a}} w_{\mathfrak{b}} r(\mathfrak{a}\mathfrak{b}) \operatorname{spin}(\mathfrak{a}\mathfrak{b}), \tag{7.1}$$

where $v_{\mathfrak{a}}, w_{\mathfrak{b}}$ are arbitrary complex numbers with $|v_{\mathfrak{a}}| \leqslant 1$, $|w_{\mathfrak{b}}| \leqslant 1$. Recall that the factor $r(\mathfrak{a}\mathfrak{b})$ means that $\mathfrak{a}\mathfrak{b}$ is a principal ideal which has a totally positive generator in the residue class $\mu$ modulo $\mathfrak{M}$.

**Proposition 7.1** *Let $K/\mathbb{Q}$ be a totally real Galois extension of degree $n \geqslant 3$. Then,*

$$\mathcal{B}(x,y) \ll (x+y)^{\frac{1}{6n}}(xy)^{1-\frac{1}{6n}+\varepsilon} \tag{7.2}$$

*for any $x, y \geqslant 2$ and $\varepsilon > 0$, the implied constant depending only on $\varepsilon$ and the field $K$.*

*Proof* Since the coefficients $v_{\mathfrak{a}}, w_{\mathfrak{b}}$ are arbitrary, we can assume without loss of generality that they are supported on fixed ideal classes, say

$$\mathfrak{a}\mathfrak{A} = (\alpha), \quad \alpha \succ 0, \tag{7.3}$$

$$\mathfrak{b}\mathfrak{B} = (\beta), \quad \beta \succ 0, \tag{7.4}$$

as in (3.7), with $\mathfrak{A} \neq \mathfrak{B}$. Furthermore we can assume that $\alpha, \beta$ have fixed residue classes modulo 8. Then, spin$(\mathfrak{a}\mathfrak{b})$ factors as in (3.8). The middle symbols in (3.8) separate $\mathfrak{a}$ from $\mathfrak{b}$ so they can be attached to the coefficients $v_{\mathfrak{a}}, w_{\mathfrak{b}}$. Hence we have

$$\left|\mathcal{B}(x,y)\right| \leqslant \sum_{\substack{(\mathfrak{a},F)=1 \\ N\mathfrak{a}\leqslant x}} \left| \sum_{\substack{(\mathfrak{b},F)=1 \\ N\mathfrak{b}\leqslant y}} w_{\mathfrak{b}} \left(\frac{\alpha}{\mathfrak{b}'\mathfrak{b}^-}\right)\right|.$$

Here, the coefficients $v_{\mathfrak{a}}$ have disappeared and $w_{\mathfrak{b}}$ are complex numbers with $|w_{\mathfrak{b}}| \leqslant 1$, not necessarily the original ones in (7.1). Note that we camouflaged the fact that $\mathfrak{b}$ satisfies (7.4) by incorporating this information into the coefficients $w_{\mathfrak{b}}$ because we no longer will make any use of this. Note also that the characteristic function $r(\mathfrak{a}\mathfrak{b})$ has disappeared for the same reason. Moreover, we do not need all the information about the ideal $\mathfrak{a}$ coming from (7.3) but we must keep (7.3) in mind for a while until the relation of $\alpha$ being a function of $\mathfrak{a}$ disappears.

Our strategy is to create another bilinear form, one in which the variables have very different sizes. To this end we apply a high power Hölder inequality and use the multiplicativity of the quadratic residue symbol with respect to the modulus, which holds by definition. We obtain

$$\left|\mathcal{B}(x,y)\right|^k \leqslant \mathcal{N}(x)^{k-1} \sum_{\substack{(\mathfrak{a},F)=1 \\ N\mathfrak{a}\leqslant x}} \left| \sum_{\substack{(\mathfrak{b},F)=1 \\ N\mathfrak{b}\leqslant y}} w_{\mathfrak{b}} \left(\frac{\alpha}{\mathfrak{b}'\mathfrak{b}^-}\right)\right|^k,$$

where $\mathcal{N}(x)$ is the number of ideals $\mathfrak{a}$ with $N\mathfrak{a} \leqslant x$, so $\mathcal{N}(x) \ll x$. Here, $k$ is a positive integer to be chosen later, not necessarily even. Next, we get

$$\sum_{\mathfrak{a}} \left| \sum_{\mathfrak{b}} \right|^k \leqslant \sum_{(\mathfrak{c},F)=1} \left| \sum_{\substack{(\mathfrak{a},F)=1 \\ N\mathfrak{a}\leqslant x}} \varepsilon(\mathfrak{a}) \left(\frac{\alpha}{\mathfrak{c}'\mathfrak{c}^-}\right)\right|,$$

where $|\varepsilon(\mathfrak{a})| = 1$ (precisely, $\bar{\varepsilon}(\mathfrak{a})$ is the $k$-th power of the complex sign of the inner sum over $\mathfrak{b}$), and $\mathfrak{c} = \mathfrak{b}_1 \cdots \mathfrak{b}_k$ with $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ running independently over all ideals of norm $\leqslant y$. Therefore, $N\mathfrak{c} \leqslant y^k = Y$, say, and the number of representations of $\mathfrak{c}$ as the product of $k$ ideals is $\tau_k(\mathfrak{c}) \ll y^\varepsilon$. Hence we find

$$\left|\mathcal{B}(x,y)\right|^k \ll y^\varepsilon x^{k-1} \sum_{\substack{(\mathfrak{c},F)=1\\ N\mathfrak{c}\leqslant Y}} \left| \sum_{\substack{(\mathfrak{a},F)=1\\ N\mathfrak{a}\leqslant x}} \varepsilon(\mathfrak{a}) \left(\frac{\alpha}{\mathfrak{c}'\mathfrak{c}^-}\right) \right|,$$

where the implied constant depends on $\varepsilon, k$ and the field $K$. At this point our mission is accomplished because, if $k$ is sufficiently large, then $Y = y^k$ is much larger than $x$. To take advantage of this disproportion of the sizes of $\mathfrak{c}$ and $\mathfrak{a}$, we intend to execute the summation over $\mathfrak{c}$ first while holding $\mathfrak{a}$ inactive. This requires however an interchange of the positions of $\mathfrak{c}$ and $\mathfrak{a}$ which can be accomplished by the reciprocity law, followed by an application of Cauchy's inequality.

