Max-Planck-Institut für Mathematik
Bonn

A density of ramified primes

by

Stephanie Chan
Christine McMeekin
Djordjo Milovic

Max-Planck-Institut für Mathematik
Preprint Series 2020 (33)

A density of ramified primes

by

Stephanie Chan
Christine McMeekin
Djordjo Milovic

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
University College London
London WC1E 6BT
UK

Department of Mathematics
University of Connecticut
Storrs, CT 06269
USA

MPIM 20-33

A DENSITY OF RAMIFIED PRIMES

STEPHANIE CHAN, CHRISTINE MCMEEKIN, AND DJORDJO MILOVIC

Abstract. Let K be a cyclic totally real number field of odd degree over $\mathbb{Q}$ with odd class number, such that every totally positive unit is the square of a unit, and such that 2 is inert in $K/\mathbb{Q}$. We define a family of number fields $\{K(p)\}_p$, depending on K and indexed by the rational primes p that split completely in $K/\mathbb{Q}$, such that p is always ramified in $K(p)$ of degree 2. Conditional on a standard conjecture on short character sums, the density of such rational primes p that exhibit one of two possible ramified factorizations in $K(p)/\mathbb{Q}$ is strictly between 0 and 1 and is given explicitly as a formula in terms of $[K:\mathbb{Q}]$. Our results are unconditional in the cubic case. Our proof relies on a detailed study of the joint distribution of spins of prime ideals.

Contents

1. Introduction

Given a number field, let $\mathcal{O}$, Cl, and Cl^+ denote its ring of integers, its class group, and its narrow class group, respectively. We will prove certain density theorems for number fields K satisfying the following five properties:

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, and $\mathrm{Cl}^+ = \mathrm{Cl}$;
(P2) the class number $h = |\mathrm{Cl}|$ of K is odd;
(P3) the degree n of $K/\mathbb{Q}$ is odd;

Date: May 20, 2020.

(P4) the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic; and
(P5) the prime 2 is inert in $K/\mathbb{Q}$.

Recall that Cl^+ is the quotient of the group of invertible fractional ideals of K by the subgroup of principal fractional ideals that can be generated by a totally positive element; in other words, Cl^+ is the ray class group of conductor equal to the product of all real places. If $\alpha \in K$ is totally positive, i.e., if $\sigma(\alpha) > 0$ for all real embeddings $\sigma : K \hookrightarrow \mathbb{R}$, we will sometimes write $\alpha \succ 0$. If K is totally real, then $\mathrm{Cl}^+ = \mathrm{Cl}$ if and only if every totally positive unit in $\mathcal{O}$ is a square; see Lemma 2.1. Hence, property (P1) can be restated as

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, and $\mathcal{O}_+^\times := \{u \in \mathcal{O}^\times : u \succ 0\} = (\mathcal{O}^\times)^2$.

Number fields satisfying properties (P1) and (P4) were studied by Friedlander, Iwaniec, Mazur, and Rubin [FIMR13]. More precisely, Friedlander et al. proved that if σ is a (fixed) generator of $\mathrm{Gal}(K/\mathbb{Q})$, then the density of principal prime ideals $\pi\mathcal{O}$ that split in the quadratic extension $K(\sqrt{\sigma(\pi)})/K$ is equal to $1/2$. Koymans and Milovic [KM] extended the results of Friedlander et al. in two different aspects. First, the number field K now needs to satisfy only property (P1), i.e., $K/\mathbb{Q}$ need not be cyclic; second, density theorems about the splitting behavior of principal prime ideals are proved for multi-quadratic extensions of the form $K(\{\sqrt{\sigma(\pi)} : \sigma \in S\})/K$, where S is a fixed subset of $\mathrm{Gal}(K/\mathbb{Q})$ with the property that $\sigma \notin S$ whenever $\sigma^{-1} \in S$.

Our main goal is to further extend these results to a certain setting where $S = \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$; in this setting, we in fact have $\sigma \in S$ whenever $\sigma^{-1} \in S$, and so our work features a new interplay of the Chebotarev Density Theorem and the method of sums of type I and type II. In particular, the densities appearing in our main theorems are of greater complexity than those appearing in [FIMR13] or [KM].

Another innovation in our work is that by assuming property (P2), we are now also able to study the splitting behavior of *all* prime ideals, and not only those that are principal. While our generalization of “spin” to non-principal ideals may appear innocuous (see Definition 3.1), it is of note that it still encodes the relevant splitting information as well as that the study of its oscillations requires new ideas, carried out in Section 6.

Let K be a number field satisfying properties (P1) and (P2), and let p be a rational prime that splits completely in $K/\mathbb{Q}$. We will now define an extension $K(p)/\mathbb{Q}$ where p ramifies; this extension was first studied by McMeekin [McM18]. Let $\mathfrak{p}$ be an unramified prime ideal of degree one in $\mathcal{O}$. Let $R_\mathfrak{p}^\infty$ denote the maximal abelian extension of K unramified at all finite primes other than $\mathfrak{p}$; in other words, $R_\mathfrak{p}^\infty$ is the ray class field of K of conductor $\mathfrak{p}\infty$, where ∞ denotes the product of all real places of K. There is a unique subfield $K(\mathfrak{p}) \subset R_\mathfrak{p}^\infty$ of degree 2 over K; see Lemma 2.2. Finally, we define $K(p)$ to be the compositum of $K(\mathfrak{p})$ over all primes $\mathfrak{p}$ lying above p, i.e.,

$$K(p) = \prod_{\mathfrak{p}|p} K(\mathfrak{p}).$$

As $K(p)/\mathbb{Q}$ is Galois, the residue field degree $f_{K(p)/\mathbb{Q}}(p)$ of p in $K(p)/\mathbb{Q}$ is well-defined. Our goal is to study the distribution of $f_{K(p)/\mathbb{Q}}(p)$ as p varies. Note that because p splits completely in $K/\mathbb{Q}$, $f_{K(p)/\mathbb{Q}}(p)$ is equal to the residue field degree $f_{K(p)/K}(\mathfrak{p})$ of $\mathfrak{p}$ in $K(p)/\mathbb{Q}$ for any prime $\mathfrak{p}$ of K lying above p.

To state our main results, we now introduce the relevant notions of density. For sets of primes $A \subseteq B$, we define the restricted density of A (restricted to B) to be

$$d(A|B) := \lim_{N\to\infty} \frac{\#A|_N}{\#B|_N}.$$

where $A|_N := \{p \in A : \mathfrak{N}(p) < N\}$ and $B|_N$ is defined similarly. When Π consists of all but finitely many primes, then $d(A) := d(A|\Pi)$ is the usual natural density of A.

Let $\mathscr{P}^2_{\mathbb{Q}}$ denote the set of rational primes co-prime to 2. For a fixed sign, ±, we define the following sets of rational primes.

$$\begin{aligned} S \quad &:= \{p \in \mathscr{P}^2_{\mathbb{Q}} : p \text{ splits completely in } K/\mathbb{Q}\}, \\ S_\pm \quad &:= \{p \in S : p \equiv \pm 1 \bmod 4\mathbb{Z}\}, \\ F \quad &:= \{p \in S : f_{K(p)/\mathbb{Q}}(p) = 1\}, \\ F_\pm \quad &:= S_\pm \cap F. \end{aligned}$$

Our main results are conditional on the following conjecture, a slight variant of which appears in both [FIMR13] and [KM]. In the following conjecture, the real number $\eta \in (0, 1]$ plays the role of $1/n$ from [FIMR13, Conjecture C_n, p. 738-739]

Conjecture C_η. *[FIMR13] Let η be a real number satisfying $0 < \eta \le 1$. Then there exists a real number $\delta = \delta(\eta) > 0$ such that for all $\epsilon > 0$ there exists a real number $C = C(\eta, \epsilon) > 0$ such that for all integers $Q \ge 3$, all real non-principal characters χ of conductor $q \le Q$, all integers $N \le Q^\eta$, and all integers M, we have*

$$\left| \sum_{M<a\le M+N} \chi(a) \right| \le CQ^{\eta(1-\delta)+\epsilon}.$$

We note that Conjecture C_η is known for $\eta > 1/4$, as a consequence of the classical Burgess's inequality [Bur63], and remains open for $\eta \le 1/4$. Moreover, for sums as above starting at $M = 0$, Conjecture C_η (for any η) is a consequence of the Grand Riemann Hypothesis for the L-function $L(s, \chi)$. We are now ready to state our main results.

Theorem 1.1. *Let K be a number field satisfying conditions $(P1)-(P5)$. Assume Conjecture C_η holds for $\eta = \frac{2}{n(n-1)}$. For $k \ne 1$ dividing n let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then for a fixed sign ±,*

$$d(F_\pm|S_\pm) = \frac{s_\pm}{2^{3(n-1)/2}}, \quad \textit{and} \quad d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}$$

where

$$s_+ = 1 + \prod_{\substack{k|n \\ d_k\, odd \\ k\ne 1}} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{\substack{k|n \\ d_k\, odd \\ k\ne 1}} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$s_- = \prod_{\substack{k|n \\ d_k\, even \\ k\ne 1}} (2^{d_k/2} + 1)^{\frac{\phi(k)}{d_k}} \prod_{\substack{k|n \\ d_k\, odd \\ k\ne 1}} (2^{d_k} - 1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function. In particular, when n is prime, writing $d = d_n$,

$$(s_+, s_-) = \begin{cases} \left(1 + 2^{\frac{n-1}{2d}}(2^{\frac{n-1}{2}} - 1),\ (2^d - 1)^{\frac{n-1}{2d}}\right) & \text{if } d \text{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}} + 1)^{\frac{n-1}{d}}\right) & \text{if } d \text{ is even.} \end{cases}$$

The density $d(F|S)$ is determined by the product of densities $d(F|R)$ and $d(R|S)$ where R is the set of primes satisfying a certain Hilbert symbol condition. Toward computing the density $d(R|S)$, the terms $s_\pm$ arise from counting the number of solutions to this Hilbert symbol condition over $(\mathcal{O}/4)^\times/((\mathcal{O}/4)^\times)^2$.

Table 1. Densities from Theorem 1.1, computed for K of degree n satisfying the necessary hypotheses.

n	$d(F_+\|S_+)$	$d(F_-\|S_-)$	$d(F\|S)$
3	1/8	3/8	1/4
5	1/64	5/64	3/64
7	15/512	7/512	11/512
9	1/4096	27/4096	7/2048
11	1/32768	33/32768	17/32768
13	1/262144	65/262144	33/262144
15	1/2097152	375/2097152	47/262144

In the cubic case, we have the following unconditional theorem.

Theorem 1.2. *Let $K/\mathbb{Q}$ be a cubic cyclic number field and odd class number in which 2 is inert. Then*

$$d(F|S) = \frac{1}{4},$$
$$d(F_+|S_+) = \frac{1}{8}, \quad \text{and} \quad d(F_-|S_-) = \frac{3}{8}.$$

For our main results, we have assumed that K satisfies properties (P1)-(P5). To start, we need properties (P1) and (P2) to define the extensions $K(p)/K$ for primes p that split completely in $K/\mathbb{Q}$. Coincidentally, as mentioned above, property (P2) also allows us to study the splitting behavior of all (not necessarily principal) prime ideals. Property (P3) ensures that $\mathrm{Gal}(K/\mathbb{Q})$ contains no involutions. While methods to deal with involutions do exist (see [FIMR13, Section 12, p. 745]), incorporating them into our arguments is nontrivial and may pose interesting new challenges in our analytic arguments. Properties (P4) and (P5) simplify our combinatorial arguments and allow us to give explicit density formulas. Removing the assumptions of properties (P4) and (P5) would pose new combinatorial challenges.

To end this section, we give some examples of number fields satisfying (P1)-(P5) so as to convince the reader that our theorems are not vacuous. First, many such fields can be found within the parametric families given by Friedlander et al. in [FIMR13, p. 712] and originally due to Shanks [Sha74] and Lehmer [Leh88], namely

$$\{\mathbb{Q}(\alpha_m) :\ m \in \mathbb{Z}\} \quad \text{and} \quad \{\mathbb{Q}(\beta_m) :\ m \in \mathbb{Z}\}$$

where α_m and β_m are roots of the polynomials

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

and

$$\begin{aligned} g_m(x) = x^5 &+ m^2x^4 - 2(m^3+3m^2+5m+5)x^3 \\ &+ (m^4+5m^3+11m^2+15m+5)x^2 + (m^3+4m^2+10m+10)x + 1, \end{aligned}$$

respectively. While $\mathbb{Q}(\alpha_m)$ and $\mathbb{Q}(\beta_m)$ always satisfy properties (P1), (P3), and (P4), for small m one can check for properties (P2) and (P5) using Sage or another similar mathematical software package. For instance, if β_7 is any root of

$$g_7(x) = x^5 + 49x^4 - 1060x^3 + 4765x^2 + 619x + 1,$$

then $\mathbb{Q}(\beta_7)$ is a totally real cyclic degree-5 number field of class number 1451 where 2 stays inert. We also note that one can use the law of cubic reciprocity to show that the fields $\mathbb{Q}(\alpha_m)$ always satisfy property (P5).

More generally, we can look for special subfields of cyclotomic fields. Let m be a prime number and ζ_m a primitive m-th root of unity, so that $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a cyclic extension of degree $\varphi(m)$, and suppose that n is an odd integer such that $\varphi(m) \equiv 0 \bmod 2n$. For instance, we can take n to be a Sophie Germain prime and then take $m = 2n+1$ to also be a prime. Suppose also that 2 is inert in $\mathbb{Q}(\zeta_m)$, i.e., that 2 is a primitive root modulo m. We then define K to be the unique subfield of $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ of degree n over $\mathbb{Q}$; K readily satisfies properties (P3)-(P5), while for small n the property that $\mathrm{Cl}^+ = \mathrm{Cl}$ and property (P2) can be checked using Sage. For instance, the unique degree-5 subfield of $\mathbb{Q}(\zeta_{191})$ has class number 11; it is isomorphic to $\mathbb{Q}(\beta_2)$ with β_2 a root of the polynomial g_2 as above.

2. Two Families of Number Fields

We say a modulus $\mathfrak{m}$ is *narrow* whenever it is divisible by all real infinite places. We say a modulus is *wide* whenever it is not divisible by any infinite place. We say a ray class group or ray class field is narrow or wide whenever its conductor is narrow or wide respectively.

For $\mathfrak{m}$ an ideal of $\mathcal{O}$, let $\mathrm{Cl}^+_{\mathfrak{m}}$ denote the narrow ray class group of conductor $\mathfrak{m}$. That is, $\mathrm{Cl}^+_{\mathfrak{m}}$ is the ray class group with conductor divisible by all real infinite places with finite part $\mathfrak{m}$.

The following lemma gives several equivalent formulations of property (P1).

Lemma 2.1. *Let K be a totally real number field. The following are equivalent.*

(1) $\mathrm{Cl}^+ = \mathrm{Cl}$.
(2) $\mathcal{O}^\times_+ = (\mathcal{O}^\times)^2$.
(3) *Every principal ideal has a totally positive generator.*
(4) *All signatures are represented by units.*

Proof. Since K is totally real, $\mathcal{O}^\times/(\mathcal{O}^\times)^2 \cong (\mathbb{Z}/2)^n$. Let $K^\times_+ := \{\alpha \in K^\times : \alpha \succ 0\}$. Using the narrow modulus with finite part 1, by Theorem V.1.7 [Mil13], there is an exact sequence,

$$1 \to \mathcal{O}^\times/\mathcal{O}^\times_+ \to K^\times/K^\times_+ \to \mathrm{Cl}^+ \to \mathrm{Cl} \to 1$$

and a canonical isomorphism $K^\times/K^\times_+ \cong (\mathbb{Z}/2)^n$. Therefore $\mathcal{O}^\times/\mathcal{O}^\times_+ \cong \mathcal{O}^\times/(\mathcal{O}^\times)^2$ if and only if $\mathrm{Cl}^+ \cong \mathrm{Cl}$. This proves that (1) is equivalent to (2). That (3) is equivalent to (1) follows from the definitions of the narrow and wide Hilbert class fields.

