



S. Ali Altuğ · Arul Shankar · Ila Varma · Kevin H. Wilson

The number of D_4 -fields ordered by conductor

Received July 30, 2018

Abstract. We consider families of quartic number fields whose normal closures over \mathbb{Q} have Galois group isomorphic to D_4 , the symmetries of a square. To any such field L , one can associate the Artin conductor of the corresponding 2-dimensional irreducible Galois representation with image D_4 . We determine the asymptotic number of such D_4 -quartic fields ordered by conductor, and compute the leading term explicitly as a mass formula, verifying heuristics of Kedlaya and Wood. Additionally, we are able to impose any local splitting conditions at any finite number of primes (sometimes, at an infinite number of primes), and as a consequence, we also compute the asymptotic number of order-4 elements in class groups and narrow class groups of quadratic fields ordered by discriminant.

Traditionally, there have been two approaches to counting quartic fields, using arithmetic invariant theory in combination with geometry-of-number techniques, and applying Kummer theory together with L -function methods. Both of these strategies fail in the case of D_4 -quartic fields ordered by conductor since counting quartic fields containing a quadratic subfield with large discriminant is difficult. However, when ordering by conductor, we utilize additional algebraic structure arising from the outer automorphism of D_4 combined with both approaches mentioned above to obtain exact asymptotics.

Keywords. Arithmetic statistics, Malle’s conjecture, analytic number theory

1. Introduction

The main purpose of this article is to determine the asymptotic number of quartic dihedral fields with bounded conductor. If L denotes a quartic field whose normal closure M over \mathbb{Q} has Galois group $\text{Gal}(M/\mathbb{Q})$ isomorphic to the group of symmetries of a square, we refer to L as a D_4 -quartic field. Furthermore, there is a unique (up to conjugacy) irreducible 2-dimensional Galois representation

$$\rho_M : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{C})$$

S. A. Altuğ: Radix Trading, LLC,
100 Park Ave Suite 2205, New York, NY 10017, USA; e-mail: ali.altug@gmail.com

A. Shankar: Department of Mathematics, University of Toronto,
Room 6290, 40 St George Street, M5S 2E4, Toronto, Canada; e-mail: arul.shnkr@gmail.com

I. Varma: Department of Mathematics, University of Toronto,
Room 6290, 40 St George Street, M5S 2E4, Toronto, Canada; e-mail: ila@math.toronto.edu

K. H. Wilson: The Policy Lab, Brown University,
225 Dyer Street Floor 5, Providence, RI 02903, USA; e-mail: kevin.wilson@brown.edu

Mathematics Subject Classification (2020): 11H55, 11M06, 11R16, 11R29

that factors through $\text{Gal}(M/\mathbb{Q}) \cong D_4$. We define the *conductor* of L to be equal to the Artin conductor of ρ_M (see [7, pp. 158–159]).

Theorem 1. *Let $N_{D_4}^{(r_2)}(X)$ denote the number of isomorphism classes of D_4 -quartic fields with $4 - 2r_2$ real embeddings and conductor bounded by X . Then*

$$\begin{aligned}
 N_{D_4}^{(0)}(X) &= \frac{1}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot X \log X + O(X \log \log X), \\
 N_{D_4}^{(1)}(X) &= \frac{1}{4} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot X \log X + O(X \log \log X), \\
 N_{D_4}^{(2)}(X) &= \frac{3}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot X \log X + O(X \log \log X).
 \end{aligned}$$

Understanding the distribution of number fields with fixed signature and Galois group is a fundamental question in number theory with several significant applications. For example, the inverse Galois problem follows from understanding the main terms for the asymptotic number of field extensions of each fixed degree and Galois closure over a given base field. Furthermore, if the results are refined enough to determine the asymptotic number of field extensions satisfying certain local specifications, then another application of counting number fields is towards understanding the distribution of torsion in class groups of number fields of fixed degree, i.e., to proving cases of the Cohen–Lenstra heuristics [11] as well as the extensions given by Gerth [17], Cohen–Martinet [12], and Malle [24].

There are heuristics (see [8, Conjecture 1.2]) for the order of growth for the number of field extensions of each fixed degree and Galois closure over a given base field when the extensions are bounded by their (norms of the relative) discriminants, due to Linnik, Malle, and Türkelli. Linnik predicted that the number $N_{S_n}(X)$ of S_n -degree- n number fields with discriminant bounded by X satisfies $N_{S_n}(X) \sim c_n X$ for some constant c_n as $X \rightarrow \infty$. Additionally, the heuristics of Malle [23] imply that the proportion of degree- n fields with Galois closure S_n amongst all degree- n fields is expected to be 100% only when n is a prime. Cohen, Diaz y Diaz and Olivier [9] verified a case of the strong Malle conjecture in the quartic dihedral case by proving that the number of D_4 -quartic fields with discriminant bounded by X is asymptotically equal to cX , where $c \approx .052326$.

Cohen, Diaz y Diaz and Olivier [9] prove their result by determining the asymptotic number of quadratic extensions of quadratic fields ordered by discriminant, a 100% of which are D_4 -quartic fields. They show that the number of totally real D_4 -quartic fields with absolute discriminant bounded by X is asymptotically equal to cX , where

$$c = \frac{3}{\pi^2} \cdot \left(\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < \infty}} \frac{1}{\text{Disc}(K)^2} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \right). \tag{1}$$

Our results imply that the number of totally real D_4 -quartic fields with conductor bounded by X is asymptotically equal to a similar sum:

$$N_{D_4}^{(0)}(X) \sim \frac{3}{\pi^2} \cdot \left(\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) \leq X}} \frac{1}{\text{Disc}(K)} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \right) \cdot X. \tag{2}$$

However, the methods to prove (1) and (2) vastly differ. When ordering by discriminant, only the summation terms in (1) indexed by quadratic fields K of small discriminant contribute to the main term of the asymptotics. However, when ordering by conductor, quadratic fields K in every range of the discriminant contribute to the main term. In particular, we must evaluate the contribution coming from quadratic extensions L of quadratic fields K where $\text{Nm}_{L/K}(\text{Disc}(L/K))$ is small relative to the discriminant of K . As a consequence, the analytic methods used by [9] are insufficient in our case.