For the use of the reciprocity law we must split $\mathfrak{c}$ into ideal classes and, for each class, treat the corresponding sum separately. Let this class be determined by

$$\mathfrak{c}\mathfrak{C} = (\gamma), \quad \gamma \succ 0, \tag{7.5}$$

where $\mathfrak{C} \in \mathcal{C}\ell$ is the chosen ideal which is different from $\mathfrak{A}$ in (7.3). Such a choice is possible because every ideal class has two representatives in $\mathcal{C}\ell$. Note that $N\mathfrak{C}$ is co-prime with $N\mathfrak{A}$ because of (3.6). Actually, if we kept the information (7.4) throughout, then we would already know the ideal class of $\mathfrak{c}$, namely the inverse class of $\mathfrak{B}^k$, but this information would not save us much work. Thus, we appeal to (7.5) to obtain

$$\left(\frac{\alpha}{\mathfrak{c}'\mathfrak{c}^-}\right) = \left(\frac{\alpha}{\gamma'\gamma^-}\right)\left(\frac{\alpha}{\mathfrak{C}'\mathfrak{C}^-}\right) = \pm\left(\frac{\gamma'\gamma^-}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{C}'\mathfrak{C}^-}\right),$$

where the sign $\pm$ depends only on the residue classes of $\alpha, \gamma$ modulo 8. Hence,

$$\left|\mathcal{B}(x,y)\right|^k \ll y^\varepsilon x^{k-1} \sum_{\substack{(\mathfrak{c},F)=1\\ N\mathfrak{c}\leqslant Y}} \left| \sum_{\substack{(\mathfrak{a},F)=1\\ N\mathfrak{a}\leqslant x}} \varepsilon(\mathfrak{a}) \left(\frac{\gamma'\gamma^-}{\mathfrak{a}}\right) \right|,$$

where $|\varepsilon(\mathfrak{a})| = 1$. Here, we did not display the sign $\pm$ because its dependence on $\gamma \pmod 8$ disappears by the positivity argument in our summation and its dependence on $\alpha \pmod 8$ is absorbed by the floating coefficient $\varepsilon(\mathfrak{a})$.

Now, we can forget the condition (7.3) for $\mathfrak{a}$, which we had kept in mind until now, by building it into the coefficient $\varepsilon(\mathfrak{a})$. We could not have done this earlier because $\alpha$, the generator of $\mathfrak{a}\mathfrak{A}$ was present in the quadratic residue symbol.

If we require in (7.5), as we may, that $\gamma$ belong to the fundamental domain $\mathcal{D}^*$, then there is a one-to-one correspondence between $\mathfrak{c}$ and $\gamma$ with $\gamma \equiv 0 (\operatorname{mod} \mathfrak{C})$. Hence,

$$\left|\mathcal{B}(x,y)\right|^k \ll y^\varepsilon x^{k-1} \mathcal{E}(X,x), \tag{7.6}$$

where

$$\mathcal{E}(X,x) = \sum_{\substack{\gamma \in \bar{\mathcal{D}} \\ N\gamma \leqslant X}} \left| \sum_{\substack{\mathfrak{a} \text{ odd} \\ N\mathfrak{a} \leqslant x}} \varepsilon(\mathfrak{a}) \left( \frac{\gamma' \gamma^-}{\mathfrak{a}} \right) \right|, \tag{7.7}$$

where $X = YF$. Note that we ignored the conditions $(\gamma, F) = 1, \gamma \equiv 0 (\operatorname{mod} \mathfrak{C})$ and extended $\mathcal{D}^*$ to its closure $\bar{\mathcal{D}}$ as we may, by positivity. Have in mind that $F$ is a constant, depending on the field $K$, so that $X \asymp Y = y^k$.

Applying Cauchy's inequality and changing the order of summation, we arrive at

$$\begin{aligned} \left|\mathcal{E}(X,x)\right|^2 &\leqslant \Bigg( \sum_{\substack{\gamma \in \bar{\mathcal{D}} \\ N\gamma \leqslant X}} 1 \Bigg) \sum_{\substack{\mathfrak{q} \text{ odd} \\ N\mathfrak{q} \leqslant x^2}} \left| \sum_{\mathfrak{a}_1 \mathfrak{a}_2 = \mathfrak{q}} \varepsilon(\mathfrak{a}_1) \bar{\varepsilon}(\mathfrak{a}_2) \sum_{\substack{\gamma \in \bar{\mathcal{D}} \\ N\gamma \leqslant X}} \left( \frac{\gamma' \gamma^-}{\mathfrak{q}} \right) \right| \\ &\ll X \sum_{\substack{\mathfrak{q} \text{ odd} \\ N\mathfrak{q} \leqslant x^2}} \tau(\mathfrak{q}) \left| \Sigma_{\mathfrak{q}}(X) \right|. \end{aligned} \tag{7.8}$$

Here, $\tau(\mathfrak{q})$ gives a bound for the number of representations $\mathfrak{q} = \mathfrak{a}_1 \mathfrak{a}_2$ and

$$\Sigma_{\mathfrak{q}}(X) = \sum_{\substack{\gamma \in \bar{\mathcal{D}} \\ N\gamma \leqslant X}} \left( \frac{\gamma' \gamma^-}{\mathfrak{q}} \right). \tag{7.9}$$

Let $q = N\mathfrak{q}$ be the norm of $\mathfrak{q}$. Note that the diagonal terms $\mathfrak{a}_1 = \mathfrak{a}_2$ are covered by this case. If $q$ is squarefull, we apply the trivial bound

$$\Sigma_{\mathfrak{q}}(X) \ll X.$$

If $q$ is not squarefull, that is $q$ has a prime factor $p$ whose square does not divide $q$, we split $\Sigma_{\mathfrak{q}}(X)$ into residue classes modulo $\mathfrak{q}$:

$$\Sigma_{\mathfrak{q}}(X) = \sum_{\nu (\operatorname{mod} \mathfrak{q})} \left( \frac{\nu' \nu^-}{\mathfrak{q}} \right) \mathcal{N}(x; \mathfrak{q}, \nu).$$

By Lemma 4.6 we obtain

$$\Sigma_{\mathfrak{q}}(X) = \frac{\mathcal{N}(x)}{q} \sum_{\nu \,(\mathrm{mod}\, \mathfrak{q})} \left(\frac{\nu' \nu^-}{\mathfrak{q}}\right) + O\left(q X^{1-\frac{1}{n}}\right).$$

Here, the complete sum over $\nu(\mathrm{mod}\, \mathfrak{q})$ is equal to $q^{-1}$ times the complete sum over $\alpha(\mathrm{mod}\, \mathfrak{q}'\mathfrak{q}^-)$ in (3.11), so it vanishes and we are left with

$$\Sigma_{\mathfrak{q}}(X) \ll q X^{1-\frac{1}{n}}.$$

Hence, by (7.8) we derive

$$\begin{aligned} \left|\mathcal{E}(X,x)\right|^2 &\ll X^2 \sum_{\substack{N\mathfrak{q} \leqslant x^2 \\ N\mathfrak{q} \text{ squarefull}}} 1 + X^{2-\frac{1}{n}} \sum_{N\mathfrak{q} \leqslant x^2} \tau(\mathfrak{q}) q \\ &\ll y^{2k}\left(x + y^{-k/n} x^4\right) x^{\varepsilon}, \end{aligned}$$

so that

$$\mathcal{E}(X,x) \ll y^k \left(x^{1/2} + y^{-k/2n} x^2\right) x^{\varepsilon}. \tag{7.10}$$