Two units are equivalent in $\mathcal{O}^\times/\mathcal{O}_+^\times$ exactly when they share the same signature. There are 2^n signatures. Noting that $(\mathcal{O}^\times)^2 \subseteq \mathcal{O}_+^\times$ and $\mathcal{O}^\times/(\mathcal{O}^\times)^2 \cong (\mathbb{Z}/2)^n$, it is therefore the case that $(\mathcal{O}^\times)^2$ and $\mathcal{O}_+^\times$ coincide exactly when all signatures are represented by units. □

Lemma 2.2. *Let K be a number field satisfying properties (P1) and (P2). In other words, suppose K is a totally real number field, Galois over $\mathbb{Q}$, such that the class number h is odd and $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$. Let $\mathfrak{p}$ be an odd prime of K. Then the narrow ray class field over K of conductor $\mathfrak{p}$ has a unique subextension that is quadratic over K.*

Proof. Let $\mathrm{Cl}_\mathfrak{p}^+$ denote the narrow ray class group over K of conductor $\mathfrak{p}$. We first show that $\mathrm{Cl}_\mathfrak{p}^+$ has even order. We then show that the 2-part of $\mathrm{Cl}_\mathfrak{p}^+$ is cyclic.

Let $h_\mathfrak{p}$ denote the order of $\mathrm{Cl}_\mathfrak{p}^+$. Let

$$\begin{aligned} K_{\mathfrak{p},1} &:= \{\alpha \in K^\times : \mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq 1, \alpha \succ 0\}, \\ \mathcal{O}_{\mathfrak{p},1}^\times &:= K_{\mathfrak{p},1} \cap \mathcal{O}^\times. \end{aligned}$$

Let $n := [K : \mathbb{Q}]$. By [Mil13, V.1.7], since K is totally real,

$$h_\mathfrak{p} = \frac{2^n(\mathfrak{N}(\mathfrak{p}) - 1)h}{(\mathcal{O}^\times : \mathcal{O}_{\mathfrak{p},1}^\times)}.$$

Since K is totally real and $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$,

$$(\mathcal{O}^\times : \mathcal{O}_{\mathfrak{p},1}^\times) = (\mathcal{O}^\times : \mathcal{O}_+^\times)(\mathcal{O}_+^\times : \mathcal{O}_{\mathfrak{p},1}^\times) = 2^n((\mathcal{O}^\times)^2 : \mathcal{O}_{\mathfrak{p},1}^\times).$$

Therefore

$$h_\mathfrak{p} = \frac{(\mathfrak{N}(\mathfrak{p}) - 1)h}{((\mathcal{O}^\times)^2 : \mathcal{O}_{\mathfrak{p},1}^\times)}.$$

Consider the injection $(\mathcal{O}^\times)^2/\mathcal{O}_{\mathfrak{p},1}^\times \hookrightarrow (\mathcal{O}/\mathfrak{p})^\times$ coming from the canonical isomorphism in [Mil13, V.1.7]. The image is contained in $\left((\mathcal{O}/\mathfrak{p})^\times\right)^2$ so $((\mathcal{O}^\times)^2 : \mathcal{O}_{\mathfrak{p},1}^\times)$ divides $(\mathfrak{N}(\mathfrak{p}) - 1)/2$. Therefore $h_\mathfrak{p}$ is even.

Now we show the 2-part of $\mathrm{Cl}_\mathfrak{p}^+$ is cyclic. Let L denote the maximal 2-extension of the narrow ray class field over K of conductor $\mathfrak{p}$. Let E denote the inertia group for $\mathfrak{p}$ relative to the extension L/K and let L_E denote the fixed field of E. Since $\mathfrak{p}$ is odd, $\mathfrak{p}$ is tamely ramified in L/K, so by [Mil08, 7.59], E is cyclic.

By Lemma 2.1, since $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$ and h is odd, Cl^+ also has odd degree over K. Therefore there is no non-trivial even extension of K in which all finite primes are unramified. All finite primes of K are unramified in L_E and $[L_E : K]$ divides $[L : K]$. Then since $[L : K]$ is a power of 2, $[L_E : K] = 1$ so $E = \mathrm{Gal}(L/\mathbb{Q})$. □

We may now define the multi-quadratic extension $K(p)/K$ as in Section 1.

Definition 2.3. *Let K be a number field satisfying properties (P1) and (P2).*

Given a prime p that splits completely in $K/\mathbb{Q}$ and a prime ideal $\mathfrak{p} \subset \mathcal{O}$ lying above p, let $K(\mathfrak{p})$ denote the unique quadratic subextension of the narrow ray class field over K of conductor $\mathfrak{p}$.

Furthermore, let $K(p)$ denote the compositum of the fields $K(\mathfrak{p}^\sigma)$ as σ ranges over $\mathrm{Gal}(K/\mathbb{Q})$.

We note that while each of the fields $K(\mathfrak{p}^\sigma)$ need not be Galois over $\mathbb{Q}$, their compositum $K(p)$ certainly is. Hence the residue field degree of p in $K(p)/\mathbb{Q}$ is well-defined, and we denote it by $f_{K(p)/\mathbb{Q}}(p)$.

For each number field K satisfying property (P1), we now define another family of number fields parametrized by prime numbers p. In the following, we will use the fact that for such K, a principal ideal always has a totally positive generator; see Lemma 2.1.

Definition 2.4. *Let K be a number field satisfying property (P1). Given a rational prime p, a prime ideal $\mathfrak{p} \subset \mathcal{O}$ lying above p, and a totally positive generator α of the principal ideal $\mathfrak{p}^h$, we define*

$$K_+(\mathfrak{p}) := K(\sqrt{\alpha}).$$

Define $K_+(p)$ to be the compositum of the number fields $K_+(\mathfrak{p}^\sigma)$ as σ ranges over $\mathrm{Gal}(K/\mathbb{Q})$.

We note that property (P1), i.e., that $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$, implies that $K_+(\mathfrak{p})$ does not depend on the choice of totally positive generator α. We also note, once again, that although $K_+(p)/\mathbb{Q}$ is Galois, each of the extensions $K_+(\mathfrak{p}^\sigma)/\mathbb{Q}$ need not be. As $K_+(p)/\mathbb{Q}$ is Galois, the ramification index and residue field degree of p, which we denote by $e_{K_+(p)/\mathbb{Q}}(p)$ and $f_{K_+(p)/\mathbb{Q}}(p)$, respectively, are well-defined.

Now suppose that K satisfies property (P2), i.e., that h is odd, and that p splits completely in $K/\mathbb{Q}$. Then there are n distinct primes in K lying above p, and they are of the form $\mathfrak{p}^\sigma$, where $\mathfrak{p}$ is one such prime and σ ranges over $\mathrm{Gal}(K/\mathbb{Q})$. Since h is odd, each of the extensions $K_+(\mathfrak{p}^\sigma)/K$ is a non-trivial quadratic extension whose discriminant is divisible by a prime, $\mathfrak{p}^\sigma$, that does not divide the discriminant of any of the other $n-1$ quadratic extensions. Thus, the degree of $K_+(p)/\mathbb{Q}$ is $n2^n$.

The following lemma describes how p can factor in $K_+(p)$.

Lemma 2.5. *Let K be a number field satisfying properties (P1) and (P2), let p be a prime that splits completely in $K/\mathbb{Q}$, and let $K_+(p)$ be as in Definition 2.4. Then*

1. $e_{K_+(p)/\mathbb{Q}}(p) = 2$.
2. $f_{K_+(p)/\mathbb{Q}}(p) \in \{1, 2\}$.

Proof. Let $e = e_{K_+(p)/\mathbb{Q}}(p)$, let $f = f_{K_+(p)/\mathbb{Q}}(p)$, and let g denote the number of distinct primes lying above p in $K_+(p)$. Then $n2^n = efg$ since $K_+(p)/\mathbb{Q}$ is Galois of degree $n2^n$.

Because each prime $\mathfrak{p}$ of K above p is ramified in $K_+(\mathfrak{p})$ with ramification index 2, and is unramified in $K_+(\mathfrak{p}^\sigma)$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, the overall ramification index of p in $K_+(p)/\mathbb{Q}$ is 2.

Finally, the residue field $\mathbb{Z}/p$ is cyclic and injects into $\mathcal{O}_{K_+(p)}/\mathfrak{P}$. Therefore $f \mid 2$ because there are no cyclic subextensions of $K_+(p)/K$ of degree greater than 2, and p is assumed to split completely in $K/\mathbb{Q}$. □

We will see in Corollary 3.7 that the residue field degrees of p in $K(p)/\mathbb{Q}$ and in $K_+(p)/\mathbb{Q}$ are equal, and that the possible factorizations of p in $K(p)/\mathbb{Q}$ are the same as in $K_+(p)/\mathbb{Q}$. Hence, to prove Theorem 1.1, we will prove the analogous results for the family of extensions $K_+(p)/\mathbb{Q}$.

3. The Spin of Prime Ideals

Throughout this section, we will assume that K is a number field satisfying properties (P1) and (P2), i.e., that K is a totally real Galois number field such that $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$ and such that the class number h of K is odd. We give the following definition of *spin*, which extends the definition of spin from [FIMR13] in a natural way so that it applies to all odd ideals (not necessary principal).

Definition 3.1. *Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be non-trivial. Given an odd ideal $\mathfrak{a}$, we define the spin of $\mathfrak{a}$ (with respect to σ) to be*

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

where α is any totally positive generator of the principal ideal $\mathfrak{a}^h$, and where $\left(\frac{\cdot}{\cdot}\right)$ denotes the quadratic residue symbol in K.

The assumption $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$ is important for two reasons. First, part (3) of Lemma 2.1 ensures that the principal ideal $\mathfrak{a}^h$ has a generator α that is totally positive. Second, any two totally positive generators of $\mathfrak{a}^h$ differ by a square, so the value of the quadratic residue symbol defining the spin does not depend on the choice of totally positive generator α.

If $\mathfrak{a}$ is an odd principal ideal and α_0 is a totally positive generator of $\mathfrak{a}$, then α_0^h is a totally positive generator for $\mathfrak{a}^h$. As h is odd, we have

$$\left(\frac{\alpha_0}{\mathfrak{a}^\sigma}\right) = \left(\frac{\alpha_0^h}{\mathfrak{a}^\sigma}\right),$$

so our definition coincides with that of Friedlander et al. in [FIMR13] for odd principal ideals $\mathfrak{a}$.

3.1. Known Results.

The main result in [FIMR13] can be stated as follows.

Theorem 3.2. *[FIMR13] Suppose K is a number field satisfying properties (P1) and (P4). Suppose $n = [K : \mathbb{Q}] \geq 3$. Assume Conjecture C_η holds for $\eta = 1/n$ with $\delta = \delta(\eta) > 0$. Let σ be a generator of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Then for all real numbers $x > 3$, we have*

$$\left| \sum_{\substack{\mathfrak{p} \text{ principal} \\ \text{prime ideal} \\ \mathfrak{N}(\mathfrak{p}) \leq x}} \mathrm{spin}(\mathfrak{p}, \sigma) \right| \ll x^{1-\theta+\epsilon}$$

where $\theta = \theta(n) = \frac{\delta}{2n(12n+1)}$. Here the implied constant depends only on ϵ and K.

Friedlander et al. also proved an analogous result for the case when the summation is restricted to principal prime ideals $\mathfrak{p}$ with totally positive generators satisfying a suitable congruence condition.

By Burgess's inequality, Conjecture C_η holds for $\eta = 1/3$ with $\delta = \frac{1}{48}$, so Theorem 3.2 holds unconditionally for $[K : \mathbb{Q}] = 3$ where $\theta = \frac{1}{10656}$.

In [FIMR13, Section 11], Friedlander et al. pose some questions about the joint distribution of $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ as $\mathfrak{p}$ varies over prime ideals, where σ and τ are two distinct generators of the cyclic group $\mathrm{Gal}(K/\mathbb{Q})$. In [KM], Koymans and Milovic prove that such spins are distributed independently if $n \geq 5$, i.e., that the product $\mathrm{spin}(\mathfrak{p},\sigma)\,\mathrm{spin}(\mathfrak{p},\tau)$ oscillates similarly as in Theorem 3.2. In fact, they prove that the product of spins

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

oscillates as long as the fixed non-empty subset S of $\mathrm{Gal}(K/\mathbb{Q})$ satisfies the property that $\sigma\notin S$ whenever $\sigma^{-1}\in S$. Moreover, their result holds for number fields K satisfying property (P1) and having arbitrary Galois groups, i.e., not necessarily satisfying property (P4).

The assumption in [KM] that $\sigma\notin S$ whenever $\sigma^{-1}\in S$ is made because $\mathrm{spin}(\mathfrak{p},\sigma)$ and $\mathrm{spin}(\mathfrak{p},\sigma^{-1})$ are not independent in the following sense. For a place v of K, let K_v denote the completion of K at v. For $a,b\in K$ coprime to v, the Hilbert Symbol $(a,b)_v$ is defined to be 1 if the equation $ax^2+by^2=z^2$ has a solution $x,y,z\in K_v$ with at least one of x, y, or z nonzero and -1 otherwise.

Proposition 3.3. *[FIMR13] Suppose K is a number field satisfying properties (P1) and (P4). Suppose $\mathfrak{p}\subset\mathcal{O}$ is a prime ideal and $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ is an automorphism such that $\mathfrak{p}$ and $\mathfrak{p}^\sigma$ are relatively prime. Then*

$$\mathrm{spin}(\mathfrak{p},\sigma)\,\mathrm{spin}(\mathfrak{p},\sigma^{-1})=\prod_{v|2}(\alpha,\alpha^\sigma)_v,$$

where α is a totally positive generator of $\mathfrak{p}^h$ and the product is taken over places v dividing 2.

Proof. This is essentially Lemma 11.1 in [FIMR13]. The proof uses the fact that

$$\prod_v(\alpha,\alpha^\sigma)_v=1.$$

Since $\alpha\succ0$, $(\alpha,\alpha^\sigma)_v=1$ for all infinite places v.

Consider v, a finite place not equal to $\mathfrak{p}$, $\mathfrak{p}^\sigma$ and not dividing 2. Since $v\neq\mathfrak{p},\mathfrak{p}^\sigma$, α and α^σ are nonzero modulo v. Consider the equation

$$\alpha^\sigma x^2\equiv1-\alpha y^2 \bmod v.$$

The right hand side and the left hand side each take on $(\mathfrak{N}(v)+1)/2$ values, so there is a solution by the pigeon hole principle.

It can not be the case that both x and y are 0. Suppose $x\not\equiv0 \bmod v$. Since v is prime to 2 and $x\not\equiv0$, Hensel's Lemma implies there exists a solution in the completion at v. Therefore $(\alpha,\alpha^\sigma)_v=1$. If y is nonzero, a similar argument works.

Since α and α^σ are relatively prime, $(\alpha,\alpha^\sigma)_{\mathfrak{p}}=\mathrm{spin}(\mathfrak{p},\sigma^{-1})$ and $(\alpha,\alpha^\sigma)_{\mathfrak{p}^\sigma}=\mathrm{spin}(\mathfrak{p},\sigma)$. Then since $\prod_v(\alpha,\alpha^\sigma)_v=1$, we are done. □

In this paper, we study the joint distribution of multiple spins $\mathrm{spin}(\mathfrak{p},\sigma)$, $\sigma\in S$, in a setting where there are in fact many $\sigma\in S$ such that $\sigma^{-1}\in S$ as well. From the discussion above, we see that this might involve combining the work of Koymans and Milovic with the study of the products $\mathrm{spin}(\mathfrak{p},\sigma)\,\mathrm{spin}(\mathfrak{p},\sigma^{-1})$ for various σ.

3.2. **Factorization and Spin.**

The spin of prime ideals is related to the splitting behavior of p in both $K_+(p)$ and $K(p)$ as we will see in Proposition 3.6 and Corollary 3.7.