In addition to proving that (2) holds, we establish an explicit formula for the main term of the asymptotic:

Theorem 2. *We have the following:*

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) \leq X}} \frac{1}{\text{Disc}(K)} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \sim \frac{\zeta(2)}{2} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot \log X,$$

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ -X \leq \text{Disc}(K) < 0}} \frac{1}{|\text{Disc}(K)|} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \sim \frac{\zeta(2)}{2} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot \log X.$$

In conjunction with (2) (and the analogous statements for the non-totally-real splitting types), Theorem 2 implies Theorem 1. We are also able to determine refined asymptotics for families of D_4 -quartic fields with certain prescribed local specifications, but to describe these results, we must first introduce some notation.

We say that $\Sigma = (\Sigma_v)_v$ is a *collection of local specifications* if for each place v of \mathbb{Q} , Σ_v contains pairs (L_v, K_v) consisting of an étale algebra L_v of \mathbb{Q}_v of degree 4 along with a quadratic subalgebra K_v . We say that such a collection Σ is *acceptable* if for all but finitely many primes p , the set Σ_p contains all pairs (L_p, K_p) with conductor indivisible by p^2 . Here, the *conductor* C of such a pair is equal to

$$C(L_p, K_p) := \text{Disc}(L_p)/\text{Disc}(K_p),$$

and we also let C_p denote the p -part of C . Such a collection Σ is said to be *complete* if for each place v and each splitting type ς , the set Σ_v contains either all or none of the pairs (L_v, K_v) having splitting type ς . If $\mathcal{L}(\Sigma)$ denotes all D_4 -quartic fields L such that $L \otimes \mathbb{Q}_v \in \Sigma_v$ for all v , and $N_{D_4}(\Sigma, X)$ denotes the number of isomorphism classes of D_4 -quartic fields in $\mathcal{L}(\Sigma)$ whose conductor is bounded by X , we then have:

Theorem 3. *If $\Sigma = (\Sigma_v)_v$ is an acceptable and complete collection of local specifications such that Σ_2 contains every degree-4 étale algebra of \mathbb{Q}_2 containing a quadratic subalgebra, then*

$$N_{D_4}(\Sigma, X) \sim \frac{1}{2} \cdot \left(\sum_{(L, K) \in \Sigma_\infty} \frac{1}{\#\text{Aut}(L, K)} \right) \cdot \prod_p \left(\sum_{(L_p, K_p) \in \Sigma_p} \frac{1}{\#\text{Aut}(L_p, K_p)} \cdot \frac{1}{C_p(L_p, K_p)} \right) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X,$$

where for all v , $\text{Aut}(L_v, K_v)$ consists of the automorphisms of L_v which send K_v to itself.

In previous results of Gauss, Davenport–Heilbronn [14] and Bhargava [2, 4], the constant c_n of the main term of the asymptotic number of S_n -degree- n number fields (for $n \leq 5$) can also be explicitly given as a *mass formula*, i.e., the constants c_n take the form of an Euler product of local masses. In [3], Bhargava predicted the constants c_n for all n , explicitly describing them in terms of Euler products of local masses derived from the heuristic assumption that the completions of S_n -degree- n number fields at different places behave independently of one another. The constant determined in Theorem 3 is completely analogous to the constants $c_{n, \Sigma}$ predicted in [3, (4.2)]. However, the analogous product of local masses for D_4 -quartic fields ordered by discriminant is not equal to the constant c computed in [9]; in other words, the analogue of Theorem 3 when ordering by discriminant is false!

The existence of mass formulae when ordering by invariants other than the discriminant has been studied by Kedlaya [20], Wood [29], and Johnson [18], building on work of Mäki [22]. However, the question remains:

Question 4. *Let G denote a finite group, and let C be a virtual conductor¹ for G . A G -number field K is a normal field extension of \mathbb{Q} with Galois group $\text{Gal}(K/\mathbb{Q}) = G$. Does the product of local C -masses for the weighted number of G -étale algebras of \mathbb{Q}_p over all places p predict the asymptotic number of G -number fields ordered by C ?*

This question for abelian G has been studied extensively by Wood in [31], in which a sufficient condition for answering Question 4 in the affirmative is given for C . For non-abelian G , the only conductors C for which both the main term and the constant have been explicitly obtained correspond to discriminant functions (see [14, 2, 4, 6]). On the other hand, we show that the result of [9] in which D_4 -quartic fields are ordered by their discriminants gives a negative answer to Question 4 (see (11)); however, Theorem 3 gives an affirmative answer when ordering D_4 -fields by their (2-dimensional) conductors. Moreover, Theorem 3 is the first non-abelian case that answers Question 4 for a conductor C that does not arise as a discriminant function. Overall, the choice of invariant appears to be a subtle issue when determining asymptotics for families of G -number fields.

Theorem 3 allows us to compute the asymptotic number of order-4 elements in class groups and narrow class groups of quadratic fields ordered by discriminant. Such elements

¹ A *virtual conductor* for G is the Artin conductor for a virtual character of G .

in the class groups of a quadratic field K determine D_4 -quartic fields L whose normal closures over \mathbb{Q} contain K as the fixed field of C_4 . We obtain the following theorem by determining asymptotics for the acceptable collection of D_4 -quartic fields that arise in this manner, even when we restrict the set of quadratic fields by imposing local specifications at a finite set of primes. We remark that it is crucial for the result below that we order D_4 -quartic fields by conductor, and furthermore, that we can impose acceptable local specifications at infinitely many primes.