Inserting the result into (7.6), we find that

$$\mathcal{B}(x,y) \ll (xy)^{1+\varepsilon}\left(x^{-1/2k} + y^{-1/2n} x^{1/k}\right).$$

We choose $k = 3n$, obtaining

$$\begin{aligned} \mathcal{B}(x,y) &\ll (xy)^{1+\varepsilon}\left(x^{-1/6n} + y^{-1/2n} x^{1/3n}\right) \\ &< (xy)^{1-1/6n+\varepsilon} (x+y)^{1/6n} \left(1 + y^{-1} x\right)^{1/3n}. \end{aligned}$$

By the symmetry of the bilinear form we can assume that $x \leqslant y$, getting (7.2). □

## 8 Conclusion of proof

We now have all the pieces for the application of Proposition 5.2 to the sum of the spins of prime ideals. Specifically, we apply Proposition 5.2 for the sequence $\mathcal{A} = (a_{\mathfrak{n}})$ with $a_{\mathfrak{n}} = 1$ if $(\mathfrak{n}, F) = 1$, $\mathfrak{n} = (\alpha)$, $\alpha \succ 0$, $\alpha \equiv \mu (\mathrm{mod}\, \mathfrak{M})$ and $a_{\mathfrak{n}} = 0$ otherwise.

First, (6.3) gives us (5.6) with $\vartheta = \delta/2n$. Next, (7.2) gives us (5.7) with $\theta = 1/6n$. Therefore, (5.8) becomes

$$\sum_{\substack{N\mathfrak{n} \leqslant x \\ (\mathfrak{n}, F) = 1}} \Lambda(\mathfrak{n}) r(\mathfrak{n}) \,\mathrm{spin}(\mathfrak{n}) \ll x^{1-\delta/2n(12n+1)+\varepsilon}. \tag{8.1}$$

Here, the condition $(\mathfrak{n}, F) = 1$ can be removed because the powers of prime ideals which divide $F$ contribute a negligible quantity. Moreover, the powers of primes which are not primes also contribute a negligible amount, so we are left with $\mathfrak{n} = \mathfrak{p}$, each one weighted by $\log N\mathfrak{p}$. These logarithmic weights can be removed by partial summation. Hence (8.1) implies (1.2).

## 9 Direct estimates for character sums

Our arguments in this paper are powered by estimates for real character sums over short intervals,

$$S_\chi(M, N) = \sum_{M<n\leqslant M+N} \chi(n), \qquad N \geqslant 1. \tag{9.1}$$

If $\chi(\bmod q)$ is not principal, one should expect to beat the trivial bound $S_\chi(M, N) \ll N$ by exploiting some cancellation due to the random sign changes of $\chi(n)$. The celebrated result of D. Burgess [2] gives us the bound

$$S_\chi(M, N) \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\varepsilon}, \tag{9.2}$$

with any integer $r \geqslant 1$ and any $\varepsilon > 0$, the implied constant depending only on $r$ and $\varepsilon$. The bound becomes trivial if $N \leqslant q^{(r+1)/4r}$ so, no matter how large we choose $r$ in (9.2), we get nothing useful for sums of length $N \leqslant q^{1/4}$. Fortunately, for our application to estimate the sums of spins in this paper (see Sect. 6), in the case of a cubic field we encounter sums of length $N$ as large as $q^{1/3}$ and we can appeal to Burgess' estimate. We take (9.2) with $r = 6$ to obtain:

**Corollary 9.1** *Let $\chi(\bmod q)$ be a non-principal real character. Then*

$$S_\chi(M, N) \ll N^{\frac{5}{6}} q^{\frac{7}{144}+\varepsilon}, \tag{9.3}$$

*with any $\varepsilon > 0$, the implied constant depending only on $\varepsilon$.*

When the degree of the field $K$ is $n > 3$ we need a non-trivial bound for $S_\chi(M, N)$ with $N$ of size about $q^{1/n}$ and nothing useful is available at present for such short sums (except in the case of special moduli, cf. [8]). Thus, in order to cover the fields of higher degree we have no option other than to postulate adequate estimates for these short character sums.

**Conjecture** $C_n$: *Let $n \geqslant 3$, $Q \geqslant 3$, $N \leqslant Q^{1/n}$. For any real non-principal character $\chi(\bmod q)$ of modulus $q \leqslant Q$ we have*

$$S_\chi(M, N) \ll Q^{\frac{1-\delta}{n}+\varepsilon}, \tag{9.4}$$

*with some $\delta = \delta(n) > 0$ and any $\varepsilon > 0$ the implied constant depending only on $\varepsilon$ and $n$.*

*Remarks* Burgess stated his estimate (9.2) for any $r \geqslant 1$ and any non-principal character $\chi \pmod q$, but, in the case of general $r$, only for $q$ cube-free. However, if $\chi$ is real, the character sum does not change if $q$ is reduced, as it always can be, to some cube-free divisor of $q$ by dividing out the largest square which does not remove any prime factor completely. Thus (9.3) is correct as stated. Actually, we are only using these bounds in the case of square-free modulus.

If $N \leqslant Q^{1/3}$ and $q \leqslant Q$ then (9.3) implies (9.4) proving Conjecture $C_3$ with

$$\delta = \delta(3) = \frac{1}{48}. \tag{9.5}$$

It is very important that (9.4) holds for character sums over any interval of length $N$, not only for the initial segment $0 < n \leqslant N$. If $M = 0$ the Riemann Hypothesis yields

$$S_\chi(0, N) \ll N^{\frac{1}{2}} q^{\varepsilon}, \tag{9.6}$$

so (9.4) holds with $\delta = 1/2$, but this special case is not sufficient for our applications. We hope that Conjecture $C_n$ will be established in the not too distant future by advancing the tools of analytic number theory so our main theorem will become unconditional for fields of any degree $n \geqslant 3$. Note that by Burgess' result (9.2), we narrowly missed Conjecture $C_4$.

Recall, we actually needed these bounds for character sums over an arithmetic progression. Fortunately, there is an immediate consequence of Conjecture $C_n$ for such sums:

$$S_\chi(M, N; k, \ell) = \sum_{\substack{M < n \leqslant M+N \\ n \equiv \ell \pmod k}} \chi(n). \tag{9.7}$$

This can be written as

$$\sum_{\frac{M-\ell}{k} < m \leqslant \frac{M+N-\ell}{k}} \chi(km + \ell).$$

Now, suppose $(k, q) = 1$. Take $\bar{k}$ with $\bar{k}k \equiv 1 \pmod q$. Then, we have

$$\bar{\chi}(k) S_\chi(M, N; k, \ell) = \sum_{\frac{M-\ell}{k} < m \leqslant \frac{M+N-\ell}{k}} \chi(m + \ell\bar{k}) = S_\chi\big(M', N/k\big)$$

with $M' = (M - \ell)k^{-1} + \ell\bar{k}$. Since the bound (9.4) does not depend on $M$, it remains valid for $S_\chi(M, N; k, \ell)$ provided $\chi \pmod q$ is not principal and $(k, q) = 1$.