Let $R_{\mathfrak{m}}^{+}$ denote the narrow ray class field over K of conductor $\mathfrak{m}$. Let $\mathfrak{p}$ be an odd prime of K. Recall from Definition 2.3 that Lemma 2.2 gives the existence of a unique quadratic subextension of $R_{\mathfrak{p}}^{+}/K$, denoted by $K(\mathfrak{p})$.

Proposition 3.4. *Suppose K is a number field satisfying properties (P1) and (P2). Let $\mathfrak{p} \subset \mathcal{O}$ be an odd prime ideal. Let $\alpha \in \mathcal{O}$ be a totally positive generator of $\mathfrak{p}^h$. Then*

$$K(\mathfrak{p}) = K(\sqrt{u\alpha})$$

for some unit $u \in \mathcal{O}^{\times}$ well-defined modulo $(\mathcal{O}^{\times})^2$. We denote the unit class of u by $\mathbf{u}_K(\mathfrak{p}) \in \mathcal{O}^{\times}/(\mathcal{O}^{\times})^2$. Furthermore, $\mathbf{u}_K(\mathfrak{p}^{\sigma}) = \mathbf{u}_K(\mathfrak{p})^{\sigma}$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Proof. By [Koc00, 3.10.3,3.10.4], $K(\mathfrak{p}) = K(\gamma)$ for some $\gamma \in \mathcal{O}$ with minimal polynomial over K Eisenstein at $\mathfrak{p}$. If $f_{\gamma}(x) = x^2 + c_1 x + c_0 \in K[x]$ is the minimal polynomial of γ over K, we could take $\gamma' := 2\gamma + c_1 \in K(\mathfrak{p})$ and the minimal polynomial of γ' is $x^2 - (c_1^2 - 4c_0)$, which is also Eisenstein at $\mathfrak{p}$ since $\mathfrak{p}$ is odd. Therefore we can assume the minimal polynomial of γ over K takes the form $f_{\gamma}(x) = x^2 - c$ for some $c \in \mathcal{O}$ where $f_{\gamma}(x)$ is Eisenstein at $\mathfrak{p}$.

If (c) had a prime factor $\mathfrak{q} \neq \mathfrak{p}$ with odd multiplicity, then $K(\mathfrak{p})$ would be ramified at $\mathfrak{q}$, which is impossible as $K(\mathfrak{p}) \subseteq R_{\mathfrak{p}}^{+}$. Therefore $(c) = \mathfrak{p}I^2$ for some ideal $I \subseteq \mathcal{O}$ coprime to $\mathfrak{p}$. Let $b \in \mathcal{O}$ be a generator of I^h. Let $\alpha \in \mathcal{O}$ be a totally positive generator of $\mathfrak{p}^h$, which exists by Lemma 2.1. Raising to the power of h gives $(c)^h = (\alpha)(b)^2$. Since h is odd, we can write

$$u\alpha = c\left(\frac{c^{(h-1)/2}}{b}\right)^2 \tag{1}$$

for some unit $u \in \mathcal{O}^{\times}$. Therefore

$$K(\sqrt{u\alpha}) = K(\sqrt{c}) = K(\gamma) = K(\mathfrak{p}).$$

As $K(\mathfrak{p}) \subset R_{\mathfrak{p}}^{+}$, we note that $u\alpha$ is a square in $R_{\mathfrak{p}}^{+}$.

If $u\alpha$ and $v\alpha$ are both squares in $R_{\mathfrak{p}}^{+}$ for $u, v \in \mathcal{O}^{\times}$, then $K(\sqrt{u\alpha})$ and $K(\sqrt{v\alpha})$ are both contained in $R_{\mathfrak{p}}^{+}$. By Lemma 2.2, this implies $K(\sqrt{u\alpha}) = K(\sqrt{v\alpha})$. Then we can write

$$\sqrt{u\alpha} = r_1 + r_2\sqrt{v\alpha}$$

for some $r_1, r_2 \in K$. Then $u\alpha = r_1^2 + 2r_1r_2\sqrt{v\alpha} + v\alpha r_2^2$ so one of r_1 or r_2 must be 0. Since $u\alpha$ generates a prime to an odd power, $u\alpha$ cannot be a square in K so $r_2 \neq 0$. Then $r_1 = 0$ so $u\alpha = v\alpha r_2^2$. Therefore r_2 is a unit and u and v represent the same class in $\mathcal{O}^{\times}/(\mathcal{O}^{\times})^2$.

It remains to prove that $\mathbf{u}_K(\mathfrak{p}^{\sigma}) = \mathbf{u}_K(\mathfrak{p})^{\sigma}$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{p}$, c, and α be as above, and let u be a unit in the class $\mathbf{u}_K(\mathfrak{p})$. It suffices to show that u^{σ} is in the class $\mathbf{u}_K(\mathfrak{p}^{\sigma})$. Note that α^{σ} is a totally positive generator of $(\mathfrak{p}^{\sigma})^h$. Hence it suffices to show that $K(\mathfrak{p}^{\sigma}) = K(\sqrt{u^{\sigma}\alpha^{\sigma}})$.

Now observe that since $x^2 - c$ is Eisenstein at $\mathfrak{p}$, $x^2 - c^{\sigma}$ is Eisenstein at $\mathfrak{p}^{\sigma}$. Hence

$$K(\mathfrak{p}^{\sigma}) = K(\sqrt{c^{\sigma}}) = K(\sqrt{(u\alpha)^{\sigma}}),$$

by (1), as desired. □

Lemma 3.5. *Suppose K is a number field satisfying properties (P1), (P2), and (P5). Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are distinct odd primes of K, and suppose α and β are* *totally positive generators of $\mathfrak{a}^h$ and $\mathfrak{b}^h$, respectively, such that 2 is unramified in $K(\sqrt{\beta})/K$. Then*

$$\left(\frac{\alpha}{\mathfrak{b}}\right) = \left(\frac{\beta}{\mathfrak{a}}\right),$$

where $(\cdot/\cdot)$ denotes the quadratic residue symbol in K.

Proof. Since h is odd and $\mathfrak{b}$ and $\mathfrak{a}$ are coprime, we have

$$\left(\frac{\alpha}{\mathfrak{b}}\right) = \left(\frac{\alpha}{\mathfrak{b}}\right)^h = \left(\frac{\alpha}{\mathfrak{b}^h}\right) = \left(\frac{\alpha}{\beta}\right). \tag{2}$$

Similarly,

$$\left(\frac{\beta}{\mathfrak{a}}\right) = \left(\frac{\beta}{\mathfrak{a}}\right)^h = \left(\frac{\beta}{\mathfrak{a}^h}\right) = \left(\frac{\beta}{\alpha}\right). \tag{3}$$

By the law of quadratic reciprocity for K [Neu99, Theorem VI.8.3, p. 415], we have

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\beta}{\alpha}\right) \prod_{v \mid 2\infty} (\alpha, \beta)_v,$$

where $(\cdot, \cdot)_v$ is the Hilbert symbol on K and the product above is over all places v lying above 2 and infinity.

For each infinite place v, we have $(\alpha, \beta)_v = 1$ since α is totally positive (and thus also positive in the embedding of K into $\mathbb{R}$ corresponding to v).

By assumption, 2 is inert in $K/\mathbb{Q}$, and we now prove that $(\alpha, \beta)_v = 1$ for the place v lying above 2 as well. $K_v(\sqrt{\beta})/K_v$ is unramified since 2 is unramified in $K(\sqrt{\beta})/K$ by assumption. If 2 splits in $K_v(\sqrt{\beta})/K_v$, i.e., if $K_v(\sqrt{\beta})/K_v$ is a trivial extension, then β is a square in K_v, which means that $\alpha x^2 + \beta y^2 = z^2$ has a nontrivial solution over K_v with $x = 0$ and $y = 1$. Otherwise, if 2 is inert in $K_v(\sqrt{\beta})/K_v$, then [Neu99, Corollary V.1.2, p. 319] implies that α is a norm from $K_v(\sqrt{\beta})$ to K_v. The corresponding norm equation gives a nontrivial solution of $\alpha x^2 + \beta y^2 = z^2$ over K_v with $x = 1$. In either case, we have shown that $(\alpha, \beta)_v = 1$ for the place v lying above 2.

We thus deduce that

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

which in combination with (3) and (2) yields the desired result. □

Given a rational prime p, fix a prime $\mathfrak{p}$ above p and a totally positive generator α of $\mathfrak{p}^h$. Recall from Definition 2.4 that $K_+(p)$ is the composite of $K_+(\mathfrak{p}^\sigma)$ as σ varies over all elements of $\mathrm{Gal}(K/\mathbb{Q})$, where $K_+(\mathfrak{p}^\sigma) := K(\sqrt{\alpha^\sigma})$. As before, denote by $K(\mathfrak{p}^\sigma)$ the unique quadratic subextension of the narrow ray class field over K of conductor $\mathfrak{p}^\sigma$.

The factorization of p in $K_+(p)$ or $K(p)$ is determined by the factorizations of $\mathfrak{p}$ in each $K_+(\mathfrak{p}^\sigma)$ or $K(\mathfrak{p}^\sigma)$ respectively, which is in turn determined by the spin of $\mathfrak{p}$ with respect to σ or σ^{-1}, respectively.

For an abelian extension of number fields L/E and a prime $\mathfrak{p}$ of E, let $f_{L/E}(\mathfrak{p})$ denote the residue field degree of $\mathfrak{p}$ in L/E.

Proposition 3.6. *Assume K satisfies properties (P1), (P2), and (P5). For a fixed odd prime $\mathfrak{p}$ of K that splits completely in $K/\mathbb{Q}$ and σ non-trivial in* $\mathrm{Gal}(K/\mathbb{Q})$, *the following are equivalent.*

(1) $\mathrm{spin}(\mathfrak{p},\sigma)=1$,
(2) $f_{K(\mathfrak{p}^\sigma)/K}(\mathfrak{p})=1$,
(3) $f_{K_+(\mathfrak{p}^{\sigma^{-1}})/K}(\mathfrak{p})=1$.

Proof. For $\gamma\in\mathcal{O}$, $L:=K(\sqrt{\gamma})$, and $\mathfrak{q}$ any prime of K, $f_{L/K}(\mathfrak{q})=1$ if and only if γ is a square modulo $\mathfrak{q}$ because the natural injective homomorphism of residue class fields is surjective exactly when $\sqrt{\gamma}$ has a pre-image. If $\mathfrak{q}$ is unramified in L/K, then $f_{L/K}(\mathfrak{q})=1$ exactly when the quadratic residue $(\gamma/\mathfrak{q})=1$.

Take $\mathfrak{p}$ to be an odd prime of K splitting completely in $K/\mathbb{Q}$, take α to be a totally positive generator of $\mathfrak{p}^h$, and take $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ non-trivial so that $\mathfrak{p}$ is unramified in $K_+(\mathfrak{p}^{\sigma^{-1}})/K$. Then $f_{K_+(\mathfrak{p}^{\sigma^{-1}})/K}(\mathfrak{p})=1$ if and only if

$$\left(\frac{\alpha^{\sigma^{-1}}}{\mathfrak{p}}\right)=\left(\frac{\alpha}{\mathfrak{p}^\sigma}\right)=\mathrm{spin}(\mathfrak{p},\sigma)=1.$$

By Proposition 3.4, $K(\mathfrak{p}^\sigma)=K(\sqrt{(u\alpha)^\sigma})$ where u is in the unit class $\mathbf{u}_K(\mathfrak{p})$. Then $f_{K(\mathfrak{p}^\sigma)/K}(\mathfrak{p})=1$ if and only if

$$\left(\frac{(u\alpha)^\sigma}{\mathfrak{p}}\right)=1.$$

Since $\mathfrak{p}$ and $\mathfrak{p}^\sigma$ are co-prime, and since 2 is unramified in $K(\sqrt{(u\alpha)^\sigma})$ because $K(\sqrt{(u\alpha)^\sigma})\subseteq R^+_{\mathfrak{p}^\sigma}$, by Lemma 3.5, $((u\alpha)^\sigma/\mathfrak{p})=(\alpha/\mathfrak{p}^\sigma)$. Therefore $f_{K(\mathfrak{p}^\sigma)/K}(\mathfrak{p})=1$ if and only if

$$\left(\frac{\alpha}{\mathfrak{p}^\sigma}\right)=\mathrm{spin}(\mathfrak{p},\sigma)=1.$$

□

Corollary 3.7. *For a fixed odd rational prime p splitting completely in $K/\mathbb{Q}$, the residue field degrees of p in the extensions $K(p)/\mathbb{Q}$ and $K_+(p)/\mathbb{Q}$ are equal to 1 if and only if $\mathrm{spin}(\mathfrak{p},\sigma)=1$ for all non-trivial $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$.*

Proof. $f_{K(p)/\mathbb{Q}}(p)=1$ exactly when $f_{K(\mathfrak{p}^\sigma)/K}(\mathfrak{p})=1$ for all $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$. Similarly, $f_{K_+(p)/\mathbb{Q}}(p)=1$ exactly when $f_{K_+(\mathfrak{p}^{\sigma^{-1}})/K}(\mathfrak{p})=1$ for all $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$. Apply Proposition 3.6. □

3.3. **Summary of Strategy.** Let Π denote the set of odd prime ideals of K. Let $\Lambda_\sigma:=\{\mathfrak{p}\in\Pi:\mathrm{spin}(\mathfrak{p},\sigma)=1\}$.

It is a Corollary of Theorem 3.2 that for a fixed generator $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$,

$$d(\Lambda_\sigma|\Pi)=\frac{1}{2},$$

and restriction to congruence classes does not change the density.

Let S be the set of rational primes that split completely in $K/\mathbb{Q}$. By Corollary 3.7,

$$\begin{aligned}F&:=\{p\in S:f_{K_+(p)/\mathbb{Q}}(p)=1\}\\&=\{p\in S:f_{K(p)/\mathbb{Q}}(p)=1\}\\&=\{p\in S:\mathrm{spin}(\mathfrak{p},\sigma)=1\text{ for all }\sigma\neq1\in\mathrm{Gal}(K/\mathbb{Q})\},\end{aligned}$$

where $\mathfrak{p}$ is a prime of K above p. Letting F' denote the set of primes of K above primes in F, then

$$F' = \bigcap_{\sigma \neq 1} \Lambda_\sigma,$$

the intersection taken over $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

If the spins of a fixed prime ideal $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ were independent for all non-trivial $\sigma \neq \tau \in \mathrm{Gal}(K/\mathbb{Q})$, then one might expect the density of F restricted to S to be $2^{-(n-1)}$. However, Proposition 3.3 gives a relation between the spins of a prime ideal suggesting the following strategy towards a proof of Theorem 1.1. Define

$$R := \{p \in S : \mathrm{spin}(\mathfrak{p}, \sigma)\, \mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = 1 \text{ for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})\},$$

where $\mathfrak{p}$ is a fixed prime of K above p. Observe that $F \subseteq R \subseteq S$, so if the limits exist then

$$d(F|S) = d(F|R)d(R|S).$$

We will see that R is in fact a Chebotarev class, and so $d(R|S)$ can be obtained via classical Dirichlet methods. We evaluate $d(F|R)$ in Section 6 using results from [KM]. The value of $d(R|S)$ is given by Proposition 5.3 together with Theorem 4.11.

4. A Consequence of Chebotarev's Theorem

In this section, we use Chebotarev's Theorem to prove that the primes of K are equidistributed in $\mathbf{M}_4$ as defined below, where the mapping takes primes to a totally positive generator considered in $\mathbf{M}_4$. This contributes toward the density $d(R|S)$ of rational primes p that satisfy the spin relation,

$$\mathrm{spin}(\mathfrak{p}, \sigma)\, \mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = 1 \quad \text{for all non-trivial } \sigma \in \mathrm{Gal}(K/\mathbb{Q}),$$

where $\mathfrak{p}$ is a prime of K above p, restricted to the rational primes splitting completely in $K/\mathbb{Q}$. We will also give this density restricted modulo $4\mathbb{Z}$. Theorem 4.11 and Proposition 5.3 together give the density of such primes satisfying the spin relation.