Theorem 5. *For a quadratic field K , let $\text{Cl}_{2^k}(K)$ (resp. $\text{Cl}_{2^k}^+(K)$) denote the 2^k -torsion subgroup in its ideal class group $\text{Cl}(K)$ (resp. narrow class group $\text{Cl}^+(K)$). Let \mathcal{K} denote a family of quadratic fields with prescribed splitting types at a finite set S consisting of odd primes. Then*

$$\begin{aligned}
 \text{(a)} \quad & \sum_{\substack{K \in \mathcal{K} \\ 0 < \text{Disc}(K) \leq X}} (\#\text{Cl}_4(K) - \#\text{Cl}_2(K)) \sim \frac{1}{16} \cdot \prod_{p \in S} m_{\text{Cl}}(p) \cdot \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \\
 & \quad \cdot X \log X, \\
 \text{(b)} \quad & \sum_{\substack{K \in \mathcal{K} \\ -X \leq \text{Disc}(K) < 0}} (\#\text{Cl}_4(K) - \#\text{Cl}_2(K)) \sim \frac{1}{4} \cdot \prod_{p \in S} m_{\text{Cl}}(p) \cdot \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \\
 & \quad \cdot X \log X, \\
 \text{(c)} \quad & \sum_{\substack{K \in \mathcal{K} \\ 0 < \text{Disc}(K) \leq X}} (\#\text{Cl}_4^+(K) - \#\text{Cl}_2^+(K)) \sim \frac{1}{8} \cdot \prod_{p \in S} m_{\text{Cl}}(p) \cdot \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \\
 & \quad \cdot X \log X.
 \end{aligned}$$

Here, $m_{\text{Cl}}(p)$ is determined in terms of the prescribed splitting type for $p \in S$:

$$m_{\text{Cl}}(p) := \frac{2}{p+2} \quad \text{if } p \text{ ramifies,} \quad m_{\text{Cl}}(p) := \frac{p}{2p+2} \quad \text{otherwise.}$$

The above result is a generalization of work of Fouvry–Klüners [16] that is derived from their own previous results [15] completely verifying Gerth’s extension [17] of the Cohen–Lenstra heuristics to the 4-rank of the narrow class group of quadratic fields. In [15], Fouvry–Klüners compute all moments for the 4-ranks of narrow class groups of quadratic fields ordered by discriminant. In conjunction with those results, Theorem 5 gives evidence towards the belief that the 4-ranks and the sizes of 2-torsion subgroups in class groups and narrow class groups of quadratic fields behave independently (see Remark 9.6).

As a byproduct of the methods used to obtain (2), we also prove a refinement of Theorem 2 that allows for imposing local specifications at a finite number of primes.

Theorem 6. *Let \mathcal{K} denote a set of quadratic fields with prescribed splitting types at a finite set S of odd primes. Then*

$$\begin{aligned}
 \text{(a)} \quad & \sum_{\substack{K \in \mathcal{K} \\ 0 < \text{Disc}(K) \leq X}} \frac{1}{\text{Disc}(K)} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \\
 & \sim \frac{\zeta(2)}{2} \cdot \prod_{p \in S} \frac{m(p)}{2p^2 + 4p + 4} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) \cdot \log X,
 \end{aligned}$$

$$\begin{aligned}
 \text{(b)} \quad & \sum_{\substack{K \in \mathcal{K} \\ -X < \text{Disc}(K) \leq 0}} \frac{1}{|\text{Disc}(K)|} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \\
 & \sim \frac{\zeta(2)}{2} \cdot \prod_{p \in S} \frac{m(p)}{2p^2 + 4p + 4} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot \log X,
 \end{aligned}$$

where $m(p)$ is determined in terms of the prescribed splitting type for $p \in S$:

$$m(p) := \begin{cases} p^2 + 2p + 1 & \text{if } p \text{ splits,} \\ p^2 + 1 & \text{if } p \text{ is inert,} \\ 2(p + 1) & \text{if } p \text{ is ramified.} \end{cases}$$

We next summarize the arguments for proving the main results. First, to establish Theorem 2, we use the fact that for a quadratic field K , $\frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})}$ can be written as a product of infinite sums simply using Möbius inversion:

$$\frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} = \left(\sum_{n=1}^{\infty} \frac{\chi_K(n)}{n} \right) \cdot \left(\sum_{m=1}^{\infty} \mu(m) \cdot \frac{\chi_K(m)}{m^2} \right), \tag{3}$$

where χ_K is the quadratic character associated to K . The proof then relies on the following observation: weighting this product by $\text{Disc}(K)^{-1}$, the main contribution when summing over quadratic fields K with bounded discriminant as in (2) comes from certain diagonal terms of the right hand side of (3), i.e., terms where mn is a square. For each K , the sum of these diagonal terms is expressible as an Euler product (see (21)), which then yields Theorem 2.

If we were to instead weight the product in (3) by $\text{Disc}(K)^{-2}$ when summing over all quadratic fields K as in (1), then the non-diagonal terms are no longer negligible. It is these terms that cause the constant c to fail Question 4; in fact, we show that the sum over quadratic fields with discriminant bounded by X of the *diagonal terms* in the right hand side of (3) weighted by $\text{Disc}(K)^{-2}$ is asymptotically equal to

$$\frac{3 \cdot 11^2}{2^6 \cdot 17} \cdot \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4} \right) \cdot X,$$

which is equal to the mass formula predicted for the number of D_4 -quartic fields of bounded discriminant (see Theorem 5.4).

Before discussing the proof of Theorem 1, we describe the differences in obtaining (2) and (1) as in [9, Corollary 1.2]. Because of the convergence of $\sum_K \text{Disc}(K)^{-2}$ when K runs over all quadratic fields, the main contribution to the sum in (1) comes from the terms indexed by K with $\text{Disc}(K) < X^{1/2}$, i.e., quadratic fields with small discriminant relative to X . However, this is not the case for the sum in (2); furthermore, the combination of Kummer theory and L -function methods utilized in [9] to prove (1) can only be used to determine the asymptotic number of D_4 -quartic fields with conductor bounded by X whose quadratic subfield has small discriminant relative to X (see Theorem 4.3). Additionally, adapting the geometry-of-numbers techniques of [2] in combination with

Wood's parametrization of quartic rings with a quadratic subring [30] is also limited to counting D_4 -quartic fields whose quadratic subfields have small discriminant.