## 10 Relating spins and Selmer groups

Suppose $E$ is an elliptic curve over $\mathbb{Q}$, and let $K = \mathbb{Q}(E[2])$, the number field generated by the points of order 2 in $E(\bar{\mathbb{Q}})$. We assume that $K$ is a cyclic cubic extension of $\mathbb{Q}$ and that all totally positive units of $K$ are squares, so $K$ satisfies the hypotheses of the earlier sections of this paper.

Let

$$y^2 = f(x)$$

be a Weierstrass model of $E$. Then $f$ is irreducible over $\mathbb{Q}$, and we can identify $K$ with $\mathbb{Q}[T]/f(T)$. For every place $v$ of $\mathbb{Q}$, we let $K_v = K \otimes \mathbb{Q}_v = \mathbb{Q}_v[T]/f(T)$. If $d \in \mathbb{Q}^\times$, then the quadratic twist $E^{(d)}$ of $E$ by $d$ is the elliptic curve $dy^2 = f(x)$.

See for example [11, § 2] for the definition of the 2-Selmer group $\mathrm{Sel}_2(E)$, or else take the description (10.1) below as the definition. The 2-Selmer group is an $\mathbb{F}_2$-vector subspace of $H^1(\mathbb{Q}, E[2])$, sitting in an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E) \to Ш(E)[2] \to 0,$$

where $Ш(E)$ is the Shafarevich-Tate group of $E/\mathbb{Q}$. Let

$$\Sigma = \{\text{primes } \ell : E \text{ has bad reduction at } \ell, \text{ and } \ell \text{ is unramified in } K\} \cup \{2\}.$$

The main result of this section is the following.

**Theorem 10.1** *Suppose $p$ is a prime that splits completely in $\mathbb{Q}(E[4])$, and let $\mathfrak{p}$ be a prime of $K$ above $p$. Suppose further that $\mathfrak{p}$ has a totally positive generator $\pi$ such that $\pi$ is a square in $K_\ell$ for every prime $\ell \in \Sigma$. Then viewing* $\mathrm{Sel}_2(E), \mathrm{Sel}_2(E^{(p)}) \subset H^1(\mathbb{Q}, E[2])$, *we have* $\mathrm{Sel}_2(E) \subset \mathrm{Sel}_2(E^{(p)})$ *and*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2\big(E^{(p)}\big) = \begin{cases} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) + 2 & \text{if } \mathrm{spin}(\mathfrak{p}) = +1, \\ \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) & \text{if } \mathrm{spin}(\mathfrak{p}) = -1. \end{cases}$$

To prove Theorem 10.1, we will use the description of the 2-Selmer group given in [1]. Namely, let

$$\big(K^\times/(K^\times)^2\big)^{N=1} := \big\{\alpha \in K^\times/(K^\times)^2 : N_{K/\mathbb{Q}}(\alpha) \in (\mathbb{Q}^\times)^2\big\}$$

and similarly for $(K_v^\times/(K_v^\times)^2)^{N=1}$, for every place $v$ of $K$. For every $v$ there is a commutative diagram

$$\begin{array}{ccc} E(\mathbb{Q})/2E(\mathbb{Q}) & \xhookrightarrow{\lambda_{E/\mathbb{Q}}} & (K^\times/(K^\times)^2)^{N=1} \\ \downarrow & & \downarrow \iota_v \\ E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) & \xhookrightarrow{\lambda_{E/\mathbb{Q}_v}} & (K_v^\times/(K_v^\times)^2)^{N=1}. \end{array}$$

The injection $\lambda_{E/\mathbb{Q}}$ is defined for $P \in E(\mathbb{Q}) - E(\mathbb{Q})[2]$ by $\lambda_E(P) := x(P) - T$, where $x(P)$ denotes the $x$-coordinate of $P$ and we identify $K = \mathbb{Q}[T]/f(T)$, and $\lambda_{E/\mathbb{Q}_v}$ is defined similarly. By [1, § 2] there is a natural identification

$$\mathrm{Sel}_2(E) = \left\{\alpha \in \left(K^\times/\left(K^\times\right)^2\right)^{N=1} : \iota_v(\alpha) \in \mathrm{image}(\lambda_{E/\mathbb{Q}_v}) \text{ for every } v\right\}. \tag{10.1}$$

Fix a generator $\sigma$ of $\mathrm{Gal}(K/\mathbb{Q})$. If $\mathfrak{p}$ is a prime of degree one of $K$, lying above the rational prime $p$, we identify $K_p$ with $\mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p$. The map $\iota_p$ is then given by

$$\iota_p(\alpha) = \left(\alpha, \alpha^\sigma, \alpha^{\sigma^2}\right) \in \left(K_\mathfrak{p}^\times/\left(K_\mathfrak{p}^\times\right)^2\right)^3 = \left(\mathbb{Q}_p^\times/\left(\mathbb{Q}_p^\times\right)^2\right)^3. \tag{10.2}$$

**Lemma 10.2** *Suppose $p$ is an odd prime that splits completely in $\mathbb{Q}(E[4])$, and $E$ has good reduction at $p$. With the identification above, we have*

$$\mathrm{image}(\lambda_{E/\mathbb{Q}_p}) \textit{ is generated by } (u, u, 1) \textit{ and } (u, 1, u), \tag{10.3}$$

*where $u \in \mathbb{Z}_p^\times$ is a nonsquare, and*

$$\mathrm{image}(\lambda_{E^{(p)}/\mathbb{Q}_p}) \textit{ is generated by } (p, p, 1) \textit{ and } (p, 1, p). \tag{10.4}$$

*Proof* Assertion (10.3) is [1, Corollary 3.3].