Definition 4.1. *For q a power of 2, define*

$$\mathbf{M}_q := (\mathcal{O}/q\mathcal{O})^\times / \left((\mathcal{O}/q\mathcal{O})^\times\right)^2.$$

Note that $\mathbf{M}_q$ is a group with a natural action from $\mathrm{Gal}(K/\mathbb{Q})$.

Proposition 4.2. *Let K be a cyclic number field of odd degree n over $\mathbb{Q}$ such that 2 is inert in K. Then*

1. *$\mathbf{M}_4 \cong (\mathbb{Z}/2)^n$ as $\mathbb{Z}/2$-vector spaces,*
2. *the invariants of the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbf{M}_4$ are exactly ± 1.*

Proof. Let $U_m := (\mathcal{O}/m)^\times$.

1. Fix a set of representatives $\mathcal{R}$ for $\mathcal{O}/2$ in $\mathcal{O}$. Let $\mathcal{R}^\times$ be a subset of $\mathcal{R}$ containing representatives for $(\mathcal{O}/2)^\times$. Observe that $\{x + 2y : x \in \mathcal{R}^\times, y \in \mathcal{R}\}$ is a set of representatives for U_4 and $\#U_4 = 2^n(2^n - 1)$. Therefore elements of U_4^2 are of the form $(x + 2y)^2 \equiv x^2 \bmod 4\mathcal{O}$ for $x \in \mathcal{R}^\times$ and $y \in \mathcal{R}$. Since $\#(\mathcal{O}/2)^\times = 2^n - 1$ is odd, the squaring map on $U_2 = (\mathcal{O}/2)^\times$ is surjective and so $\#U_4^2 = 2^n - 1$. Therefore $\#\mathbf{M}_4 = \#U_4/\#U_4^2 = 2^n$.

Since $\mathbf{M}_4$ is formed by taking the quotient of U_4 modulo squares, $\mathbf{M}_4$ is a direct product of cyclic groups of order 2.

For any $\alpha \in \mathcal{O}$ coprime to 2, write $[\alpha]$ as the projection of $\alpha\mathcal{O}$ in $\mathbf{M}_4$. Since every $x \in \mathcal{R}^\times$ is a square in U_2, we can write down the isomorphism explicitly with isomorphism

$$\mathbf{M}_4 \to \mathcal{O}/2 \cong \mathbb{F}_{2^n} \qquad [x+2y] = [1+2x^{-1}y] \mapsto x^{-1}y. \tag{4}$$

We see that $\mathbf{M}_4 = \{[1+2y] : y \in \mathcal{O}/2\}$.

(2) Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. The action of σ on $[1+2y] \in \mathbf{M}_4$, simply maps y to y^σ. Then we see that $y \equiv y^\sigma \bmod \mathcal{O}/2$ if and only if $y \equiv 0$ or $1 \bmod \mathcal{O}/2$. These correspond to ± 1 in $\mathcal{M}_4$.

□

Lemma 4.3. *The Hilbert symbol $(\cdot\,,\cdot)_2$ is well-defined on $\mathbf{M}_4$.*

Proof. We show that $(\alpha,\beta)_2 = (\alpha+4B,\beta)_2$ for any $B \in \mathcal{O}$ coprime to 2, which implies that $(\cdot\,,\cdot)_2$ is well-defined on $(\mathcal{O}/4\mathcal{O})^\times \times (\mathcal{O}/4\mathcal{O})^\times$. Suppose $B \in \mathcal{O}$ is coprime to 2. It suffices to show that $(\alpha,\beta)_2 = 1$ implies $(\alpha+4B,\beta)_2 = 1$. Take $x, y, z \in \mathcal{O}$ not all divisible by 2 satisfying $x^2 - \alpha y^2 = \beta z^2 \bmod 8$. Since $(\mathcal{O}/2\mathcal{O})^\times$ contains all its squares, there exists $C, D \in \mathcal{O}$ such that $C^2 \equiv \alpha^{-1}\beta B \bmod 2$ and $D^2 \equiv \alpha^{-1}\beta^{-1}B \bmod 2$. Take $X = x + 2Cz$, $y = Y$ and $Z = z + 2Dx$, then one can check that $X^2 - (\alpha+4B)Y^2 \equiv \beta Z^2 \bmod 8$. □

Lemma 4.4. *The Hilbert symbol $(\cdot\,,\cdot)_2$ is non-degenerate on $\mathbf{M}_4$.*

Proof. Fix some $\alpha \in \mathcal{O}$ coprime to 2. We claim that $(\alpha+4B, 2)_2 = 1$ for some $B \in \mathcal{O}$. Since $(\mathcal{O}/2\mathcal{O})^\times$ contains all its squareroots, there exist some $\gamma, z \in \mathcal{O}$ such that $\alpha \equiv \gamma^2 - 2z^2 \bmod 4$. Write $x = \gamma + 2x'$ for some $x' \in \mathcal{O}$, set $B = x'\gamma + x'^2$ and $y = 1$. Then $x^2 - (\alpha+4B)y^2 \equiv 2z^2 \bmod 8$. This proves our claim.

Now suppose $(\alpha,\beta)_2 = 1$ for all $\beta \in \mathcal{O}$ coprime to 2. Then taking B from the above claim, $(\alpha+4B,\beta)_2 = 1$ holds for all $\beta \in \mathcal{O}$ coprime to 2 by Lemma 4.3, and for all $\beta \in \mathcal{O}$ divisible by 2, by the above claim. Since the Hilbert symbol is non-degenerate on $K_2/K_2^\times$ [Ser79, Chapter XIV, Proposition 7], this implies that $\alpha + 4B \in \mathcal{O}^2$. Hence $[\alpha] = [\alpha+4B]$ is trivial in $\mathbf{M}_4$. □

For $\mathfrak{m}$ an ideal of K, let $\mathscr{P}_K^{\mathfrak{m}}$ denote the set of prime ideals of $\mathcal{O}$ co-prime to $\mathfrak{m}$. For K, totally real with odd class number h such that $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$, we can define the following map.

Definition 4.5. *For q a power of 2, define the map*

$$\begin{aligned} \mathbf{r}_q :&\mathscr{P}_K^2 \to \mathbf{M}_q \\ &\mathfrak{p} \mapsto \alpha \end{aligned}$$

where $\alpha \in \mathcal{O}$ is a totally positive generator of the principal ideal $\mathfrak{p}^h$.

Recall that as stated in Lemma 2.1, $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$ if and only if all principal ideals have a totally positive generator. Since squares are trivial in $\mathbf{M}_4$ by definition and $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$, the map $\mathbf{r}_q$ is well-defined. Note that $\mathbf{r}_q$ commutes with the Galois action, i.e. $\mathbf{r}_q(\mathfrak{p}^\sigma) = \mathbf{r}_q(\mathfrak{p})^\sigma$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

For $\mathfrak{m}$ an ideal of $\mathcal{O}$, let $J_K^{\mathfrak{m}}$ denote the group of fractional ideals of K prime to $\mathfrak{m}$.

Lemma 4.6. *[McM19] For K a totally real number field with odd class number satisfying the condition that $\mathcal{O}_{+}^{\times} = (\mathcal{O}^{\times})^2$, the homomorphism $J_K^2 \to \mathbf{M}_4$ induced by $\mathbf{r}_q$ induces a canonical surjective homomorphism,*

$$\varphi_q : \mathrm{Cl}_q^{+} \to \mathbf{M}_q.$$

Proof. We expand on the proof of Lemma 3.5 in [McM19]. In [McM19], the result is stated with more assumptions, but the same proof holds more generally.

The proof from [McM19] shows that φ_q is well-defined. We elaborate on the proof of surjectivity provided there. Let

$$K_{\mathfrak{m}} := \{a \in K^{\times} : \mathrm{ord}_2(a) = 0\}, \quad \text{and}$$
$$K_{\mathfrak{m},1} := \{a \in K^{\times} : \mathrm{ord}_2(a-1) \geq \mathrm{ord}_2(q), a \succ 0\}$$

We have the following commutative diagram of homomorphisms. The map ψ_0 is induced by the corresponding homomorphism in the exact sequence from class field theory as in [Mil13, V.1.7] and the map i is induced by the canonical isomorphism given in [Mil13, V.1.7].

$$\begin{tikzcd}
(K_{\mathfrak{m}}/K_{\mathfrak{m},1})/(K_{\mathfrak{m}}/K_{\mathfrak{m},1})^2 \arrow[r, "\psi_0"] \arrow[d, "i"'] & \mathrm{Cl}_4^{+}/(\mathrm{Cl}_4^{+})^2 \arrow[r, "\varphi_q"] & \mathbf{M}_q \\
(\pm)^n \times \mathbf{M}_q \arrow[ur, "\psi"'] & &
\end{tikzcd}$$

Fix $X \in \mathbf{M}_q$. Consider $(1, X) \in (\pm)^n \times \mathbf{M}_q$. Since i is an isomorphism, there exists $\beta \in (K_{\mathfrak{m}}/K_{\mathfrak{m},1})/(K_{\mathfrak{m}}/K_{\mathfrak{m},1})^2$ such that $i(\beta) = (1, X)$. Since $i(\beta)$ maps to 1 in the projection to $(\pm)^n$, β is totally positive. Since $\beta \succ 0$, we can choose $a, b \in \mathcal{O}$ totally positive such that $\beta = a/b$. (Writing $\beta = a/b$ for any $a, b \in \mathcal{O}$, one could then consider $\beta = a^2/ab$). Then $X = [ab^{-1}]$.

The map ψ_0 takes β to the class represented by the fractional ideal $(a)(b)^{-1}$. Since a and b are totally positive, $\varphi_q((a)(b)^{-1}) = [ab^{-1}] = X$ and so $\varphi_q \circ \psi$ is surjective, so φ_q is surjective. □

Lemma 4.7. *[McM19] Assume K satisfies (P1) and (P2).*

(1) *For any $\alpha \in \mathbf{M}_4$, the density of primes $\mathfrak{p}$ of K such that $\varphi_4(\mathfrak{p}) = \alpha$ is $\frac{1}{2^n}$. That is,*

$$d(\mathbf{r}_4^{-1}(\alpha)) = \frac{1}{\#\mathbf{M}_4} = \frac{1}{2^n}.$$

(2) *Furthermore, the density does not change when we restrict to primes of K that split completely in $K/\mathbb{Q}$. That is,*

$$d(\mathbf{r}_4^{-1}(\alpha) \cap S' | S') = \frac{1}{\#\mathbf{M}_4} = \frac{1}{2^n}.$$

Proof. See Lemma 4.3 in [McM19]. There the result is stated with more assumptions, but the same proof holds more generally. □

Definition 4.8. *Assume K satisfies (P1), (P2), and (P5). Let $\alpha \in \mathbf{M}_4$. Let $\mathfrak{p}$ be an odd prime of K such that $\mathbf{r}_4(\mathfrak{p}) = \alpha$. The map*

$$\begin{aligned} \mathbf{N} : \mathbf{M}_4 &\to (\mathbb{Z}/4)^\times \\ \alpha &\mapsto \mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p}) \bmod 4\mathbb{Z} \end{aligned}$$

is well-defined and $\mathbf{N}(\alpha) = \mathbf{N}(\alpha^\sigma)$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Proof. By Lemma 4.7, for any $\alpha \in \mathbf{M}_4$, there exists a prime $\mathfrak{p} \in \mathscr{P}_K^2$ such that $\mathbf{r}_4(\mathfrak{p}) = \alpha$.

Let $\mathfrak{p}$ and $\mathfrak{q}$ be (odd) primes of K such that $\mathbf{r}_4(\mathfrak{p}) = \mathbf{r}_4(\mathfrak{q})$. Let α be a totally positive generator of $\mathfrak{p}^h$ and let β be a totally positive generator of $\mathfrak{q}^h$, where h is the (odd) class number of K. Since $\mathbf{r}_4(\mathfrak{p}) = \mathbf{r}_4(\mathfrak{q})$, $\alpha \equiv \beta$ in $\mathbf{M}_4$. Then $\alpha \equiv \beta\gamma^2 \bmod 4\mathcal{O}$ for some $\gamma \in \mathcal{O}$. Since 2 is inert, $\alpha^\sigma \equiv \beta^\sigma(\gamma^\sigma)^2 \bmod 4\mathcal{O}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Therefore $\mathfrak{N}(\alpha) \equiv \mathfrak{N}(\beta)\mathfrak{N}(\gamma)^2 \bmod 4\mathcal{O}$. Since the norms are in $\mathbb{Z}$, $\mathfrak{N}(\alpha) \equiv \mathfrak{N}(\beta) \bmod 4\mathbb{Z}$. □

We now state an extended version of Lemma 4.7 that handles the densities restricted to primes of a fixed congruence class modulo $4\mathbb{Z}$.

Lemma 4.9. *Assume K satisfies conditions (P1)-(P3) and (P5). For a fixed sign $\pm$, let $S'_\pm$ denote the set of primes of K laying above some $p \in S$ such that $p \equiv \pm 1 \bmod 4\mathbb{Z}$. For any $\alpha \in \mathbf{M}_4$, the density of $\mathfrak{p} \in S'_\pm$ such that $\varphi_4(\mathfrak{p}) = \alpha$ is given by*

$$d(\mathbf{r}_4^{-1}(\alpha) \cap S'_\pm | S'_\pm) = \begin{cases} \frac{1}{2^{n-1}} & \textit{if } \mathbf{N}(\alpha) = \pm 1 \bmod 4 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. By Lemma 4.6, the map $\mathbf{r}_4 : \mathscr{P}_K^2 \to \mathbf{M}_4$ from Definition 4.5 induces a surjective canonical group homomorphism

$$\varphi_4 : \mathrm{Cl}_4^+ \twoheadrightarrow \mathbf{M}_4,$$

which commutes with the action from $\mathrm{Gal}(K/\mathbb{Q})$. Define $H := \mathrm{Art}(\ker(\varphi_4))$ where Art denotes the Artin map.

Let R_4^+ denote the narrow ray class field over K of conductor 4. Define L to be the fixed field of H in $\mathrm{Gal}(R_4^+/K)$. Then φ_4 induces a canonical isomorphism

$$\mathrm{Gal}(L/K) \cong \mathbf{M}_4,$$

which commutes with the action from $\mathrm{Gal}(K/\mathbb{Q})$.

Let $K_{\mathfrak{p},1} := \{\alpha \in K^\times : \mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq 1, \alpha \succ 0\}$ and $\mathcal{O}_{\mathfrak{p},1}^\times := K_{\mathfrak{p},1} \cap \mathcal{O}^\times$. Since K is totally real and $\mathcal{O}_+^\times = (\mathcal{O}^\times)^2$,

$$(\mathcal{O}^\times : \mathcal{O}_{\mathfrak{p},1}^\times) = (\mathcal{O}^\times : \mathcal{O}_+^\times)(\mathcal{O}_+^\times : \mathcal{O}_{\mathfrak{p},1}^\times) = 2^n((\mathcal{O}^\times)^2 : \mathcal{O}_{\mathfrak{p},1}^\times).$$

Therefore by [Mil13, V.1.7],

$$[R_4^+ : K] \mid h2^n(2^n - 1)$$

where h is the class number of K. We know $[L : K] = 2^n$ since $\mathrm{Gal}(L/K) \cong \mathbf{M}_4$ and $\#\mathbf{M}_4 = 2^n$ by Proposition 4.2. Therefore $[R_4^+ : L]$ is odd. Let F denote the composite of K and $\mathbb{Q}(\zeta_4)$. Since $[F : K] = 2$, $F \subseteq R_4^+$, and $[R_4^+ : L]$ is odd, $F \subseteq L$ and $[L : F] = 2^{n-1}$.