Nevertheless, we obtain Theorem 1 and subsequently (2) by employing algebraic properties of the conductor $C(L)$ of a D_4 -quartic field L , namely that it is invariant under the outer automorphism ϕ of D_4 . More precisely, ϕ acts on the Galois group of the normal closure M over \mathbb{Q} of L , and the fixed field of $\phi(\text{Gal}(M/L))$ is another D_4 -quartic field $\phi(L)$ in M which is not isomorphic to L . The conductors of L and $\phi(L)$ coincide (even though their discriminants do not). Moreover, we relate the discriminants of K and $\phi(K)$ using the central inertia of L (see Definition 2.3). We prove (see Proposition 2.6)

$$|\text{Disc}(K)| > C(L)^{1/2} \implies |\text{Disc}(\phi(K))| < C(\phi(L))^{1/2},$$

and we use this phenomenon to obtain $N_{D_4}^{(r_2)}(X)$ from the asymptotic number of D_4 -quartic fields ordered by conductor whose quadratic subfield has small discriminant by employing a simple sieve.

The proof of Theorem 1 does ultimately rely on both the analytic techniques of [9] used to count D_4 -quartic fields by discriminant as well as the geometry-of-numbers methods used to count S_4 -fields as in [2]. Either can be used to obtain asymptotics for D_4 -quartic fields of bounded conductor whose quadratic subfield has small discriminant, but the sieve used to determine the asymptotics of $N_{D_4}^{(r_2)}(X)$ from counting such D_4 -quartic fields requires two ingredients: first, uniform error estimates on the number of such D_4 -quartic fields having large central inertia, and second, asymptotics for the number of such D_4 -quartic fields with prescribed ramification conditions. We are able to obtain the former using analytic methods and the latter using geometry-of-numbers techniques. This method of proof allows us to count D_4 -quartic fields with prescribed splitting and ramification conditions yielding Theorems 3 and 5. Additionally, Theorem 3 in conjunction with Theorem 4.3 and p -adic density computations (see Proposition 6.7) implies Theorem 6.

The analytic methods used to prove (2) show up frequently when studying asymptotics for the number of extensions of a family of number fields of fixed degree, including when determining Malle's conjecture for D_4 -octic fields ordered by discriminant, computing the asymptotic number of S_3 -fields ordered by the radical of its discriminant, or calculating the asymptotic number of octic fields with Galois group equal to the quaternion group ordered by its (2-dimensional) Artin conductor. Additionally, in order to attack number field asymptotics for larger Galois groups as in the case of S_6 -sextic fields, utilizing algebraic inputs such as an outer automorphism in order to transfer problems of great analytic difficulty to ones that can be approached using standard methods will be crucial.

This paper is organized as follows. First, we summarize basic arithmetic properties of D_4 -quartic fields and their invariants in Section 2, including a table of the splitting behavior of primes in D_4 -quartic fields depending on their inertia and decomposition group. We explicitly relate the conductors and quadratic discriminants of D_4 -quartic fields L and $\phi(L)$. Next in Section 3, we further develop the method of [3, 20, 29] and simultaneously obtain heuristics for families of D_4 -quartic fields ordered in multiple different ways. We begin counting D_4 -quartic fields with bounded invariants in Section 4. Using the analytic methods of [9], we obtain asymptotics for the number of such fields with small

quadratic discriminant in terms of a sum of ratios of L -values. By isolating the diagonal terms, we prove Theorem 2 in Section 5. In Section 6, we recall Wood’s parametrization of quartic rings with a quadratic subrings and adapt it to obtain a modified parametrization of D_4 -quartic fields in terms of certain integral orbits of a coregular representation V for a non-reductive group G . We study the p -adic properties of this representation, including those arising from the outer automorphism ϕ . We then use geometry-of-numbers methods in Section 7 to count integral orbits of G on V having bounded invariants. Using the results and methods from Sections 4, 6, and 7, we obtain crucial uniformity estimates in Section 8 that will be necessary to carry out the various requisite sieves. Finally, in Section 9, we prove the main theorems by using the analytic results of Sections 4, 7, and 8, in conjunction with the algebraic properties of the outer automorphism ϕ proved in Sections 2 and 6.

2. General properties of D_4 -quartic fields

Recall that D_4 denotes the order-8 group of symmetries of a square, and a D_4 -quartic field is a degree-4 field extension of \mathbb{Q} whose normal closure has Galois group D_4 over \mathbb{Q} . We let σ denote a 90° -rotation of a square and τ denote a reflection of a square so that

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^3 \rangle.$$

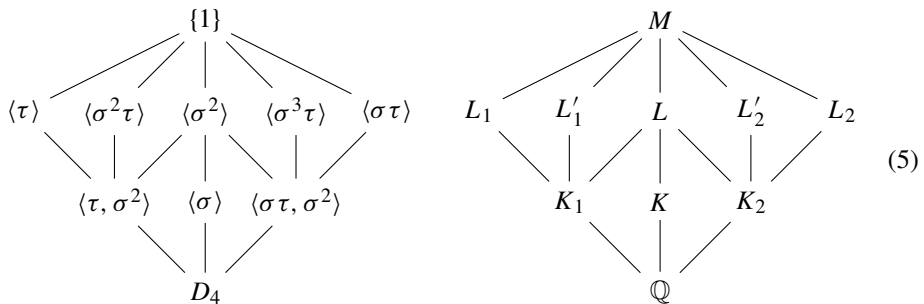
The group D_4 has non-trivial center $Z(D_4) = \{1, \sigma^2\}$.

2.1. Automorphisms of D_4 and the Galois theory of D_4 -quartics

We first describe important group-theoretic properties of D_4 as well as their applications to D_4 -quartics via Galois theory. Recall that the inner automorphism group $D_4/Z(D_4)$ is isomorphic to the Klein four group V_4 , but the full automorphism group is isomorphic to D_4 (see [27, pp. 83–85]). The non-trivial outer automorphism ϕ of D_4 has order 4 and can be described explicitly by

$$\phi(\sigma) = \sigma \quad \text{and} \quad \phi(\tau) = \sigma\tau. \tag{4}$$

Let L_1 be a D_4 -quartic, and denote its normal closure by M so that $\text{Gal}(M/\mathbb{Q}) = D_4$. Below, we describe a subfield diagram of M corresponding to the subgroup lattice of D_4 :



Here, a subgroup G of D_4 and a subfield F of M in the same position are related by $\text{Gal}(M/F) = G$. The fields L'_i are the (unique) Galois conjugates of L_i for $i = 1$ or 2 , and L is the unique quartic Galois subfield of M . While L_1 and L_2 are *not* conjugate, the outer automorphism ϕ maps $\text{Gal}(M/L_1) \rightarrow \text{Gal}(M/L_2)$ and $\text{Gal}(M/L'_1) \rightarrow \text{Gal}(M/L'_2)$. However, it sends $\text{Gal}(M/L_2) \rightarrow \text{Gal}(M/L'_1)$ and $\text{Gal}(M/L'_2) \rightarrow \text{Gal}(M/L_1)$. It also interchanges $\text{Gal}(M/K_1)$ and $\text{Gal}(M/K_2)$ while leaving $\text{Gal}(M/K)$ fixed.