Since $p$ splits completely in $\mathbb{Q}(E[4])$, $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts trivially on $E[4]$, and hence $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $E^{(p)}[4]$ by the quadratic character of $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$. It follows that the natural map $E^{(p)}(\mathbb{Q}_p)[2] \to E^{(p)}(\mathbb{Q}_p)/2E^{(p)}(\mathbb{Q}_p)$ is an isomorphism and the natural map

$$E^{(p)}(\mathbb{Q}_p)/2E^{(p)}(\mathbb{Q}_p) \to E^{(p)}\left(\mathbb{Q}_p(\sqrt{p})\right)/2E^{(p)}\left(\mathbb{Q}_p(\sqrt{p})\right)$$

is identically zero. Therefore, if $\lambda_{E^{(p)}/\mathbb{Q}_p}(P) = (t_1, t_2, t_3) \in (\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2)^3$, then $t_i$ is a square in $\mathbb{Q}_p(\sqrt{p})$ for every $i$. Since $|E^{(p)}(\mathbb{Q}_p)/2E^{(p)}(\mathbb{Q}_p)| = 4$, (10.4) follows. □

*Proof of Theorem 10.1* Suppose $p$ satisfies the hypotheses of Theorem 10.1. Then $p = N_{K/\mathbb{Q}}\pi$ is a square in $\mathbb{Q}_v$ if $v \in \Sigma \cup \{\infty\}$. Hence for such $v$, $E$ is isomorphic to $E^{(p)}$ over $\mathbb{Q}_v$, so $\text{image}(\lambda_{E/\mathbb{Q}_v}) = \text{image}(\lambda_{E^{(p)}/\mathbb{Q}_v})$. If $\ell \neq 2$ ramifies in $K$, then $E(\mathbb{Q}_\ell)[2] = E^{(p)}(\mathbb{Q}_\ell)[2] = 0$, so $E(\mathbb{Q}_\ell)/2E(\mathbb{Q}_\ell) = E^{(p)}(\mathbb{Q}_\ell)/2E^{(p)}(\mathbb{Q}_\ell) = 0$ and $\text{image}(\lambda_{E/\mathbb{Q}_\ell}) = \text{image}(\lambda_{E^{(p)}/\mathbb{Q}_\ell}) = 0$. If $\ell \nmid 2p$ is a prime where $E$ has good reduction, unramified in $K$, then [3, Lemma 4.1] shows that $\text{image}(\lambda_{E/\mathbb{Q}_\ell}) = \text{image}(\lambda_{E^{(p)}/\mathbb{Q}_\ell})$. Therefore $\text{image}(\lambda_{E/\mathbb{Q}_v}) = \text{image}(\lambda_{E^{(p)}/\mathbb{Q}_v})$ for every $v \neq p$.

Let

$$S^{(p)} = \left\{\alpha \in \left(K^\times/\left(K^\times\right)^2\right)^{N=1} : \iota_v(\alpha) \in \text{image}(\lambda_{E/\mathbb{Q}_v}) \text{ for every } v \neq p\right\},$$
$$S_{(p)} = \left\{\alpha \in S^{(p)} : \iota_p(\alpha) = 1\right\}.$$

Then

$$\text{Sel}_2(E) = \left\{\alpha \in S^{(p)} : \iota_p(\alpha) \in \text{image}(\lambda_{E/\mathbb{Q}_p})\right\},$$
$$\text{Sel}_2\left(E^{(p)}\right) = \left\{\alpha \in S^{(p)} : \iota_p(\alpha) \in \text{image}(\lambda_{E^{(p)}/\mathbb{Q}_p})\right\}.$$

By Lemma 10.2, $\text{image}(\lambda_{E/\mathbb{Q}_p}) \cap \text{image}(\lambda_{E^{(p)}/\mathbb{Q}_p}) = \{1\}$, so

$$\text{Sel}_2(E) \cap \text{Sel}_2\left(E^{(p)}\right) = S_{(p)}.$$

Global duality (see for example [11, Lemma 3.2]) shows that

$$\dim_{\mathbb{F}_2} \iota_p\left(S^{(p)}\right) = \dim_{\mathbb{F}_2}\left(S^{(p)}/S_{(p)}\right) = 2. \tag{10.5}$$

Let $\pi$ be the totally positive generator of a prime above $p$, as in the statement of Theorem 10.1, and let $\alpha = \pi\pi^\sigma$. Then $N_{K/\mathbb{Q}}\alpha = p^2$. Since $\pi$ is totally positive, $\alpha \in (K_\infty^\times)^2$. By assumption, $\alpha \in (K_\ell^\times)^2$ if $\ell = 2$ or if $\ell$ is a prime of bad reduction, unramified in $K$. If $\ell$ is odd and $\ell$ ramifies in $K$, then $\alpha \equiv \pi^2$ modulo the prime of $K$ above $\ell$, so $\alpha \in (K_\ell^\times)^2$ in this case as well. Finally, if $\ell \neq p$ then $\alpha$ is a unit at $\ell$, so if $\ell$ is a prime of good reduction then (again using [3, Lemma 4.1]) we have $\iota_\ell(\alpha) \in \text{image}(\lambda_{E/\mathbb{Q}_\ell})$. Therefore $\alpha \in S^{(p)}$.

Since $\iota_p(\alpha)$ and $\iota_p(\alpha^\sigma)$ are distinct and nonzero in $K_p^\times/(K_p^\times)^2$, we see by (10.5) that $\alpha, \alpha^\sigma$ generate $S^{(p)}/S_{(p)}$. By (10.3), $\iota_p(\alpha)$ and $\iota_p(\alpha^\sigma)$ generate a subgroup visibly disjoint from $\text{image}(\lambda_{E/\mathbb{Q}_p})$. Thus

$$\iota_p\left(S^{(p)}\right) \cap \text{image}(\lambda_{E/\mathbb{Q}_p}) = \{1\}$$

so $\text{Sel}_2(E) = S_{(p)}$.

By (10.2) we have

$$\begin{aligned}\iota_p(\alpha) &= \left(\pi\pi^\sigma, \pi^\sigma\pi^{\sigma^2}, \pi\pi^{\sigma^2}\right)\\ &= (p, 1, p)\cdot\left(1/\pi^{\sigma^2}, \pi^\sigma\pi^{\sigma^2}, 1/\pi^\sigma\right) \in K_p^\times/\left(K_p^\times\right)^2.\end{aligned}$$

Since $\pi$ is a square in $K_2^\times$, Lemma 11.1 in the next section shows that $\pi^\sigma, \pi^{\sigma^2} \in (K_{\mathfrak{p}}^\times)^2$ if and only if $\operatorname{spin}(\mathfrak{p}) = +1$. Thus, by (10.4)

$$\iota_p(\alpha) \in \operatorname{image}(\lambda_{E^{(p)}/\mathbb{Q}_p}) \iff \operatorname{spin}(\mathfrak{p}) = +1.$$

The same holds for $\alpha^\sigma$ and $\alpha\alpha^\sigma$, so we have

$$\operatorname{Sel}_2\left(E^{(p)}\right) = \begin{cases} S^{(p)} & \text{if } \operatorname{spin}(\mathfrak{p}) = +1,\\ S_{(p)} & \text{if } \operatorname{spin}(\mathfrak{p}) = -1.\end{cases}$$

Now the theorem follows from (10.5). □

*Example* Let $E$ be the elliptic curve $y^2 = x^3 + x^2 - 16x - 29$ of conductor 784, as in the introduction. Then $\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) = 1$, $K = \mathbb{Q}(E[2])$ is the real subfield of the field of 7-th roots of unity, and every totally positive unit of $K$ is a square.