Let T/E be Galois extension of conductor dividing $\mathfrak{m}$, let p be a prime of E, and let $\tau \in \mathrm{Gal}(T/E)$. Let $(p, T/E)$ denote the conjugacy class of $\mathrm{Gal}(T/E)$ containing the Frobenius of $\mathfrak{p}$ where $\mathfrak{p}$ is a prime of T above p. Let

$$\begin{aligned}\mathcal{A}^{E}_{T|E}(\tau) &:= \{p \in \mathscr{P}^{\mathfrak{m}}_{E} : (p, T/E) = \langle \tau \rangle\},\\ \mathcal{A}^{T}_{T|E}(\tau) &:= \{\mathfrak{p} \in \mathscr{P}^{\mathfrak{m}}_{T} : \mathfrak{p} \text{ lies above } p \in \mathcal{A}^{E}_{T|E}(\tau)\}.\end{aligned}$$

Let $\alpha \in \mathbf{M}_4$ and let $\sigma \in \mathrm{Gal}(L/K)$ corresponding to α via the isomorphism induced by φ_4. Note that $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/\mathbb{Q})$.

Fix a sign ± and let $\tau_0 \in \mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$ such that

$$\mathcal{A}^{\mathbb{Q}}_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(\tau_0) = \{p \in \mathscr{P}^{2}_{\mathbb{Q}} : p \equiv \pm 1 \bmod 4\mathbb{Z}\}.$$

Note that since $n = [K : \mathbb{Q}]$ is odd and $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2$, $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$ canonically. Let $\tau \in \mathrm{Gal}(F/K)$ corresponding to τ_0 in $\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$. Note that $\mathrm{Gal}(F/K) \trianglelefteq \mathrm{Gal}(F/\mathbb{Q})$.

Recalling that φ_4 is induced by $\mathbf{r}_4$, observe that

$$\mathbf{r}_4^{-1}(\alpha) = \mathcal{A}^{K}_{L/K}(\sigma), \quad S' = \mathcal{A}^{K}_{K/\mathbb{Q}}(1), \quad \text{and} \quad S'_{\pm} = \mathcal{A}^{K}_{F/K}(\tau) \cap S'.$$

Then the density in question is

$$d_{\pm} := d\left(\frac{\mathbf{r}_4^{-1}(\alpha) \cap S'_{\pm}}{S'_{\pm}}\right) = d\left(\frac{\mathcal{A}^{K}_{K/\mathbb{Q}}(1) \cap \mathcal{A}^{K}_{L/K}(\sigma) \cap \mathcal{A}^{K}_{F/K}(\tau)}{\mathcal{A}^{K}_{K/\mathbb{Q}}(1) \cap \mathcal{A}^{K}_{F/K}(\tau)}\right)$$

Consider $\bar{\sigma} \in \mathrm{Gal}(F/K)$ taken to be the image of σ under the natural surjection,

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(F/K).$$

Note that $\bar{\sigma} = \tau$ exactly when $\mathbf{N}(\alpha) = \pm 1 \bmod 4$. If $\bar{\sigma} \neq \tau$ then $\mathbf{r}_4^{-1}(\alpha) \cap S'_{\pm} = \emptyset$ so the density in question is 0. We now assume $\mathbf{N}(\alpha) = \pm 1 \bmod 4$ so that $\bar{\sigma} = \tau$. Then

$$\mathcal{A}^{K}_{L/K}(\sigma) \cap \mathcal{A}^{K}_{F/K}(\tau) = \mathcal{A}^{K}_{L/K}(\sigma).$$

Therefore

$$d_{\pm} = d\left(\frac{\mathcal{A}^{K}_{K/\mathbb{Q}}(1) \cap \mathcal{A}^{K}_{L/K}(\sigma)}{\mathcal{A}^{K}_{K/\mathbb{Q}}(1) \cap \mathcal{A}^{K}_{F/K}(\tau)}\right).$$

Restricting to primes of norm over $\mathbb{Q}$ less than N, there are surjective maps of the following indices

$$\mathcal{A}^{K}_{K/\mathbb{Q}}(1) \cap \mathcal{A}^{K}_{L/K}(\sigma)|_N \to \mathcal{A}^{\mathbb{Q}}_{L/\mathbb{Q}}(\sigma)|_N \qquad \text{with index} = \#\,\mathrm{Stab}(\sigma)$$

and

$$\mathcal{A}^{K}_{K/\mathbb{Q}}(1) \cap \mathcal{A}^{K}_{F/K}(\tau)|_N \to \mathcal{A}^{\mathbb{Q}}_{F/\mathbb{Q}}(\tau)|_N \qquad \text{with index} = \#\,\mathrm{Stab}(\tau)$$

where $\mathrm{Stab}(\sigma)$ and $\mathrm{Stab}(\tau)$ denote the stabalizers of σ and τ respectively under the action from $\mathrm{Gal}(K/\mathbb{Q})$. Then by Chebotarev's Theorem (see Theorem [Neu99, VII.13.4] for Dirichlet density or [Ser81, 4] for natural density) and by the Orbit-Stabilizer Theorem,

$$\begin{aligned}
d_{\pm} &= \frac{\#\operatorname{Stab}(\sigma)}{\#\operatorname{Stab}(\tau)} d\left(\frac{\mathcal{A}^{\mathbb{Q}}_{L/\mathbb{Q}}(\sigma)}{\mathcal{A}^{\mathbb{Q}}_{F/\mathbb{Q}}(\tau)}\right) \\
&= \frac{\#\operatorname{Stab}(\sigma) d(\mathcal{A}^{\mathbb{Q}}_{L/\mathbb{Q}}(\sigma))}{\#\operatorname{Stab}(\tau) d(\mathcal{A}^{\mathbb{Q}}_{F/\mathbb{Q}}(\tau))} \\
&= \left(\frac{\#\operatorname{Stab}(\sigma)\#\langle\sigma\rangle}{\#\operatorname{Stab}(\tau)\#\operatorname{Gal}(L/K)}\right) \Big/ \left(\frac{\#\langle\tau\rangle}{\#\operatorname{Gal}(F/K)}\right) \\
&= \frac{\#\operatorname{Stab}(\sigma)\#\langle\sigma\rangle}{\#\operatorname{Stab}(\tau)\#\langle\tau\rangle\,\#\operatorname{Gal}(L/F)} \\
&= \frac{1}{\#\operatorname{Gal}(L/F)} \\
&= \frac{1}{2^{n-1}}.
\end{aligned}$$

□

Recall that Proposition 3.3 stated that for $\mathfrak{p}$ a prime of K with totally positive generator $\alpha \in \mathcal{O}$, and for $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ a generator,

$$\operatorname{spin}(\mathfrak{p},\sigma)\operatorname{spin}(\mathfrak{p},\sigma^{-1}) = (\alpha,\alpha^{\sigma})_2,$$

which motivates the following definition.

Definition 4.10. *[McM19] Assume K satisfies (P1), (P2), and (P5) with abelian Galois group. Let $\alpha \in \mathcal{O}$ denote a representative of $\bar{\alpha} \in \mathbf{M}_4$. Define the map*

$$\begin{aligned}
\star:\ \mathbf{M}_4 &\to \{\pm 1\} \\
\bar{\alpha} &\mapsto \begin{cases} 1 & \textit{if } (\alpha,\alpha^{\sigma})_2 = 1 \textit{ for all non-trivial } \sigma \in \operatorname{Gal}(K/\mathbb{Q}), \\ -1 & \textit{otherwise.} \end{cases}
\end{aligned}$$

Observe that $\star$ is a well-defined map by Lemma 4.3. If (5) holds for some $\alpha \in \mathcal{O}$, then it holds for α^{σ} for any $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$. Therefore $\star(\alpha) = \star(\alpha^{\sigma})$ for all $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$.

Recall the map $\mathbf{N} : \mathbf{M}_4 \to \pm 1$ from Definition 4.8. Let $\star_+$ denote the restriction of $\star$ to

$$\mathbf{M}_4^+ := \{\alpha \in \mathbf{M}_4 : \mathbf{N}(\alpha) = 1\}$$

and let $\star_-$ denote the restriction of $\star$ to

$$\mathbf{M}_4^- := \{\alpha \in \mathbf{M}_4 : \mathbf{N}(\alpha) = -1\}.$$

Define S_+ to be the set of odd rational primes congruent to $1 \mod 4$ that split completely in $K/\mathbb{Q}$. Similarly, define S_- to be the set of odd rational primes congruent to $-1 \mod 4$ that split completely in $K/\mathbb{Q}$. Recall

$$R := \{p \in S : \operatorname{spin}(\mathfrak{p},\sigma)\operatorname{spin}(\mathfrak{p},\sigma^{-1}) = 1 \text{ for all } \sigma \neq 1 \in \operatorname{Gal}(K/\mathbb{Q})\}.$$

For a fixed sign ±, define $R_{\pm} := R \cap S_{\pm}$.

Theorem 4.11. *Assume K satisfies properties (P1)-(P5). Then*

$$d(R|S) = \frac{\#\ker(\star)}{2^n},$$

$$d(R_+|S_+) = \frac{\#\ker(\star_+)}{2^{n-1}} \quad \textit{and} \quad d(R_-|S_-) = \frac{\#\ker(\star_-)}{2^{n-1}}.$$

Proof. That $d(R|S) = \#\ker(\star)/2^n$ is proven in [McM19, 6.2], though it will also follow from the proof that $d(R_\pm|S_\pm) = \#\ker(\star_\pm)/2^{n-1}$ since $d(S_\pm|S) = 1/2$ and $\ker(\star)$ is the disjoint union of $\ker(\star_+)$ and $\ker(\star_-)$ and R is the disjoint union of R_+ and R_-.

Recall the map $\mathbf{r}_4$ from Definition 4.5. As shown in Definition 4.10, $\star(\alpha) = \star(\alpha^\sigma)$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ so $\star \circ \mathbf{r}_4(\mathfrak{p}) = \star \circ \mathbf{r}_4(\mathfrak{p}^\sigma)$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. By Proposition 3.3, for each fixed sign $\pm$,

$$R_\pm = \{p \in S_\pm : \star \circ \mathbf{r}_4(\mathfrak{p}) = 1 \text{ for } \mathfrak{p} \text{ a prime of } K \text{ above } p\}.$$

For $N \in \mathbb{Z}_+$, let $R_{\pm,N} := \{p \in R_\pm : p < N\}$ and $S_{\pm,N} := \{p \in S_\pm : p < N\}$. We will prove that

$$d(R_\pm|S_\pm) = \frac{\#\ker(\star_\pm)}{\#\mathbf{M}_4^\pm}.$$

Then since K is cyclic of odd degree and 2 is inert in $K/\mathbb{Q}$, we can apply Proposition 4.2 to get that $\#\mathbf{M}_4 = 2^n$. Then since half the elements of $\mathbf{M}_4$ are in $\mathbf{M}_4^+$ and half in $\mathbf{M}_4^-$, $\#\mathbf{M}_4^+ = \#\mathbf{M}_4^- = 2^{n-1}$.

Let $\pm$ denote a fixed sign and let $\mp$ denote the opposite sign. Let $S'_{\pm,N}$ denote the set of primes of K laying above primes in $S_{\pm,N}$ and let $R'_{\pm,N}$ denote the set of primes of K laying above primes in $R_{\pm,N}$. Since primes in S split completely,

$$\frac{\#R_{\pm,N}}{\#S_{\pm,N}} = \frac{\#R'_{\pm,N}}{\#S'_{\pm,N}}.$$

Let $\mathbf{r}_{4,N}$ denote the restriction of $\mathbf{r}_4$ to $S'_{\pm,N}$. Then $R'_{\pm,N}$ is the disjoint union

$$R'_{\pm,N} = \bigsqcup_{\alpha \in \ker(\star_\pm)} \left(S'_{\pm,N} \cap \mathbf{r}_{4,N}^{-1}(\alpha)\right),$$

taken over elements $\alpha \in \ker(\star_\pm)$, i.e. elements of $\alpha \in \mathbf{M}_4$ such that $\mathbf{N}(\alpha) = \pm 1 \bmod 4$ and $\star(\alpha) = 1$. Therefore

$$\frac{\#R'_{\pm,N}}{\#S'_{\pm,N}} = \sum_{\alpha \in \ker(\star_\pm)} \frac{\#\left(S'_{\pm,N} \cap \mathbf{r}_{4,N}^{-1}(\alpha)\right)}{\#S'_{\pm,N}}$$

By Lemma 4.9, for all $\alpha \in \ker(\star_\pm)$,

$$d(\mathbf{r}_4^{-1}(\alpha) \cap S'_\pm|S'_\pm) = \frac{1}{\#\mathbf{M}_4^\pm} = \frac{1}{2^{n-1}}.$$

Therefore

$$\begin{aligned} d(R_{\pm}|S_{\pm}) = d(R'_{\pm}|S'_{\pm}) &= \lim_{N\to\infty} \sum_{\alpha\in\ker(\star_{\pm})} \frac{\#\left(S'_{\pm,N}\cap \mathbf{r}_{4,N}^{-1}(\alpha)\right)}{\# S'_{\pm,N}} \\ &= \sum_{\alpha\in\ker(\star_{\pm})} \lim_{N\to\infty} \frac{\#\left(S'_{\pm,N}\cap \mathbf{r}_{4,N}^{-1}(\alpha)\right)}{\# S'_{\pm,N}} \\ &= \sum_{\alpha\in\ker(\star_{\pm})} d(\mathbf{r}_4^{-1}(\alpha)\cap S'_{\pm}|S'_{\pm}) \\ &= \sum_{\alpha\in\ker(\star_{\pm})} \frac{1}{2^{n-1}} = \frac{\#\ker(\star_{\pm})}{2^{n-1}}. \end{aligned}$$

□

5. Counting Solutions to a Hilbert Symbol Condition

In this section, we will prove formulae for $\#\ker(\star_{\pm})$. Recall that $K/\mathbb{Q}$ be cyclic odd degree n extension and 2 is inert in $K/\mathbb{Q}$.

Lemma 5.1. $(-1,-1)_2 = -1$.

Proof. Assume for contradiction that $(-1,1)_2 = 1$. Consider a homomorphism $\psi : \mathbf{M}_4 \to \{\pm 1\}$ given by $[\alpha] \mapsto (\alpha,-1)_2$. Since the Hilbert symbol is non-degenerate, and -1 is not a square modulo 4 in K, ψ is not identically 1. Therefore the size of $\ker\psi$ is $|\mathbf{M}_4|/|\operatorname{im}\psi| = 2^{n-1}$.

For any $[\alpha] \in \mathbf{M}_4 \setminus \{\pm 1\}$, we have $(\alpha_{(k)},-1)_2 = (\alpha,-1)_2$ for any k. Therefore ψ is stable under the Galois action. The size of each Galois orbit is n except the orbit of ± 1. But then n divides both $|\{[\alpha] \in \mathbf{M}_4 \setminus \{\pm 1\} : \psi(\alpha) = 1\}| = |\{[\alpha] \in \mathbf{M}_4 : \psi(\alpha) = 1\}| - 2 = 2^{n-1} - 2$ and $|\{[\alpha] \in \mathbf{M}_4 : \psi(\alpha) = -1\}| = 2^{n-1}$, which is a contradiction. □

Our aim is to count the number of elements in $\mathbf{M}_4$ with a representative $\alpha \in \mathcal{O}$ satisfying the spin relation

$$(\alpha, \alpha^{\sigma})_2 = 1 \text{ for all non-trivial } \sigma \in \operatorname{Gal}(K/\mathbb{Q}). \tag{5}$$

By Lemma 4.4, the property (5) only depends on the class of $[\alpha] \in \mathbf{M}_4$.

Fix σ to be a generator of $\operatorname{Gal}(K/\mathbb{Q})$. Write $\alpha_{(k)} := \alpha^{\sigma^k}$ for $k \in \mathbb{Z}$.