Definition 2.1. If L_1 is a D_4 -quartic with Galois closure M over \mathbb{Q} , then we denote by $\phi(L_1)$ the quartic subfield of M fixed by $\phi(\text{Gal}(M/L_1))$. If K_1 denotes the quadratic subfield of L_1 , then we denote by $\phi(K_1)$ the quadratic subfield of M fixed by $\phi(\text{Gal}(M/K_1))$.

In the notation of (5), we have $\phi(L_1) = L_2$ and $\phi(K_1) = K_2$.

2.2. Arithmetic of D_4 -quartics

We now describe the splitting behavior of primes in D_4 -quartic fields M and their subfields.

Definition 2.2. If F is a number field, then the *splitting type* $\varsigma_p(F)$ at p of F satisfies

$$\varsigma_p(F) = (f_1^{e_1} f_2^{e_2} \dots) \iff \mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \dots$$

Similarly, if R is a ring, then the *splitting type* $\varsigma_p(R)$ at p is equal to $(f_1^{e_1} f_2^{e_2} \dots)$ if and only if

$$R/pR \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \dots$$

Let D_p denote the decomposition group of p in $\text{Gal}(M/\mathbb{Q})$, and let I_p denote the inertia subgroup of D_p . For an arbitrary prime p , we determine the splitting type of M and all of its subfields using the notation described in (5) depending on the choices for D_p and I_p in the table below.

We briefly recall how to compute the above table.² First, any subgroup can potentially be a decomposition group D_p . However, since all decomposition groups are only defined up to conjugacy, in Table 1 we only enumerate conjugacy classes of subgroups. On the other hand, the inertia group I_p must be a *normal* subgroup of D_p such that D_p/I_p is cyclic of order prime to p . Moreover, if $I'_p \trianglelefteq I_p$ is the second ramification group (which, by definition, is trivial if and only if the ramification is tame), then I_p/I'_p must be a product of cyclic groups of order p . When the Galois group is equal to D_4 , this allows us to fully enumerate the possibilities for pairs $I_p \trianglelefteq D_p$.

To compute the entries of Table 1, let $K' \leq L' \leq M$ be a tower of number fields with M normal over K' . Let $G = \text{Gal}(M/K')$ and let $H = \text{Gal}(M/L')$. Let \mathfrak{p} be a prime of K' and let $D_{\mathfrak{p}}$ be a decomposition group of \mathfrak{p} (defined up to conjugation) and let $I_{\mathfrak{p}} \trianglelefteq D_{\mathfrak{p}}$ be the corresponding inertia group. Then the primes above \mathfrak{p} in L are in one-to-one correspondence with the orbits of $D_{\mathfrak{p}}$ on $H \backslash G$. For a given $D_{\mathfrak{p}}$ -orbit, the ramification

² For more details, see Wood’s “How to determine the splitting type of a prime,” available at <https://math.berkeley.edu/~mmwood/Splitting.pdf>.

Table 1. Splitting type for a given decomposition and inertia group.

| I_p | D_p | $\varsigma_p(M)$ | $\varsigma_p(L_1)$ | $\varsigma_p(K_1)$ | $\varsigma_p(L_2)$ | $\varsigma_p(K_2)$ | $\varsigma_p(L)$ | $\varsigma_p(K)$ | | |
|--|--|---------------------|--------------------|--------------------|--------------------|--------------------|------------------|------------------|------------|-----------------------|
| {1} | {1} | (11111111) | (1111) | (11) | (1111) | (11) | (1111) | (11) | Unramified | Lacks central inertia |
| {1} | $\langle \sigma^2 \rangle$ | (2222) | (22) | (11) | (22) | (11) | (1111) | (11) | | |
| {1} | $\langle \sigma\tau \rangle$ | (2222) | (22) | (2) | (112) | (11) | (22) | (2) | | |
| {1} | $\langle \tau \rangle$ | (2222) | (112) | (11) | (22) | (2) | (22) | (2) | | |
| {1} | $\langle \sigma \rangle$ | (44) | (4) | (2) | (4) | (2) | (22) | (11) | | |
| $\langle \tau \rangle$ | $\langle \tau \rangle$ | $(1^2 1^2 1^2 1^2)$ | $(1^2 11)$ | (11) | $(1^2 1^2)$ | (1^2) | $(1^2 1^2)$ | (1^2) | Tame | Has central inertia |
| $\langle \tau \rangle$ | $\langle \tau, \sigma^2 \rangle$ | $(2^2 2^2)$ | $(1^2 2)$ | (11) | (2^2) | (1^2) | $(1^2 1^2)$ | (1^2) | | |
| $\langle \sigma\tau \rangle$ | $\langle \sigma\tau \rangle$ | $(1^2 1^2 1^2 1^2)$ | $(1^2 1^2)$ | (1^2) | $(1^2 11)$ | (11) | $(1^2 1^2)$ | (1^2) | | |
| $\langle \sigma\tau \rangle$ | $\langle \sigma\tau, \sigma^2 \rangle$ | $(2^2 2^2)$ | (2^2) | (1^2) | $(1^2 2)$ | (11) | $(1^2 1^2)$ | (1^2) | | |
| $\langle \sigma \rangle$ | $\langle \sigma \rangle$ | $(1^4 1^4)$ | (1^4) | (1^2) | (1^4) | (1^2) | $(1^2 1^2)$ | (11) | Tame | Has central inertia |
| $\langle \sigma \rangle$ | D_4 | (2^4) | (1^4) | (1^2) | (1^4) | (1^2) | (2^2) | (2) | | |
| $\langle \sigma^2 \rangle$ | $\langle \sigma^2 \rangle$ | $(1^2 1^2 1^2 1^2)$ | $(1^2 1^2)$ | (11) | $(1^2 1^2)$ | (11) | (1111) | (11) | | |
| $\langle \sigma^2 \rangle$ | $\langle \tau, \sigma^2 \rangle$ | $(2^2 2^2)$ | $(1^2 1^2)$ | (11) | (2^2) | (2) | (22) | (2) | | |
| $\langle \sigma^2 \rangle$ | $\langle \sigma\tau, \sigma^2 \rangle$ | $(2^2 2^2)$ | (2^2) | (2) | $(1^2 1^2)$ | (11) | (22) | (2) | | |
| $\langle \sigma^2 \rangle$ | $\langle \sigma \rangle$ | $(2^2 2^2)$ | (2^2) | (2) | (2^2) | (2) | (22) | (11) | | |
| $\langle \tau, \sigma^2 \rangle$ | $\langle \tau, \sigma^2 \rangle$ | $(1^4 1^4)$ | $(1^2 1^2)$ | (11) | (1^4) | (1^2) | $(1^2 1^2)$ | (1^2) | Wild | Has central inertia |
| $\langle \sigma\tau, \sigma^2 \rangle$ | $\langle \sigma\tau, \sigma^2 \rangle$ | $(1^4 1^4)$ | (1^4) | (1^2) | $(1^2 1^2)$ | (11) | $(1^2 1^2)$ | (1^2) | | |
| D_4 | D_4 | (1^8) | (1^4) | (1^2) | (1^4) | (1^2) | (1^4) | (1^2) | | |