The only prime of bad reduction for $E$ that is unramified in $K$ is 2, and $\mathbb{Q}(E[4])$ is contained in the ray class field of $K$ modulo $8\infty_1\infty_2\infty_3$. Hence if $p$ is a rational prime that splits completely in $K$, and a prime $\mathfrak{p}$ above $p$ has a totally positive generator congruent to 1 modulo 8, then $p$ splits completely in $\mathbb{Q}(E[4])$ and Theorem 10.1 applies to show that

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2\left(E^{(p)}\right) = \begin{cases} 3 & \text{if } \operatorname{spin}(\mathfrak{p}) = +1,\\ 1 & \text{if } \operatorname{spin}(\mathfrak{p}) = -1.\end{cases}$$

## 11 More than one spin

There is plenty of scope for further work on the subject of this paper. We can for example ask what happens if one or more of the various restrictions are dropped from those we placed on the number fields being considered: "totally real, Galois, cyclic, units achieving all signs".

Even keeping these assumptions in place, there remain interesting problems. A particularly natural one is the question of the joint distribution of the $n$ different spins attached to the primes by the various automorphisms of $G = \operatorname{Gal}(K/\mathbb{Q})$. An instantaneous guess might be that the distributions are independent of each other but, even in the simplest case of cyclic $G$, there are relations amongst the spins which make the situation a little more complicated, and perhaps more interesting.

Let $\sigma$ and $\tau$ be two elements of $G$ which, given our assumptions, commute. Let $\mathfrak{a} = (\alpha)$ where $\alpha$ is odd and totally positive. Recovering our notation from (1.1), we have

$$\operatorname{spin}(\sigma, \mathfrak{a}^\tau) = \left(\frac{\alpha^\tau}{(\alpha)^{\tau\sigma}}\right) = \left(\frac{\alpha^\tau}{(\alpha)^{\sigma\tau}}\right) = \left(\frac{\alpha}{(\alpha)^{\sigma}}\right) = \operatorname{spin}(\sigma, \mathfrak{a}),$$

a fact we have already been using. Specializing to $\tau = \sigma^{-1}$ we find that

$$\operatorname{spin}(\sigma^{-1}, \mathfrak{a}) = \left(\frac{\alpha}{(\alpha)^{\sigma^{-1}}}\right) = \left(\frac{\alpha^\sigma}{(\alpha)^{\sigma^{-1}\sigma}}\right) = \left(\frac{\alpha^\sigma}{\alpha}\right),$$

so that, by quadratic reciprocity:

**Lemma 11.1** *We have*

$$\operatorname{spin}(\sigma, \mathfrak{a}) = \operatorname{spin}(\sigma^{-1}, \mathfrak{a})\mu_2(\alpha, \alpha^\sigma),$$

*where* $\mu_2(\alpha, \alpha^\sigma)$ *is a product of the local Hilbert symbols at primes* $\mathfrak{p} \mid 2$. *In particular,* $\mu_2(\alpha, \alpha^\sigma) = 1$ *if* $\alpha \equiv 1 (\operatorname{mod} 4)$.

If we now let $\sigma$ be a generator of $G$ then, for each $k$, $1 \leqslant k \leqslant n-1$, there is an evident dependence between $\operatorname{spin}(\sigma^k, \mathfrak{a})$ and $\operatorname{spin}(\sigma^{n-k}, \mathfrak{a})$. For fields of odd degree this shows that there is no non-identity spin whose distribution is independent of all of the others and the question arises as to whether these are the only dependencies among the spins. For the simplest possible example we can ask:

**Problem** For $K$ totally real, of degree $n \geqslant 5$ (odd or even), with all totally positive units being squares, and $G = \operatorname{Gal}(K/\mathbb{Q})$ being cyclic and generated by $\sigma$, are the distributions of $\operatorname{spin}(\sigma, \mathfrak{a})$ and $\operatorname{spin}(\sigma^2, \mathfrak{a})$ independent?

If we consider fields $K$ of even degree the (non-identity) spins also pair off and the same questions arise, apart from the middle spin, $k = n/2$. Here, we have an involution, say $\sigma = \sigma^{-1}$, and a somewhat different picture emerges. Recall that, in addition to our assumptions about the field, we have also been restricting our attention to generators of the Galois group so that, even though we are now talking about a single spin, we have not dealt with this situation. In Sect. 12 using very different arguments, we give results which show that equidistribution holds for the sum of prime spins attached to such an involution.

## 12 Prime spins for an involution

In this section we are going to require our Galois automorphism $\sigma$ to be an involution (not the identity), rather than a generator of the group so, in addition to our previous restrictions, we ask that $K$ have even degree $n$ and we denote by $L$ the fixed field of $\sigma$ so that $K/L$ is a quadratic field extension. Thus, in particular, $K$ could be a real quadratic field so long as its fundamental unit has norm $-1$. We shall also make some further simplifications as we proceed.

Our first main result gives a natural arithmetic characterization of the spin attached to such an involution.

**Proposition 12.1** *Let $K/\mathbb{Q}$ be a totally real Galois extension of even degree $n \geqslant 2$ with $\mathcal{U}^+ = \mathcal{U}^2$. Let L be the subfield of K fixed by the involution $\sigma$ and suppose that the discriminant $\mathfrak{D}$ of the quadratic extension $K/L$ is odd. Let $\alpha \in \mathcal{O}_K$, with $(\alpha, \alpha^\sigma) = 1, \alpha \equiv 1 (\bmod 8), \alpha \succ 0$. Then, for $\mathfrak{a} = (\alpha)$, we have*

$$\operatorname{spin}(\sigma, \mathfrak{a}) = \left(\frac{\beta}{\mathfrak{D}}\right)_L, \tag{12.1}$$

*where*

$$\beta = \frac{1}{2}\left(\alpha + \alpha^\sigma\right) = \frac{1}{2} T_{K/L}(\alpha).$$

Note that the notation in the quadratic symbol now reflects the field. This reduction of the spin to something so close to the field character imparts multiplicativity properties which render inoperable the method we have employed up to now but open the possibility of using the theory of $L$-functions. As a result, we shall obtain the following theorem.

**Theorem 12.2** *Let $K/\mathbb{Q}$ be a totally real Galois extension of even degree $n \geqslant 2$ with $\mathcal{U}^+ = \mathcal{U}^2$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be an involution and let the discriminant of the relative quadratic extension be odd. Let $\mathfrak{P}$ run over the principal prime ideals of K with*

$$\mathfrak{P} = (\alpha), \quad \alpha \succ 0, \alpha \equiv 1 (\bmod 8).$$

*Then, we have*

$$\sum_{N\mathfrak{P} \leqslant x} \operatorname{spin}(\sigma, \mathfrak{P}) \ll x \exp(-C\sqrt{\log x}),$$

*where the positive constant C and the implied constant depend on the field K. On assumption of the Riemann Hypothesis for Hecke L-functions, the above* *bound can be sharpened to*

$$\sum_{N\mathfrak{P}\leqslant x} \mathrm{spin}(\sigma,\mathfrak{P}) \ll x^{\frac{1}{2}}(\log x)^A,$$

*where now the positive constant $A$ depends on the degree of the field $K$.*

Note that we now denote the prime ideals of $K$ by $\mathfrak{P}$ rather than by $\mathfrak{p}$ as before, because we reserve $\mathfrak{p}$ for the prime ideals of the subfield $L$.