5.1. The Hilbert symbol as a bilinear form on $\mathbf{M}_4$.

By the Kronecker–Weber theorem, K is contained in the cyclotomic field $\mathbb{Q}(\zeta_{\mathfrak{f}})$, where $\mathfrak{f}$ is the conductor of K. The conductor $\mathfrak{f}$ is odd since we assumed that 2 is unramified in K. By [FvzGS99, Theorem 4.5], there exists a normal 2-integral basis of $\mathbb{Q}(\zeta_{\mathfrak{f}})$, i.e. we can find some $a \in \mathcal{O}_{\mathbb{Q}(\zeta_{\mathfrak{f}})}$ such that the localization of $\mathcal{O}_{\mathbb{Q}(\zeta_{\mathfrak{f}})}$ at 2 can be written as $\mathcal{O}_{\mathbb{Q}(\zeta_{\mathfrak{f}}),2} = \oplus_{g\in\operatorname{Gal}(\mathbb{Q}(\zeta_{\mathfrak{f}})/\mathbb{Q})} \mathbb{Z}_{(2)} a^g$. Similar to the classic result for integral bases [Nar04, Proposition 4.31(i)], taking $y = \operatorname{Tr}_{\mathbb{Q}(\zeta_{\mathfrak{f}})/K}(a)$, then $\{y, y^{\sigma}, \ldots, y^{\sigma^{n-1}}\}$ gives a normal 2-integral basis of K. Since $\mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathcal{O}_{K,2}/2\mathcal{O}_{K,2} \cong \mathcal{O}/2\mathcal{O}$, we know that $y, y^{\sigma}, \ldots, y^{\sigma^{n-1}}$ also form a normal $\mathbb{F}_2$-basis of $\mathcal{O}/2\mathcal{O}$.

Set $\alpha = 1 + 2y$. It follows from the isomorphism in (4) that

$$\mathbf{M}_4 = \left\{ \prod_{i=1}^{n-1} [\alpha_{(i)}]^{u_i} : (u_0, \dots, u_{n-1}) \in \mathbb{F}_2^n \right\}.$$

Write $(\alpha, \alpha_{(i)})_2 = (-1)^{c_i}$, $c_i \in \{0, 1\}$. Note that $(\alpha_{(i)}, \alpha_{(j)})_2 = (\alpha, \alpha_{(j-i)})_2$. The Hilbert symbol is multiplicatively bilinear, so we can represent $(\,\cdot\,,\,\cdot\,)_2$ by the matrix

$$A := \begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \dots & c_1 \\ c_1 & c_0 & c_{n-1} & \dots & c_2 \\ c_2 & c_1 & c_0 & \dots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_0 \end{pmatrix}$$

with respect to the basis $[\alpha_{(i)}]$, $0 \le i \le n-1$. For any $\mathbf{u} = (u_0, \dots, u_{n-1}), \mathbf{v} = (v_0, \dots, v_{n-1}) \in \mathbb{F}_2^n$, we have

$$\left(\prod_i \alpha_{(i)}^{u_i}, \prod_j \alpha_{(j)}^{v_j} \right)_2 = (-1)^{\mathbf{u}^T A \mathbf{v}}.$$

Since $(\,\cdot\,,\,\cdot\,)_2$ is non-degenerate on $\mathbf{M}_4$ by Lemma 4.4, the matrix A has rank n and is invertible. Note also that A is symmetric.

Define the $n \times n$ $\mathbb{F}_2$-matrix

$$T_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

$T_k = T_1^k$ and $T_0 = I$. Then $\prod_i \alpha_{(i)}^{u_i}$, $\mathbf{u} = (u_0, \dots, u_{n-1}) \in \mathbb{F}_2^n$ satisfies (5) if and only if

$$\mathbf{u}^T A T_1 \mathbf{u} = \mathbf{u}^T A T_2 \mathbf{u} = \dots = \mathbf{u}^T A T_{n-1} \mathbf{u} = 0. \tag{6}$$

Since $\{T_0, T_1, \dots, T_{n-1}\}$ is a basis of $\mathrm{GL}_n(\mathbb{F}_2)$, we can write

$$A = \sum_{i=0}^{n-1} c_i T_i, \qquad c_i \in \mathbb{F}_2.$$

Then (6) becomes

$$A \begin{pmatrix} \mathbf{u}^T T_0 \mathbf{u} \\ \mathbf{u}^T T_1 \mathbf{u} \\ \vdots \\ \mathbf{u}^T T_{n-1} \mathbf{u} \end{pmatrix} \in \left\{ \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}. \tag{7}$$

There is the following one-to-one correspondence

$$\begin{aligned} \Psi : & \mathbb{F}_2^n \to \mathbb{F}_2[x]/(x^n - 1) \\ & \mathbf{u} = (u_0, \dots, u_{n-1}) \mapsto F_{\mathbf{u}}(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{n-1} x^{n-1}. \end{aligned}$$

Define a map

$$\begin{aligned} B : \mathbb{F}_2^n \to \mathbb{F}_2^n &\xrightarrow{\Psi} \mathbb{F}_2[x]/(x^n-1) \\ \mathbf{u} \mapsto (\mathbf{u}^T T_0 \mathbf{u},\ \mathbf{u}^T T_1 \mathbf{u},\ \dots,\ \mathbf{u}^T T_{n-1}\mathbf{u}) &\mapsto x^n \cdot F_{\mathbf{u}}(x) F_{\mathbf{u}}(1/x) \bmod (x^n-1). \end{aligned}$$

Since A is invertible, we can set $h(x) = \Psi(A^{-1}(1,0,\dots,0))$. Then (7) becomes $B(\mathbf{u}) \in \{0, h(x)\}$. Since A is symmetric, A^{-1} is also symmetric, so $h(x) \equiv x^n h(1/x) \bmod (x^n-1)$. In particular $\#\ker(\star_+) = \left|B^{-1}(0)\right|$ and $\#\ker(\star_-) = \left|B^{-1}(h(x))\right|$.

5.2. **The counting problem.** Our aim is to obtain the size of the preimage of 0 and $h(x)$ under B. For any polynomial f, let f^* denote its reciprocal, i.e. $f^*(x) = x^{\deg f} \cdot f(1/x)$.

The first case $B(\mathbf{u}) = 0$ implies $(x^n - 1) \mid F_{\mathbf{u}}(x) F_{\mathbf{u}}^*(x)$.

Lemma 5.2. *For any factor $k \neq 1$ of n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Also set $d_1 = 1$. Consider the following factorisation in $\mathbb{F}_2[x]$,*

$$x^n - 1 = f_1(x) \dots f_r(x) f_{m+1}^*(x) \dots f_r^*(x), \tag{8}$$

where f_i are irreducible and $f_i = f_i^*$ for $i = 1, \dots, m$. Then $\sum_{i=1}^r \deg f_i = \sum_{k|n} r_k d_k$ and $r = \sum_{k|n} r_k$ and $m = \sum_{k|n} m_k$, where $r_1 = m_1 = 1$, and

$$(r_k, m_k) = \begin{cases} \left(\frac{\phi(k)}{2d_k},\ 0\right) & \text{if } d_k \text{ is odd,} \\ \left(\frac{\phi(k)}{d_k},\ \frac{\phi(k)}{d_k}\right) & \text{if } d_k \text{ is even,} \end{cases}$$

for $k \neq 1$.

Proof. Take f to be an irreducible factor of $x^n - 1$ in $\mathbb{F}_2[x]$. Let γ be a root of f in an extension of $\mathbb{F}_2$. Then γ is a primitive k-th root of unity, where k is some integer dividing n. Galois theory on finite fields shows that $\mathrm{Gal}(\mathbb{F}_2(\gamma)/\mathbb{F}_2)$ is generated by the Frobenius $\varphi : x \mapsto x^2$. Since $\varphi^i : x \mapsto x^{2^i}$ for any $i \in \mathbb{Z}$, we see that the order of φ must be d_k, the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Therefore $\deg f = d_k$. The set of roots of f is $\{\gamma, \varphi(\gamma), \varphi^2(\gamma), \dots, \varphi^{d_k - 1}(\gamma)\}$, which is closed under inversion precisely when d_k is even. Therefore f is self-reciprocal if and only if d_k is even. There are $\phi(k)$ roots of $x^n - 1$ which are primitive k-th root of unity, so $(2r_k - m_k)d_k = \phi(k)$. □

Obtain the following factorisation in $\mathbb{F}_2[x]$ as described in Lemma 5.2,

$$x^n - 1 = f_1(x) \dots f_r(x) f_{m+1}^*(x) \dots f_r^*(x), \tag{9}$$

where $f_1(x) = x + 1$, f_i are irreducible and $f_i = f_i^*$ for $i = 1, \dots, m$. Write $F_{\mathbf{u}} = G \cdot H$, where $G = \gcd(F_{\mathbf{u}}, x^n - 1)$. Then for each $k = 0, \dots, r$, we have $f_k \mid F_{\mathbf{u}}$ or $f_i^* \mid F_{\mathbf{u}}$. This leaves us with 2^{r-m} choices for G. Since

$$\deg\left((x^n-1)/G\right) = n - \sum_{i=1}^r \deg f_i = \sum_{k|n} (r_k - m_k) d_k,$$

There are $2^{\sum_{k|n}(r_k - m_k)d_k} - 1$ choices for $H \not\equiv 0 \bmod (x^n-1)/G$, so

$$\#\ker(\star_+) = 1 + \left|B^{-1}(0) \setminus \{0\}\right| = 1 + 2^{r-m}\left(2^{\sum_{k|n}(r_k - m_k)d_k} - 1\right). \tag{10}$$

The second case $B(\mathbf{u}) = h(x)$. We count the number of $\mathbf{u} \in \mathbb{F}_2^n$ such that

$$x^n \cdot F_{\mathbf{u}}(x) F_{\mathbf{u}}(1/x) \equiv h(x) \bmod (x^n - 1). \tag{11}$$

Fix a primitive complex n-th root of unity ζ_n. Consider the isomorphism

$$(\mathbb{F}_2[x]/(x^n-1))^\times \to (\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times \qquad F_{\mathbf{u}}(x) \mapsto F_{\mathbf{u}}(\zeta_n) \bmod 2.$$

Now (11) becomes

$$F_{\mathbf{u}}(\zeta_n)\overline{F_{\mathbf{u}}(\zeta_n)} \equiv h(\zeta_n) \bmod 2.$$

Notice that $h(\zeta_n) = h(\zeta_n^{-1}) = \overline{h(\zeta_n)}$ is real. We compute from (9),

$$\begin{aligned}
&\left|(\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times\right| \\
&= \left|(\mathbb{F}_2[x]/(x^n-1))^\times\right| \\
&= \left|(\mathbb{F}_2[x]/(f_1))^\times \times \cdots \times (\mathbb{F}_2[x]/(f_r))^\times \times (\mathbb{F}_2[x]/(f_{m+1}^*))^\times \times \cdots \times (\mathbb{F}_2[x]/(f_r^*))^\times\right| \\
&= \prod_{k|n} (2^{d_k}-1)^{2r_k - m_k}.
\end{aligned}$$

Take $g \in \mathbb{F}_2[x]$ such that

$$\frac{x^n-1}{x-1} \equiv x^{n-1} + x^{n-2} + \cdots + x + 1 = x^{\frac{n-1}{2}} g(x + x^{-1}).$$

We can factorise $g(x) = g_2(x)\dots g_r(x)$, where $x^{\deg g_k} \cdot g_k(x+x^{-1}) = f_k(x)$ for $2 \le k \le m$ and $x^{\deg g_k} \cdot g_k(x+x^{-1}) = f_k(x) f_k^*(x)$ for $m+1 \le k \le r$. Then since $(\mathbb{Z}[\zeta_n + \zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times \cong (\mathbb{F}_2[x]/(g))^\times$, we compute

$$\begin{aligned}
\left|(\mathbb{Z}[\zeta_n + \zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times\right| &= \left|(\mathbb{F}_2[x]/(g))^\times\right| \\
&= \left|(\mathbb{F}_2[x]/(g_2))^\times \times \cdots \times (\mathbb{F}_2[x]/(g_r))^\times\right| \\
&= \prod_{k|n,\ k\neq 1} (2^{d_k/2}-1)^{m_k}(2^{d_k}-1)^{r_k-m_k}.
\end{aligned}$$

Our goal is to compute the size of the kernel of the homomorphism

$$\psi : (\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times \to (\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times \qquad \beta \mapsto \beta\overline{\beta}.$$

We claim that ψ is surjective. Since $(\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times$ has odd order, every element is a square, so suppose $\beta^2 \in (\mathbb{Z}[\zeta_n+\zeta_n^{-1}]/2\mathbb{Z}[\zeta_n+\zeta_n^{-1}])^\times$, then $\psi(\hat{\beta}) = \beta^2$ for any lift $\hat{\beta} \in \mathbb{Z}[\zeta_n+\zeta_n^{-1}]$ of β. Therefore

$$\begin{aligned}
(12)\quad \#\ker(\star_-) = \left|B^{-1}(h(x))\right| = |\ker\psi| &= \frac{|(\mathbb{Z}[\zeta_n]/2\mathbb{Z}[\zeta_n])^\times|}{|\mathrm{im}\,\psi|} \\
&= \prod_{k|n,\ k\neq 1} (2^{d_k/2}+1)^{m_k}(2^{d_k}-1)^{r_k-m_k}.
\end{aligned}$$

Putting in (10) and (12) the values of r and m in terms of n and d as in Lemma 5.2, we have the following.

Proposition 5.3. *For each $k \neq 1$ dividing n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then*

$$\#\ker(\star_+) = 1 + \prod_{k|n,\ d_k\,odd,\ k\neq 1} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{k|n,\ d_k\,odd,\ k\neq 1} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$\#\ker(\star_-) = \prod_{k|n,\ d_k\,even,\ k\neq 1} (2^{d_k/2}+1)^{\frac{\phi(k)}{d_k}} \prod_{k|n,\ d_k\,odd,\ k\neq 1} (2^{d_k}-1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function. If n is a prime, then writing $d = d_n$,

$$(\#\ker(\star_+), \#\ker(\star_-)) = \begin{cases} \left(1 + 2^{\frac{n-1}{2d}}(2^{\frac{n-1}{2}} - 1),\ (2^d - 1)^{\frac{n-1}{2d}}\right) & \text{if } d \text{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}} + 1)^{\frac{n-1}{d}}\right) & \text{if } d \text{ is even.} \end{cases}$$

In particular, when $n = 3$, $\#\ker(\star_+) = 1$ and $\#\ker(\star_-) = 3$.

6. Joint Spins

Fix a sign $\mu \in \{\pm\}$. Recall that S_μ is the set of rational primes $p \equiv \mu 1 \bmod 4$ that split completely in $K/\mathbb{Q}$, i.e., unramified and of residue degree 1 in $K/\mathbb{Q}$, and that F_μ is the set of $p \in S_\mu$ of residue degree 1 in $K(p)/\mathbb{Q}$. By Corollary 3.7, a prime $p \in S_\mu$ belongs to F_μ if and only if $\mathrm{spin}(\mathfrak{p}, \sigma) = 1$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and any prime ideal $\mathfrak{p}$ of K lying above p. Recall that R_μ is the set of primes $p \in S_\mu$ such that $\mathrm{spin}(\mathfrak{p}, \sigma)\,\mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = 1$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and all prime ideals $\mathfrak{p}$ of K lying above p, so that $F_\mu \subset R_\mu$. In this section, we will prove the following formula for the relative density of F_μ in R_μ, denoted by $d(F_\mu|R_\mu)$.

Theorem 6.1. *Assume Conjecture C_η for $\eta = \frac{2}{n(n-1)}$. Then*

$$d(F_\mu|R_\mu) = 2^{-\frac{n-1}{2}}.$$

Since each $p \in S_\mu$ splits into exactly the same number of prime ideals in $\mathcal{O}$, and since R_μ is a set of primes of positive natural density, it suffices to show that

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ lies over } p \in F_\mu}} 1 = 2^{-\frac{n-1}{2}} \sum_{\substack{\mathfrak{N}(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ lies over } p \in R_\mu}} 1 + o(X(\log X)^{-1}). \tag{13}$$

Let τ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, a cyclic group of order n. Then, by definition of the set R_μ, a prime $p \in R_\mu$ belongs to the set F_μ if and only if $\mathrm{spin}(\mathfrak{p}, \tau^k) = 1$ for all $k \in \{1, 2, \ldots, \frac{n-1}{2}\}$. The product

$$\prod_{k=1}^{\frac{n-1}{2}} \frac{1 + \mathrm{spin}(\mathfrak{p}, \tau^k)}{2}$$

is the indicator function of the property that $\mathrm{spin}(\mathfrak{p}, \tau^k) = 1$ for all $k \in \{1, 2, \ldots, \frac{n-1}{2}\}$. Expanding this product gives

$$2^{-\frac{n-1}{2}} \sum_{H \subset \{\tau, \ldots, \tau^{\frac{n-1}{2}}\}} \prod_{\sigma \in H} \mathrm{spin}(\mathfrak{p}, \sigma), \tag{14}$$

where the sum is over all subsets H of $\{\tau, \tau^2, \ldots, \tau^{\frac{n-1}{2}}\}$. When $H = \emptyset$, the product is 1 by convention.