index e of the prime it corresponds to is the size of an I_p -orbit therein and the inertia degree f is the number of such suborbits. (Note all such suborbits have the same size since I_p is normal in D_p .) To compute all the values in Table 1, we have an example script available at <https://github.com/khwilson/D4Counting>.

In Table 1, the first group consists of unramified splitting types, the second and third groups consist of tamely ramified splitting types, and the fourth group consists of wildly ramified splitting types. In particular, the splitting type of an odd prime p must appear in the first three groups of Table 1. We distinguish between the tamely ramified splitting types depending on whether the center $\langle \sigma^2 \rangle$ of D_4 is contained in I_p .

Definition 2.3. We say that a D_4 -quartic L_1 (or a pair (L_1, K_1) consisting of a D_4 -quartic L_1 and its quadratic subfield K_1) has central inertia at p when I_p contains σ^2 , or equivalently when the pair $(\varsigma_p(L_1), \varsigma_p(K_1))$ is $((1^2 1^2), (11))$, $((2^2), (2))$, or $((1^4), (1^2))$.

Note that if M and K are as in (5), the extension M/K is ramified at a prime p if and only if (L_1, K_1) has central inertia at p .

By analogy, we define splitting types at ∞ . If K is any quadratic field and L is any quartic field, we write

$$\varsigma_\infty(K) := \begin{cases} (11) & \text{if } K \otimes \mathbb{R} = \mathbb{R}^2, \\ (2) & \text{if } K \otimes \mathbb{R} = \mathbb{C}; \end{cases} \quad \varsigma_\infty(L) := \begin{cases} (1111) & \text{if } L \otimes \mathbb{R} = \mathbb{R}^4, \\ (112) & \text{if } L \otimes \mathbb{R} = \mathbb{R}^2 \oplus \mathbb{C}, \\ (22) & \text{if } L \otimes \mathbb{R} = \mathbb{C}^2. \end{cases} \quad (6)$$

2.3. Invariants of D_4 -quartics

Next, we compare the Artin conductor of a D_4 -quartic L_1 to the discriminant of L_1 as well as the products of the discriminants of certain subfields of the normal closure of L_1 . Additionally, we define two fundamental invariants and a slightly refined conductor that partially recovers the splitting type of L_1 at ∞ .

If $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denotes the absolute Galois group of \mathbb{Q} , and M is the normal closure of L_1 as in (5), then there is a (unique up to conjugacy) irreducible 2-dimensional Galois representation

$$\rho_M : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{C})$$

that factors through $\text{Gal}(M/\mathbb{Q})$. It arises as the composition of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \text{Gal}(M/\mathbb{Q})$ and the unique 2-dimensional irreducible representation of $D_4 \cong \text{Gal}(M/\mathbb{Q})$. We let $\text{Cond}(\rho_M)$ denote the Artin conductor of ρ_M . This invariant can be described in terms of the discriminant of the quadratic subfield K_1 and $\text{Nm}_{K_1}(\text{Disc}(L_1/K_1))$, the image under the norm map of K_1 of the relative discriminant of L_1 over K_1 :

Proposition 2.4. *Let L_1 denote a D_4 -quartic with normal closure M , and let K_1 be its quadratic subfield. Then*

$$\text{Cond}(\rho_M) = |\text{Disc}(K_1) \cdot \text{Nm}_{K_1}(\text{Disc}(L_1/K_1))|.$$

Proof. The proposition will follow from the fact that the representation $\text{Ind}_{\langle \tau \rangle}^{D_4} \mathbb{1}$ of D_4 decomposes into a direct sum of $\text{Ind}_{\langle \tau, \sigma^2 \rangle}^{D_4} \mathbb{1}$ and the irreducible 2-dimensional representation of D_4 . To prove this fact, first note that each coset of $\langle \tau \rangle$ in D_4 contains a unique power of σ , so we can represent $\text{Ind}_{\langle \tau \rangle}^{D_4}$ in terms of the basis $\langle [1], [\sigma], [\sigma^2], [\sigma^3] \rangle$. We can then decompose $\text{Ind}_{\langle \tau \rangle}^{D_4} \mathbb{1} = V_1 \oplus V_2$ where

$$V_1 = \langle [1] + [\sigma^2], [\sigma] + [\sigma^3] \rangle, \quad V_2 = \langle [1] - [\sigma^2], [\sigma] - [\sigma^3] \rangle.$$

Since σ swaps the two basis elements of V_1 while τ and σ^2 act trivially, V_1 can be identified with $\text{Ind}_{\langle \tau, \sigma^2 \rangle}^{D_4} \mathbb{1}$. Furthermore, one can see that V_2 is irreducible, and it is well-known that there is a unique irreducible 2-dimensional representation of D_4 .