The path to Proposition 12.1 passes through a number of lemmas which lead to progressively simpler expressions for the spin. We begin with

**Lemma 12.3** *If $\mathfrak{P} \subset \mathcal{O}_K$ is an odd prime with $(\mathfrak{P}, \mathfrak{P}^\sigma) = 1$ then, for $x \in \mathcal{O}_L$ we have*

$$\left(\frac{x}{\mathfrak{P}}\right)_K = \left(\frac{x}{\mathfrak{p}}\right)_L \quad \text{with } \mathfrak{p} = \mathfrak{P}\mathfrak{P}^\sigma. \tag{12.2}$$

*Proof* This follows quickly on combining the Euler criteria for the two fields:

$$\left(\frac{x}{\mathfrak{P}}\right)_K \equiv x^{\frac{1}{2}(N_{K/\mathbb{Q}}(\mathfrak{P})-1)} (\mathrm{mod}\, \mathfrak{P}),$$

$$\left(\frac{x}{\mathfrak{p}}\right)_L \equiv x^{\frac{1}{2}(N_{L/\mathbb{Q}}(\mathfrak{p})-1)} (\mathrm{mod}\, \mathfrak{p}),$$

valid for $(x, \mathfrak{p}) = 1$. Here, $N_{K/\mathbb{Q}}(\mathfrak{P}) = N_{L/\mathbb{Q}}(\mathfrak{p})$. □

**Corollary 12.4** *If $\alpha \in \mathcal{O}_K$ is odd and $(\alpha, \alpha^\sigma) = 1$ then, for $x \in \mathcal{O}_L$, we have*

$$\left(\frac{x}{\alpha}\right)_K = \left(\frac{x}{\alpha\alpha^\sigma}\right)_L. \tag{12.3}$$

Now, let $\alpha \in \mathcal{O}_K$ be odd, $(\alpha, \alpha^\sigma) = 1$ and $\alpha \succ 0$. Then, the Corollary gives

$$\mathrm{spin}(\sigma,\alpha) = \left(\frac{\alpha}{\alpha^\sigma}\right)_K = \left(\frac{\alpha+\alpha^\sigma}{\alpha^\sigma}\right)_K = \left(\frac{\alpha+\alpha^\sigma}{\alpha\alpha^\sigma}\right)_L.$$

Suppose that $\alpha \equiv 1 (\mathrm{mod}\, 8)$. Then,

$$\beta = \frac{1}{2}\big(\alpha + \alpha^\sigma\big) \equiv 1 (\mathrm{mod}\, 4), \qquad \gamma = \frac{1}{2}\big(\alpha - \alpha^\sigma\big) \equiv 0 (\mathrm{mod}\, 4),$$

satisfy $(\beta,\gamma)=1$, $\beta\succ 0$ and $\alpha\alpha^\sigma=\beta^2-\gamma^2\equiv 1 (\mathrm{mod}\, 8)$. We have $\beta\in\mathcal{O}_L$ and $\gamma^2\in\mathcal{O}_L$. Hence, the spin simplifies to

$$\mathrm{spin}(\sigma,\alpha)=\left(\frac{2}{\alpha\alpha^\sigma}\right)_L\left(\frac{\beta}{\alpha\alpha^\sigma}\right)_L=\left(\frac{2}{\alpha\alpha^\sigma}\right)_L\left(\frac{\alpha\alpha^\sigma}{\beta}\right)_L=\left(\frac{-\gamma^2}{\beta}\right)_L, \tag{12.4}$$

since $\alpha\equiv 1 (\mathrm{mod}\, 8)$ implies $\alpha^\sigma\equiv 1 (\mathrm{mod}\, 8)$, which implies $(\frac{2}{\alpha\alpha^\sigma})_L=1$.

The final lemma in this chain is:

**Lemma 12.5** *If $\beta\equiv 1 (\mathrm{mod}\, 4)$ and $\delta$ odd, are in $\mathcal{O}_L$, then*

$$\left(\frac{\beta,\delta}{\mathfrak{p}}\right)=1 \quad \textit{for every } \mathfrak{p}\mid 2.$$

*Proof* First we consider the special case $\delta\equiv 1 (\mathrm{mod}\, 2)$. Here, we use the identity $1+4x=(1+2y)^2-4\delta y^2$ with $x=y+(1-\delta)y^2$. Given $x\in\mathcal{O}_L$ the latter equation is solvable for $y\in L_{\mathfrak{p}}$ by Hensel's Lemma. This yields the result.

In general, if $\delta$ is odd, there exists an odd positive integer $r$ such that we have $\delta^r\equiv 1 (\mathrm{mod}\, 2)$. This follows from Fermat's Little Theorem with $r=N\mathfrak{p}-1$ for any $\mathfrak{p}\mid 2$. Hence, the result follows from the special case by the multiplicativity of the Hilbert symbol. □

Now, consider the submodule $\mathcal{M}=\mathcal{O}_L+\frac{(1+\alpha)}{2}\mathcal{O}_L$ of $\mathcal{O}_K$. Since

$$\det\begin{pmatrix}1 & (1+\alpha)/2\\ 1 & (1+\alpha^\sigma)/2\end{pmatrix}=-\gamma,$$

the discriminant of $\mathcal{M}$ is the principal ideal $(\gamma^2)$ of $\mathcal{O}_L$. Hence, $(\gamma^2)=\mathfrak{a}^2\mathfrak{D}$ where $\mathfrak{a}$ is an ideal of $\mathcal{O}_L$ such that $\mathcal{O}_K/\mathcal{M}\cong\mathcal{O}_L/\mathfrak{a}$ and $\mathfrak{D}$ is the discriminant of the relative quadratic extension $K/L$. We have $(\beta,\gamma^2)=1$ so $(\beta,\mathfrak{a}^2\mathfrak{D})=1$. Choose an ideal $\mathfrak{b}$ of $\mathcal{O}_L$ with $\mathfrak{b}\sim\mathfrak{a}$ and $(\mathfrak{b},2\beta\mathfrak{a})=1$ and choose $\mu\in L$ such that $(\mu)=\mathfrak{a}^{-1}\mathfrak{b}$. Put $\gamma_1=\gamma\mu\in K$. Then, $\gamma_1^2=\gamma^2\mu^2\in L$ and, in fact,

$$(\gamma_1^2)=(\gamma^2)(\mu)^2=\mathfrak{a}^2\mathfrak{D}(\mathfrak{a}^{-1}\mathfrak{b})^2=\mathfrak{b}^2\mathfrak{D}, \tag{12.5}$$

so $\gamma_1^2\in\mathcal{O}_L$. Since $(\beta,\mathfrak{a}\mathfrak{b})=1$ we have

$$\left(\frac{-\gamma_1^2}{\beta}\right)_L=\left(\frac{-\gamma^2\mu^2}{\beta}\right)_L=\left(\frac{-\gamma^2}{\beta}\right)_L.$$

By (12.5), $(\gamma_1^2, 2\beta) = 1$ and

$$\left(\frac{-\gamma_1^2}{\beta}\right)_L = \left(\frac{\beta}{\gamma_1^2}\right)_L \prod_{\mathfrak{p}|2\infty} \left(\frac{\beta, -\gamma_1^2}{\mathfrak{p}}\right) = \left(\frac{\beta}{\gamma_1^2}\right)_L = \left(\frac{\beta}{\mathfrak{D}}\right)_L,$$

by the reciprocity law and Lemma 12.5. Now, by (12.4), this completes the proof of Proposition 12.1.