Let L/K be an abelian extension with Galois group isomorphic to $\mathbf{M}_4^\mu$, and let $\mathcal{A}$ denote the set of disjoint G-orbits of elements of $\mathbf{M}_4^\mu$, so that we can write

$$\mathbf{M}_4^\mu = \bigsqcup_{A \in \mathcal{A}} A.$$

Each G-orbit A is then a collection of invertible congruence classes modulo $4\mathcal{O}$ that are distinct modulo squares. Let $\mathcal{A}_0 \subset \mathcal{A}$ be the set of G-orbits A such that $\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1})$ for all non-trivial $\sigma \in G$ and for all prime ideals $\mathfrak{p}$ such that $\mathbf{r}_4(\mathfrak{p}) \in A$. Note that a prime ideal $\mathfrak{p}$ in $\mathcal{O}$ lies over a prime $p \in R_\mu$ if and only if $\mathbf{r}_4(\mathfrak{p}) \in A$ for some $A \in \mathcal{A}_0$.

Summing (14) over all prime ideals $\mathfrak{p}$ of norm $\mathfrak{N}(\mathfrak{p}) \leq X$, we get that

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p})\leq X\\ p\in F_\mu}} 1 = 2^{-\frac{n-1}{2}} \sum_{\substack{H\subset\{\tau,\dots,\tau^{\frac{n-1}{2}}\}\\ A\in\mathcal{A}_0}} \Sigma(X;H,A),$$

where

$$\Sigma(X;H,A) = \sum_{\substack{\mathfrak{N}(\mathfrak{p})\leq X\\ \mathbf{r}_4(\mathfrak{p})\in A}} \prod_{\sigma\in H} \mathrm{spin}(\mathfrak{p},\sigma).$$

The sums $\Sigma(X;\emptyset,A)$ feature no cancellation and provide the main term in (13). It then remains to show that

$$\Sigma(X;H,A) = o(X/\log X) \tag{15}$$

for each non-empty subset H of $\{\tau,\dots,\tau^{\frac{n-1}{2}}\}$ and each $A\in\mathcal{A}_0$. To this end, we will use a slight generalization of Theorem 1 of [KM].

We cannot apply the results of [KM] directly for two reasons. First, the class number h of K need not be 1 – this forces us to relate $\mathrm{spin}(\mathfrak{a},\sigma)$ to quadratic residue symbols involving elements "smaller" than the totally positive generators of $\mathfrak{a}^h$. Second, the sums $\Sigma(X;H,A)$ feature the additional restriction that $\mathbf{r}_4(\mathfrak{p})\in A$. Since A is a collection of congruence classes modulo $4\mathcal{O}$, the restriction that $\mathbf{r}_4(\mathfrak{p})\in A$ is reminiscent of the restriction to a congruence class as in [FIMR13, Theorem 1.2, p. 699]. Despite the similarity, there is a technical difference that we will explain.

Fix once and for all a set $\mathcal{C}$ consisting of h unramified degree-one prime ideals in $\mathcal{O}$ that is a complete set of representatives of ideal classes in the class group of K; its existence is guaranteed by an application of the Chebotarev Density Theorem to the Hilbert class field of K.

Now suppose that $\mathfrak{a}$ is a non-zero ideal in $\mathcal{O}$ coprime to $\prod_{\mathfrak{p}\in\mathcal{C}}\mathfrak{N}(\mathfrak{p})$, and let α denote a totally positive generator of $\mathfrak{a}^h$. As h is odd, the set $\{\mathfrak{p}^2 : \mathfrak{p}\in\mathcal{C}\}$ is also a complete set of representatives. Hence there exists $\mathfrak{p}\in\mathcal{C}$ such that $\mathfrak{a}\mathfrak{p}^2$ is a principal ideal. Let π denote a totally positive generator of the ideal $\mathfrak{p}^h$. Let α_0 denote a totally positive generator of $\mathfrak{a}\mathfrak{p}^2$. Then α_0^h and $\alpha\pi^2$ are both totally positive generators of the ideal $(\mathfrak{a}\mathfrak{p}^2)^h$, so we have

$$\mathrm{spin}(\mathfrak{a},\sigma) = \left(\frac{\alpha}{\sigma(\mathfrak{a})}\right) = \left(\frac{\alpha\pi^2}{\sigma(\mathfrak{a}\mathfrak{p}^2)}\right) = \mathrm{spin}(\mathfrak{a}\mathfrak{p}^2,\sigma) = \left(\frac{\alpha_0^h}{\sigma(\mathfrak{a}\mathfrak{p}^2)}\right) = \left(\frac{\alpha_0}{\sigma(\alpha_0)}\right), \tag{16}$$

since h is odd. Note that for each $\mathfrak{p}\in\mathcal{C}$ there is a bijection

$$\begin{aligned}\{\mathfrak{a}\subset\mathcal{O} : \mathfrak{N}(\mathfrak{a})\leq x, \mathfrak{a}\mathfrak{p}^2 \text{ is principal}\}&\\ \simeq \{\alpha_0\in\mathcal{D} : \mathfrak{N}(\alpha_0)\leq x\mathfrak{N}(\mathfrak{p})^2, \alpha_0\equiv 0 \bmod \mathfrak{p}^2\}&\end{aligned} \tag{17}$$

given by $\mathfrak{a}\mapsto\alpha_0$ as above. Moreover, $\mathbf{r}_4(\mathfrak{a})$ is the class in $\mathbf{M}_4$ of a totally positive generator of $\mathfrak{a}^h$, i.e., the class of α in $\mathbf{M}_4$. Since squares vanish in $\mathbf{M}_4$, the classes of α and $\alpha\pi^2$, and so also of α_0^h, coincide in $\mathbf{M}_4$. Hence, if A is a G-orbit, then

$$\mathbf{r}_4(\mathfrak{a})\in A \quad \text{if and only if} \quad \alpha_0^h\in A. \tag{18}$$

We will now prove the following adaptation of [KM, Theorem 1, p. 2].

Theorem 6.2. *With notation as above, let H be a non-empty subset of $\{\tau, \dots, \tau^{\frac{n-1}{2}}\}$. Assume Conjecture C_η holds true for $\eta = 1/(|H|n)$ with $\delta = \delta(\eta) > 0$ (see [KM, p. 7]). Let $\epsilon > 0$ be a real number. Then for all $X \geq 2$, we have*

$$\Sigma(X; H, A) \ll X^{1-\frac{\delta}{54|H|^2 n(12n+1)}+\epsilon},$$

where the implied constant depends only on ϵ and K.

Note that the set H above is of size at most $\frac{n-1}{2}$. Since Conjecture C_{η_1} implies Conjecture C_{η_2} whenever $\eta_1 \leq \eta_2$, we see that, conditional on Conjecture C_η for $\eta = \frac{2}{n(n-1)}$, Theorem 6.2 implies (15) for each G-orbit $A \in \mathcal{A}_0$ and each non-empty subset $H \subset \{\tau, \dots, \tau^{\frac{n-1}{2}}\}$, and hence also Theorem 6.1. It thus remains to prove Theorem 6.2.

For a non-zero ideal $\mathfrak{a} \subset \mathcal{O}$ and a G-orbit A, let

$$r(\mathfrak{a}; A) = \begin{cases} 1 & \text{if } \mathbf{r}_4(\mathfrak{a}) \in A \\ 0 & \text{otherwise,} \end{cases}$$

and let

$$s_{\mathfrak{a}} = r(\mathfrak{a}; A) \prod_{\sigma \in H} \operatorname{spin}(\mathfrak{a}, \sigma).$$

Then we have

$$\Sigma(X; H, A) = \sum_{\mathfrak{N}(\mathfrak{p}) \leq X} s_{\mathfrak{p}},$$

where the summation is over prime ideals $\mathfrak{p} \subset \mathcal{O}$ of norm at most X.

Let F be the integer defined in [KM, (2.2), p. 5]; it depends only on K. Moreover, we can choose the sets $\mathcal{C}\ell_a$ and $\mathcal{C}\ell_b$ in [KM, p. 5] so that their elements are coprime to $\prod_{\mathfrak{p} \in \mathcal{C}} \mathfrak{N}(\mathfrak{p})$. Note that F is divisible by 32.

To deduce Theorem 6.2, it suffices to prove that

$$\sum_{\substack{\mathfrak{N}(\mathfrak{p}) \leq X \\ \mathfrak{p} \nmid F}} s_{\mathfrak{p}} \ll_{\epsilon, K} X^{1-\frac{\delta}{54|H|^2 n(12n+1)}+\epsilon}$$

because F has only finitely many prime ideal divisors.

The proof of Theorem 6.2 proceeds via Vinogradov's method, with suitable estimates necessary for the sums of type I

$$A_{\mathfrak{m}}(x) = \sum_{\substack{\mathfrak{N}\mathfrak{a} \leq x \\ (\mathfrak{a}, F)=1, \ \mathfrak{m} | \mathfrak{a}}} s_{\mathfrak{a}},$$

where $\mathfrak{m}$ is any non-zero ideal coprime to $\tau(\mathfrak{m})$, and sums of type II

$$B(x, y; v, w) = \sum_{\substack{\mathfrak{N}(\mathfrak{a}) \leq x \\ (\mathfrak{a}, F)=1}} \sum_{\substack{\mathfrak{N}(\mathfrak{b}) \leq y \\ (\mathfrak{b}, F)=1}} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}},$$

where $v = \{v_{\mathfrak{a}}\}_{\mathfrak{a}}$ and $w = \{w_{\mathfrak{b}}\}_{\mathfrak{b}}$ are arbitrary sequences of complex numbers of modulus bounded by 1. By [FIMR13, Proposition 5.2, p. 722] applied with $\vartheta = \frac{\delta}{54n|H|^2}$ and $\theta = \frac{1}{6n}$, the following two propositions imply Theorem 6.2.

Proposition 6.3. *Let $\delta = \delta(|H|n) > 0$ be as in Conjecture $C_{|H|n}$. Let $\epsilon > 0$. For any non-zero ideal $\mathfrak{m} \subset \mathcal{O}$, we have*

$$\sum_{\substack{\mathfrak{N}(\mathfrak{a}) \leq x \\ (\mathfrak{a}, F)=1, \mathfrak{m}|\mathfrak{a}}} s_{\mathfrak{a}} \ll x^{1-\frac{\delta}{54n|H|^2}+\epsilon}, \tag{19}$$

where the implied constant depends only on K and ϵ.

Proposition 6.4. *Let $\epsilon > 0$. For any pair of sequences of complex numbers $\{v_{\mathfrak{a}}\}$ and $\{w_{\mathfrak{b}}\}$ indexed by non-zero ideals in $\mathcal{O}$ and satisfying $|v_{\mathfrak{a}}|, |v_{\mathfrak{b}}| \leq 1$, we have*

$$\sum_{\substack{\mathfrak{N}(\mathfrak{a}) \leq x \\ (\mathfrak{a}, F)=1}} \sum_{\substack{\mathfrak{N}(\mathfrak{b}) \leq y \\ (\mathfrak{b}, F)=1}} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}} \ll \left(x^{-\frac{1}{6n}} + y^{-\frac{1}{6n}}\right)(xy)^{1+\epsilon}, \tag{20}$$

where the implied constant depends only on K and ϵ.

6.1. **Proof of Proposition 6.3.** The proof is very similar to the proof of [KM, (2.5), p. 7], so we will outline the additional arguments necessary to prove Proposition 6.3. For each non-zero ideal $\mathfrak{a}$, there exists a prime ideal $\mathfrak{p} \in \mathcal{C}$ such that $\mathfrak{a}\mathfrak{p}^2$ is principal. We can thus write

$$A_{\mathfrak{m}}(x) = \sum_{\mathfrak{p} \in \mathcal{C}} A_{\mathfrak{m}}(x; \mathfrak{p}),$$

where

$$A_{\mathfrak{m}}(x; \mathfrak{p}) = \sum_{\substack{\mathfrak{N}(\mathfrak{a}) \leq x \\ (\mathfrak{a}, F)=1, \ \mathfrak{m}|\mathfrak{a} \\ \mathfrak{a}\mathfrak{p}^2 \text{ is principal}}} s_{\mathfrak{a}}.$$

Since $\mathcal{C}$ depends only on K, it now suffices to prove that

$$A_{\mathfrak{m}}(x; \mathfrak{p}) = \sum_{\substack{\mathfrak{N}(\mathfrak{a}) \leq x \\ (\mathfrak{a}, F)=1, \ \mathfrak{m}|\mathfrak{a} \\ \mathfrak{a}\mathfrak{p}^2 \text{ is principal}}} s_{\mathfrak{a}} \ll x^{1-\frac{\delta}{54n|H|^2}+\epsilon}$$

for each $\mathfrak{p} \in \mathcal{C}$, where the implied constant depends only on K and ϵ. We now use the bijection (17), the formula (16), and the equivalence (18) to write

$$A_{\mathfrak{m}}(x; \mathfrak{p}) = \sum_{\substack{\alpha_0 \in \mathcal{D}, \ \mathfrak{N}(\alpha_0) \leq x\mathfrak{N}(\mathfrak{p})^2 \\ (\alpha_0, F)=1, \ \alpha_0 \equiv 0 \bmod [\mathfrak{m}, \mathfrak{p}^2] \\ \alpha_0^h \in A}} \prod_{\sigma \in H} \left(\frac{\alpha_0}{\sigma(\alpha_0)}\right),$$

where $[\mathfrak{m}, \mathfrak{p}^2]$ denotes the least common multiple of $\mathfrak{m}$ and $\mathfrak{p}^2$. Again, since $\mathcal{C}$ and so also the norms $\{\mathfrak{N}(\mathfrak{p})\}_{\mathfrak{p} \in \mathcal{C}}$ depend only on K, it suffices to prove that

$$A'_{\mathfrak{m}}(x) = \sum_{\substack{\alpha \in \mathcal{D}, \ \mathfrak{N}(\alpha) \leq x \\ (\alpha, F)=1, \ \alpha \equiv 0 \bmod \mathfrak{m} \\ \alpha^h \in A}} \prod_{\sigma \in H} \left(\frac{\alpha}{\sigma(\alpha)}\right) \ll_{K,\epsilon} x^{1-\frac{\delta}{54n|H|^2}+\epsilon} \tag{21}$$

uniformly for all non-zero ideals $\mathfrak{m}$. We have thus removed the issue of summing terms involving $\mathrm{spin}(\mathfrak{a}, \sigma)$ for non-principal ideals $\mathfrak{a}$. It remains to handle the condition $\alpha^h \in A$. To this end, we split the sum into congruence classes modulo F, and we emphasize that F is a multiple of 4. We get

$$A'_{\mathfrak{m}}(x) = \sum_{\substack{\rho \bmod F \\ \rho \in \Omega_I(A)}} A'_{\mathfrak{m}}(x; \rho),$$

where

$$A'_{\mathfrak{m}}(x;\rho) = \sum_{\substack{\alpha \in \mathcal{D},\ \mathfrak{N}(\alpha) \le x \\ \alpha \equiv \rho \bmod F \\ \alpha \equiv 0 \bmod \mathfrak{m}}} \prod_{\sigma \in H} \left(\frac{\alpha}{\sigma(\alpha)} \right) \tag{22}$$

and where $\Omega_I(A)$ is the set of congruence classes ρ modulo F such that $(\rho, F) = 1$ and such that

$$\alpha \equiv \rho \bmod F \Longrightarrow \alpha^h \in A.$$

Note that $|\Omega_I(A)| \le F$.