Now, if M is the normal closure of L_1 as in (5) and ρ denotes the Galois representation constructed by composing $\text{Ind}_{\langle \tau \rangle}^{D_4} \mathbb{1}$ with $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \text{Gal}(M/\mathbb{Q})$, then its Artin conductor satisfies

$$\text{Cond}(\rho) = |\text{Disc}(L_1)|.$$

We can compute $\text{Cond}(\rho)$ as a product of the conductors of its subrepresentations: the Galois representation $\text{Ind}_{\langle \tau, \sigma^2 \rangle}^{D_4} \mathbb{1} \circ (\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \text{Gal}(M/\mathbb{Q}))$ has conductor $\text{Disc}(K_1)$, so we obtain

$$|\text{Disc}(L_1)| = |\text{Disc}(K_1)| \cdot \text{Cond}(\rho_M).$$

The relative discriminant formula implies $|\text{Disc}(L_1)| = \text{Disc}(K_1)^2 \text{Nm}_{K_1}(\text{Disc}(L_1/K_1))$, and so we conclude the proposition. □

Definition 2.5. The (signed) conductor $C(L_1)$ of a D_4 -quartic L_1 whose quadratic subfield is denoted by K_1 is defined as

$$C(L_1) := \frac{\text{Disc}(L_1)}{\text{Disc}(K_1)}.$$

From the definition of the conductor and Proposition 2.4, it follows immediately that two D_4 -quartics L_1 and L_2 with the same normal closure M have the same conductor. Furthermore, if L_1 has no central inertia, then $C(L_1) = \text{Disc}(K_1) \cdot \text{Disc}(\phi(K_1))$. More precisely, if L is a number field and p is a prime number, let $\text{Disc}_p(L)$ denote the p -part of the discriminant, and let $C_p(L)$ be the p -part of the conductor. We then have:

Proposition 2.6. *If L_1 is a D_4 -quartic with quadratic subfield K_1 , then for all odd primes p ,*

$$C_p(L_1) = \begin{cases} p^2 \cdot \text{Disc}_p(K_1) \cdot \text{Disc}_p(\phi(K_1)) & \text{if } I_p = \langle \sigma^2 \rangle, \\ \text{Disc}_p(K_1) \cdot \text{Disc}_p(\phi(K_1)) & \text{otherwise.} \end{cases}$$

Proof. We refer to the notation described in (5), where $\phi(K_1) = K_2$. Table 1 shows that if $I_p \neq \langle \sigma^2 \rangle$, then $\text{Disc}_p(K_2) = \text{Nm}_{K_1}(\text{Disc}_p(L_1/K_1))$. Thus, $C_p(L_1) = \text{Disc}_p(K_1) \cdot \text{Disc}_p(K_2)$. However, when $I_p = \langle \sigma^2 \rangle$, Table 1 implies that $\text{Disc}_p(K_1) = \text{Disc}_p(K_2) = 1$, but $\text{Nm}_{K_1}(\text{Disc}_p(L_1/K_1)) = \text{Nm}_{K_2}(\text{Disc}_p(L_2/K_2)) = p^2$. Thus, we find that $C_p(L_1) = p^2 \cdot \text{Disc}_p(K_1) \cdot \text{Disc}_p(K_2)$. □

We are now ready to define the two fundamental invariants of a D_4 -quartic.

Definition 2.7. If L_1 is a D_4 -quartic with quadratic subfield K_1 , define the *fundamental invariants* of L_1 :

$$q(L_1) := \frac{\text{Disc}(L_1)}{\text{Disc}(K_1)^2} \quad \text{and} \quad d(L_1) := \text{Disc}(K_1).$$

Remark 2.8. For a D_4 -quartic L_1 , there is a global restriction on the integers $q(L_1)$ and $d(L_1)$, namely that they are each congruent to 0 or 1 mod 4. Both of these are due to (a generalization of) Stickelberger’s Theorem, though we note that $|q(L_1)| = |\text{Nm}_{K_1}(\text{Disc}(L_1/K_1))|$ requires carefully dealing with infinite places of relative discriminants. See [25] for details.

Proposition 2.4 can be reformulated as

$$\text{Cond}(\rho_M) = |q(L_1) \cdot d(L_1)| = |q(L_2) \cdot d(L_2)|$$

for a D_4 -quartic L_1 and $L_2 = \phi(L_1)$ as in (5). Define

$$J(L_1) := \frac{C(L_1)}{\text{Disc}(K_1) \cdot \text{Disc}(\phi(K_1))} = \left| \frac{q(L_1)}{d(\phi(L_1))} \right|, \tag{7}$$

and for a prime p , let $J_p(L_1)$ denote the p -part of $J(L_1)$. Proposition 2.6 determines that for an odd prime p , $J_p(L_1)$ is equal to p^2 if and only if the inertia group I_p at p is equal to $\langle \sigma^2 \rangle \subset D_4$. Note that it is always true that $J(L_1) = J(\phi(L_1))$. Furthermore, it will not be necessary in what follows to compute J_2 ; it will be enough that J_2 is absolutely bounded.

3. Heuristics for counting D_4 -quartics by conductor

In [3], Bhargava developed heuristics for the asymptotics of the number of S_n -fields of degree n ordered by discriminant. The framework used to formulate these heuristics was expanded by Kedlaya [20] for families of Galois representations ordered by their Artin conductor. Additionally, Wood [29] predicted asymptotics (including mass formulae for the constants) for fixed-degree families of number fields whose normal closures have a fixed Galois group when such fields are ordered by invariants including the conductor. In this section, we adapt their heuristics to the family of D_4 -quartics ordered by our two fundamental invariants, q and d (see Definition 2.7). We recover the predictions in [29] for the number of D_4 -quartics ordered either by conductor or discriminant, and we additionally verify that the conjectured mass formula when ordering by discriminant is *not* equal to the constant c determined by Cohen, Diaz y Diaz and Olivier in [9].