We now turn to the proof of Theorem 12.2.

*Proof* Let $\mathfrak{P}$ run over the principal prime ideals of $K$ with

$$\mathfrak{P} = (\alpha), \quad \alpha \succ 0,\ \alpha \equiv 1 (\mathrm{mod}\, 8). \tag{12.6}$$

Denote by $S(x)$ the number of such prime ideals with $N\mathfrak{P} \leqslant x$ and by $S(x; \mathfrak{D}, \delta)$ the number of these in the residue class $\alpha \equiv \delta (\mathrm{mod}\, \mathfrak{D})$. By the Prime Ideal Theorem we have (recall that $\mathfrak{D}$ is odd)

$$S(x; \mathfrak{D}, \delta) \sim \frac{S(x)}{\varphi_K(\mathfrak{D})}, \quad \text{if } (\delta, \mathfrak{D}) = 1,$$

where $\varphi_K(\mathfrak{D})$ is the number of classes $\delta (\mathrm{mod}\, \mathfrak{D})$ in $\mathcal{O}_K$ with $(\delta, \mathfrak{D}) = 1$. More precisely, the error term satisfies

$$E(x; \mathfrak{D}, \delta) = S(x; \mathfrak{D}, \delta) - \frac{S(x)}{\varphi_K(\mathfrak{D})} \ll x \exp(-C\sqrt{\log x}) \tag{12.7}$$

unconditionally, and

$$E(x; \mathfrak{D}, \delta) \ll x^{1/2} (\log x)^A \tag{12.8}$$

subject to the Riemann Hypothesis for the relevant Hecke $L$-functions. Here $C$ and $A$ are positive constants depending on the field $K$, as do the implied constants.

Note that

$$\sum_{\substack{\delta (\mathrm{mod}\, \mathfrak{D}) \\ (\delta, \mathfrak{D})=1}} \left(\frac{\delta + \delta^\sigma}{\mathfrak{D}}\right)_L = 0. \tag{12.9}$$

To see this we change the variable $\delta$ to $\delta\eta$ with $\eta \in \mathcal{O}_L$, $(\eta, \mathfrak{D}) = 1$. We find the sum is equal to $(\eta/\mathfrak{D})_L$ times itself. Choosing $\eta$ such that $\chi_{\mathfrak{D}}(\eta) = (\eta/\mathfrak{D})_L = -1$, we obtain (12.9).

Now, put

$$S^\sigma(x) = \sum_{N\mathfrak{P} \leqslant x} \mathrm{spin}(\sigma, \mathfrak{P}), \tag{12.10}$$

where $\mathfrak{P}$ runs through the prime ideals (12.6). By the formula (12.1) we get

$$S^\sigma(x) = \left(\frac{2}{\mathfrak{D}}\right)_L \sum_{\substack{\delta (\mathrm{mod}\, \mathfrak{D}) \\ (\delta, \mathfrak{D})=1}} \left(\frac{\delta + \delta^\sigma}{\mathfrak{D}}\right)_L S(x; \mathfrak{D}, \delta) + O(1),$$

where the error term $O(1)$ takes into account the contribution of the prime ideals dividing $\mathfrak{D}$. Finally, applying the Prime Ideal Theorem in the form (12.7) or the Riemann Hypothesis in the form (12.8), we find by (12.9) that the main terms cancel out so we are left with the result claimed in the theorem. □

**Acknowledgements** This work was initiated and a significant part was accomplished during the time the authors enjoyed participating, with MSRI financial support, in the program on "Arithmetic Statistics", held at MSRI Berkeley during January–May, 2011. The second and third-named authors also received support from the Clay Mathematics Institute. Research of J.F. is supported by NSERC grant A5123, that of H.I. by NSF Grant DMS-1101574, that of B.M. by NSF Grant DMS-0968831 and that of K.R. by NSF Grant DMS-1065904. We would also like to thank the referee for a very thorough reading of the paper.

## References

1. Brumer, A., Kramer, K.: The rank of elliptic curves. Duke Math. J. **44**, 715–743 (1977)
2. Burgess, D.A.: On character sums and $L$-series II. Proc. Lond. Math. Soc. **13**, 524–536 (1963)
3. Cassels, J.W.S.: Arithmetic of curves of genus 1, VIII. J. Reine Angew. Math. **217**, 180–199 (1965)
4. Cassels, J.W.S.: Global fields. In: Algebraic Number Theory, Proc. Instructional Conf., Brighton, 1965, pp. 42–84. Thompson, Washington (1967)
5. Duke, W., Friedlander, J.B., Iwaniec, H.: Bilinear forms with Kloosterman fractions. Invent. Math. **128**, 23–43 (1997)
6. Friedlander, J.B., Iwaniec, H.: The polynomial $X^2 + Y^4$ captures its primes. Ann. Math. **148**, 945–1040 (1998)
7. Hecke, E.: Lectures on the Theory of Algebraic Numbers. Grad. Texts in Math., vol. 77. Springer, New York (1981)
8. Iwaniec, H., Kowalski, E.: Analytic Number Theory. Colloq. Pub., vol. 53. Am. Math. Soc., Providence (2004)
9. Lang, S.: Algebraic Number Theory, 2nd edn. Grad. Texts in Math., vol. 110. Springer, New York (1994)
10. Lehmer, E.: Connection between Gaussian periods and cyclic units. Math. Comput. **50**, 535–541 (1988)
11. Mazur, B., Rubin, K.: Ranks of twists of elliptic curves and Hilbert's tenth problem. Invent. Math. **181**, 541–575 (2010)
12. Neukirch, J.: Algebraic Number Theory. Grund. Math. Wiss., vol. 322. Springer, Berlin (1999)
13. Shanks, D.: The simplest cubic fields. Math. Comput. **28**, 1137–1152 (1974)
14. Shintani, T.: On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. J. Fac. Sci., Univ. Tokyo, Sect. 1A, Math. **23**, 393–417 (1976)