The sum $A'_{\mathfrak{m}}(x;\rho)$ in (22) is identical to the sum $A(x,\rho)$ in [KM, (3.2), p. 9]. Hence, the bound for $A(x,\rho)$ proved in [KM, Section 3] carries over to $A'_{\mathfrak{m}}(x;\rho)$, which, in conjunction with the fact that F depends only on K, implies the bound (21) and hence also Proposition 6.3.

6.2. **Proof of Proposition 6.4.** The proof is very similar to the proof of [KM, (2.6), p. 7], so we will outline the additional arguments necessary to prove Proposition 6.4. Given $x, y > 0$ and two sequences $v = \{v_{\mathfrak{a}}\}_{\mathfrak{a}}$ and $w = \{w_{\mathfrak{b}}\}_{\mathfrak{b}}$ of complex numbers bounded in modulus by 1, recall that we defined

$$B(x,y;v,w) = \sum_{\substack{\mathfrak{N}(\mathfrak{a}) \le x \\ (\mathfrak{a},F)=1}} \sum_{\substack{\mathfrak{N}(\mathfrak{b}) \le y \\ (\mathfrak{b},F)=1}} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}}, \tag{23}$$

and that our goal is to prove that

$$B(x,y;v,w) \ll_{K,\epsilon} \left(x^{-\frac{1}{6n}} + y^{-\frac{1}{6n}} \right) (xy)^{1+\epsilon} \tag{24}$$

for all $\epsilon > 0$, uniformly in v and w. We can write

$$B(x,y;v,w) = \sum_{\mathfrak{p}_1 \in \mathcal{C}} \sum_{\mathfrak{p}_2 \in \mathcal{C}} B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2),$$

where, for $(\mathfrak{p}_1, \mathfrak{p}_2) \in \mathcal{C} \times \mathcal{C}$, we set

$$B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2) = \sum_{\substack{\mathfrak{N}(\mathfrak{a}) \le x \\ (\mathfrak{a},F)=1 \\ \mathfrak{a}\mathfrak{p}_1^2 \text{ is principal}}} \sum_{\substack{\mathfrak{N}(\mathfrak{b}) \le y \\ (\mathfrak{b},F)=1 \\ \mathfrak{b}\mathfrak{p}_2^2 \text{ is principal}}} v_{\mathfrak{a}} w_{\mathfrak{b}} s_{\mathfrak{a}\mathfrak{b}}.$$

It suffices to prove the desired estimate for each of the h^2 sums $B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2)$. So fix $(\mathfrak{p}_1, \mathfrak{p}_2) \in \mathcal{C} \times \mathcal{C}$. Writing π_1, π_2, α_0, and β_0 for the totally positive generators of the principal ideals $\mathfrak{p}_1^h$, $\mathfrak{p}_2^h$, $\mathfrak{a}\mathfrak{p}_1^2$, and $\mathfrak{b}\mathfrak{p}_2^2$, respectively, we obtain in a similar way to (16) the formula

$$\operatorname{spin}(\mathfrak{a}\mathfrak{b}, \sigma) = \left(\frac{\alpha_0 \beta_0}{\sigma(\alpha_0 \beta_0)} \right) = \left(\frac{\alpha_0}{\sigma(\alpha_0)} \right) \left(\frac{\beta_0}{\sigma(\beta_0)} \right) \left(\frac{\alpha_0}{\sigma(\beta_0)\sigma^{-1}(\beta_0)} \right). \tag{25}$$

Using the bijection (17), the formula (25), and the equivalence (18), we deduce that

$$B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2)=\sum_{\substack{\alpha_0\in\mathcal{D}\\ \mathfrak{N}(\alpha_0)\leq x\mathfrak{N}(\mathfrak{p}_1)^2\\ (\alpha_0,F)=1\\ \alpha_0\equiv 0\text{ mod }\mathfrak{p}_1^2}}\ \sum_{\substack{\beta_0\in\mathcal{D}\\ \mathfrak{N}(\beta_0)\leq y\mathfrak{N}(\mathfrak{p}_2)^2\\ (\beta_0,F)=1\\ \beta_0\equiv 0\text{ mod }\mathfrak{p}_2^2\\ (\alpha_0\beta_0)^h\in A}} v'_{\alpha_0}w'_{\beta_0}\phi(\alpha_0,\beta_0), \tag{26}$$

where

$$v'_{\alpha_0}=v_{(\alpha_0)/\mathfrak{p}_1^2}\prod_{\sigma\in H}\left(\frac{\alpha_0}{\sigma(\alpha_0)}\right)\quad\text{and}\quad w'_{\beta_0}=w_{(\beta_0)/\mathfrak{p}_2^2}\prod_{\sigma\in H}\left(\frac{\beta_0}{\sigma(\beta_0)}\right)$$

and where $\phi(\cdot,\cdot)$ is the same function as the one defined in [KM, p. 19], i.e.,

$$\phi(\alpha_0,\beta_0)=\prod_{\sigma\in H}\left(\frac{\alpha_0}{\sigma(\beta_0)\sigma^{-1}(\beta_0)}\right).$$

We further split the sum $B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2)$ into congruence classes modulo F. As F is divisible by 4, this will have the effect of separating the variables α_0 and β_0 in the condition $(\alpha_0\beta_0)^h\in A$. We have

$$B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2)=\sum_{\rho_1\text{ mod }F}\ \sum_{\substack{\rho_2\text{ mod }F\\ (\rho_1,\rho_2)\in\Omega_{II}(A)}} B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2;\rho_1,\rho_2),$$

where

$$B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2;\rho_1,\rho_2)=\sum_{\substack{\alpha_0\in\mathcal{D}\\ \mathfrak{N}(\alpha_0)\leq x\mathfrak{N}(\mathfrak{p}_1)^2\\ \alpha_0\equiv\rho_1\text{ mod }F}}\ \sum_{\substack{\beta_0\in\mathcal{D}\\ \mathfrak{N}(\beta_0)\leq y\mathfrak{N}(\mathfrak{p}_2)^2\\ \beta_0\equiv\rho_2\text{ mod }F}} v''_{\alpha_0}w''_{\beta_0}\phi(\alpha_0,\beta_0).$$

Here

$$v''_{\alpha_0}=\mathbf{1}(\alpha_0\equiv 0\text{ mod }\mathfrak{p}_1^2)\cdot v'_{\alpha_0}$$

and

$$w''_{\beta}=\mathbf{1}(\beta_0\equiv 0\text{ mod }\mathfrak{p}_2^2)\cdot w'_{\beta_0},$$

where $\mathbf{1}(P)$ is the indicator function of a property P, and $\Omega_{II}(A)$ is the set of $(\rho_1,\rho_2)\in(\mathcal{O}/(F))^\times\times(\mathcal{O}/(F))^\times$ such that

$$\alpha_0\equiv\rho_1\text{ mod }F\text{ and }\beta_0\equiv\rho_2\text{ mod }F\Longrightarrow(\alpha_0\beta_0)^h\in A.$$

Note that $|\Omega_{II}(A)|\leq F^2$.

The sum $B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2;\rho_1,\rho_2)$ has the same shape as the sum $B_i(x,y;\alpha_0,\beta_0)$ in [KM, p. 19], and so the bound [KM, (4.5), p. 19] implies that

$$B(x,y;v,w;\mathfrak{p}_1,\mathfrak{p}_2;\rho_1,\rho_2)\ll_{K,\epsilon}\left(x^{-\frac{1}{6n}}+y^{-\frac{1}{6n}}\right)(xy)^{1+\epsilon}.$$

This finishes the proof of Proposition 6.4 and hence also of Theorem 6.2.

7. Proof of Main Results

Theorem 1.1. *Let K be a number field satisfying conditions $(P1)-(P5)$. Assume Conjecture C_η holds for $\eta = \frac{2}{n(n-1)}$. For $k \neq 1$ dividing n let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then for a fixed sign ±,*

$$d(F_\pm|S_\pm) = \frac{s_\pm}{2^{3(n-1)/2}}, \quad \textit{and} \quad d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}$$

where

$$s_+ = 1 + \prod_{\substack{k|n \\ d_k\, odd \\ k\neq 1}} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{\substack{k|n \\ d_k\, odd \\ k\neq 1}} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$s_- = \prod_{\substack{k|n \\ d_k\, even \\ k\neq 1}} (2^{d_k/2}+1)^{\frac{\phi(k)}{d_k}} \prod_{\substack{k|n \\ d_k\, odd \\ k\neq 1}} (2^{d_k}-1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function. In particular, when n is prime, writing $d = d_n$,

$$(s_+, s_-) = \begin{cases} \left(1 + 2^{\frac{n-1}{2d}}(2^{\frac{n-1}{2}}-1),\ (2^d-1)^{\frac{n-1}{2d}}\right) & \textit{if } d \textit{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}}+1)^{\frac{n-1}{d}}\right) & \textit{if } d \textit{ is even.} \end{cases}$$

Proof. By Theorem 4.11, $d(R_\pm|S_\pm) = \#\ker(\star_\pm)/2^{(n-1)}$. Then $d(R_\pm|S_\pm) = s_\pm/2^{(n-1)}$ by Proposition 5.3. By Theorem 6.1, $d(F_\pm|R_\pm) = 2^{-(n-1)/2}$. Therefore

$$d(F_\pm|S_\pm) = d(F_\pm|R_\pm)d(R_\pm|S_\pm) = \frac{s_\pm}{2^{3(n-1)/2}}.$$

Since $d(F|S) = d(F_+|S_+)d(S_+|S) + d(F_-|S_-)d(S_-|S)$, and $d(S_\pm|S) = 1/2$,

$$d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}.$$

□

Theorem 1.1 settles Conjecture 1.1 in [McM19]. This conjecture was originally stated for number fields K which in addition to satisfying properties $(P1)-(P5)$, were also assumed to have prime degree. While as originally stated, this assumption is necessary, it is artificial here. In [McM19], m_K is defined as the number of nontrivial $\mathrm{Gal}(K/\mathbb{Q})$-orbits of $\mathbf{M}_4$ with representative $\alpha \in \mathcal{O}$ such that $(\alpha, \alpha^\sigma)_2 = 1$. Let s denote the number of *elements* of $\mathbf{M}_4$ with representative $\alpha \in \mathcal{O}$ such that $(\alpha, \alpha^\sigma)_2 = 1$. When n is prime, $s = m_K n + 1$.

Let E denote the set of rational primes p such that for $\mathfrak{p}$ a prime of K above p, $\mathrm{spin}(\mathfrak{p}, \sigma) = 1$ for all nontrivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. For a fixed sign let $E_\pm$ denote the set of primes of E congruent to ±1 mod 4.

Conjecture 1.1 in [McM19] made two assertions, one regarding the density $d(E|S)$ of such primes restricted to those splitting completely in $K/\mathbb{Q}$ and one regarding the overall density $d(E)$ of such primes. The assertion regarding the restricted density is correct and the assertion regarding the overall density is slightly off due to a very simple oversight in the case in which p is not assumed to split completely in $K/\mathbb{Q}$.

Theorem 7.1. *[McM19, 1.1] Let K be a number field with prime degree satisfying properties $(P1)-(P5)$. Then*

$$d(E|S)=\frac{s}{2^{(3n-1)/2}},\quad d(E)=\frac{s}{n2^{(3n-1)/2}},$$

$$d(E_\pm|S_\pm)=\frac{s_\pm}{2^{3(n-1)/2}},\quad \text{and}\quad d(E_\pm)=\frac{s_\pm}{n2^{(3n-1)/2}}.$$

When n is prime, $s=m_Kn+1$.

Proof. If $\mathfrak{p}$ is a prime of K that does not split completely in $K/\mathbb{Q}$, then for some nontrivial $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, $\mathfrak{p}^\sigma=\mathfrak{p}$ so $\mathrm{spin}(\mathfrak{p},\sigma)=0$. Therefore $E\subseteq S$ so this E is exactly the F studied in Theorem 1.1 and $E_\pm=F_\pm$.

Where $s_\pm$ are as given in Theorem 1.1, $s=\#\ker(\star)=s_++s_-$ by Proposition 5.3. That $d(E|S)=s/2^{(3n-1)/2}$ and $d(E_\pm|S_\pm)=s_\pm/2^{3(n-1)/2}$ then follows from Theorem 1.1.

By Chebotarev's theorem, $d(S)=1/n$ and $d(S_\pm)=1/(2n)$ so breaking up the overall density as $d(E)=d(E\cap I|I)d(I)+d(E\cap S|S)d(S)$, we see that $d(E)=s/n2^{(3n-1)/2}$. Similarly, $d(E_\pm)=s_\pm/n2^{(3n-1)/2}$.

When n is prime, each nontrivial $\mathrm{Gal}(K/\mathbb{Q})$-orbit of $\mathbf{M}_4$ has n elements. As for the trivial orbits, as in [McM19, 5.2], $\star(1)=1$ and $\star(-1)=-1$. Therefore when n is prime, $s=\#\ker(\star)=m_Kn+1$. □

Theorem 1.2. *Let $K/\mathbb{Q}$ be a cubic cyclic number field and odd class number in which 2 is inert. Then*

$$d(F|S)=\frac{1}{4},$$

$$d(F_+|S_+)=\frac{1}{8},\quad \text{and}\quad d(F_-|S_-)=\frac{3}{8}.$$

Proof. For K a cyclic cubic number field with odd class number, by Theorem V in [AF67], all signatures are represented by units so by Lemma 2.1, $\mathrm{Cl}^+=\mathrm{Cl}$. It is a consequence of the classical Burgess's inequality [Bur63] that Conjecture is true for $m=3$, as is shown in Section 9 of [FIMR13]. Therefore the result follows from Theorem 1.1. □

Acknowledgements

This research was funded by the Max Planck Institute for Mathematics, Cornell University, and ERC grant agreement No. 670239. The authors would also like to thank Andrew Granville, Brian Hwang, Christian Maire, Pieter Moree, and Ravi Ramakrishna.

References

[AF67] J. V. Armitage and A. Fröhlich. Classnumbers and unit signatures. *Mathematika*, 14:94–98, 1967.

[Bur63] D. A. Burgess. On character sums and L-series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.

[FIMR13] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. The spin of prime ideals. *Invent. Math.*, 193(3):697–749, 2013.

[FvzGS99] Sandra Feisel, Joachim von zur Gathen, and M. Amin Shokrollahi. Normal bases via general Gauss periods. *Math. Comp.*, 68(225):271–290, 1999.

[KM] Peter Koymans and Djordjo Milovic. Joint distribution of spins. arXiv:1809.09597.

[Koc00] Helmut Koch. *Number theory*, volume 24 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2000. Algebraic numbers and functions, Translated from the 1997 German original by David Kramer.

[Leh88] Emma Lehmer. Connection between Gaussian periods and cyclic units. *Math. Comp.*, 50(182):535–541, 1988.

[McM18] Christine McMeekin. *A Density of Ramified Primes*. PhD thesis, Cornell University, ProQuest LLC, Ann Arbor, MI, 2018.

[McM19] Christine McMeekin. On the asymptotics of a prime spin relation. *Journal of Number Theory*, 200:407 – 426, 2019.

[Mil08] James S. Milne. Algebraic number theory (v3.01), 2008. Available at www.jmilne.org/math/.

[Mil13] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[Nar04] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Sha74] Daniel Shanks. The simplest cubic fields. *Math. Comp.*, 28:1137–1152, 1974.

(Stephanie Chan) Department of Mathematics, University College London
E-mail address: stephanie.chan.16@ucl.ac.uk

(Christine McMeekin) Department of Mathematics, University of Connecticut
E-mail address: christine.mcmeekin@gmail.com

(Djordjo Milovic) Department of Mathematics, University College London
E-mail address: dzm656@gmail.com