3.1. The expected number of D_4 -quartics with fixed fundamental invariants

Let v be a place of \mathbb{Q} , and let $K_v \subset L_v$ be étale algebras of \mathbb{Q}_v of degrees 2 and 4, respectively. When v corresponds to a finite prime p (resp. infinity), we say that such a pair (L_v, K_v) is *compatible* with a pair of integers (q, d) if the p -parts (resp. signs) of $\text{Nm}_{K_v}(\text{Disc}(L_v/K_v))$, the norm in \mathbb{Q}_v of the relative discriminant of L_v over K_v , and $\text{Disc}(K_v)$, the discriminant of K_v , agree with the p -parts (resp. signs) of q and d , respectively. Note that when $q > 0$, d can be positive or negative; however, when $q < 0$, d must be positive, otherwise no such compatible pairs (L_∞, K_∞) exist.

Given a place v of \mathbb{Q} and integers q and d , let $\Sigma_v(q, d)$ denote the set of pairs of \mathbb{Q}_v -algebras (L_v, K_v) that are compatible with (q, d) . Let the *weighted local mass* $E_v(q, d)$ be defined by

$$E_v(q, d) := \sum_{(L_v, K_v) \in \Sigma_v(q, d)} \frac{1}{\#\text{Aut}(L_v, K_v)},$$

where $\text{Aut}(L_v, K_v)$ is the group of automorphisms of L_v that restrict to endomorphisms of the subalgebra K_v . The following result evaluates $E_v(q, d)$ for all places v .

- Proposition 3.1.** (1) *If q and d are non-zero, then $E_\infty(q, d) = 1/4$ when at least one of q or d is positive.*
 (2) *If v corresponds to an odd prime p , then $E_p(q, d)$ is non-empty if and only if the p -parts of (q, d) are one of $(1, 1)$, $(p, 1)$, $(p^2, 1)$, $(1, p)$, or (p, p) . In each case, we have $E_p(q, d) = 1$.*
 (3) *The values of $E_2(q, d)$ are given below.*

Proof. The proof is by direct computation. For $p = \infty$, the result is immediate. For p odd, we note that as there is no wild ramification, the computation of q and d depends only on the Galois decomposition, and the inertia groups of the component fields of K_v and L_v . However, it turns out this enumeration depends only on whether $p \equiv 1 \pmod{4}$.

Explicitly, for odd primes p , Kummer theory implies that the quadratic extensions of a p -adic field K are in one-to-one correspondence with the non-trivial square classes

Table 2. The value of $E_2(q, d)$.

| q | d = 1 | d = 2 ² | d = 2 ³ |
|----------------|-------|--------------------|--------------------|
| 1 | 1 | 1 | 2 |
| 2 ² | 1 | 1 | 2 |
| 2 ³ | 2 | — | — |
| 2 ⁴ | 2 | 2 | 4 |
| 2 ⁵ | 2 | 4 | 8 |
| 2 ⁶ | 4 | — | — |

$K^\times/(K^\times)^2$. Combining this with Hensel’s Lemma, we conclude that for each odd prime p , there are exactly three possible quadratic extensions of any p -adic field K corresponding to adjoining the square root of u , π , and $u\pi$, where u is a (lift of a) quadratic non-residue in \mathcal{O}_K and π is a uniformizer.

For odd primes, this implies that there are up to $3 \times 3 = 9$ possible quartic fields L_v which could be extensions of K_v . However, many of these fields are actually isomorphic as fields over \mathbb{Q}_p . The number of possible isomorphism classes (and their associated automorphisms, decomposition groups, and inertia groups) turns out to only depend on the value of $p \pmod 4$.

Explicitly, the unramified quadratic extension K_0 of \mathbb{Q}_p has three quadratic extensions, one of which is $\mathbb{Q}_p(\sqrt{u'})$ where u' is a quadratic non-residue in K_0 ; it is unramified and has Galois group C_4 . Another is $\mathbb{Q}_p(\sqrt{u}, \sqrt{p})$; it is a C_2^2 field with decomposition group equal to the inertia group that fixes K_0 . The final extension is $\mathbb{Q}_p(\sqrt{u'p})$; it is ramified and has Galois group C_4 and decomposition group equal to the inertia group $C_2 \leq C_4$.

This leaves $2 \times 2 = 4$ possible quartic extensions of \mathbb{Q}_p . Hensel’s Lemma directly implies that the possible fields are $\mathbb{Q}_p(\sqrt[4]{p})$, $\mathbb{Q}_p(\sqrt[4]{4p})$, $\mathbb{Q}_p(\sqrt[4]{-2p})$, and $\mathbb{Q}_p(\sqrt[4]{-8p})$. If $p \equiv 1 \pmod 4$ then $x^4 - 1$ has four distinct roots in the residue field \mathbb{F}_p of \mathbb{Z}_p and the above fields are distinct, each with Galois group, decomposition group, and inertia group C_4 . On the other hand, when $p \equiv 3 \pmod 4$, $x^4 - 1$ has two solutions, and none of these fields is Galois and thus they are D_4 -fields. The fields $\mathbb{Q}_p(\sqrt[4]{x})$ and $\mathbb{Q}_p(\sqrt[4]{-4x})$ are isomorphic. The decomposition group is all of D_4 and the inertia group the rotation subgroup $\langle \sigma^2 \rangle$.

At $p = 2$, the number of quartic extensions of \mathbb{Q}_p is much larger, and wild ramification makes the computation of q and d much more complicated. However, a database of local fields, e.g., [21, 19], can be used. The details of the computation can be found at <http://github.com/khwilson/D4Counting>. □

The framework in [3, 29] depends on the basic heuristic assumption that for a family of number fields of fixed degree and fixed associated Galois group, the completions at different places behave independently of one another. This implies that the expected number of such number fields having given invariants is equal to the infinite product over all places v of \mathbb{Q} of the weighted number of local extensions of \mathbb{Q}_v that are compatible with those invariants. More precisely:

Assumption 3.2. *If $E(q, d)$ denotes the expected number of isomorphism classes of D_4 -quartics with fundamental invariants equal to q and d , we assume*

$$E(q, d) = \frac{1}{2} \cdot E_\infty(q, d) \cdot \prod_p E_p(q, d). \tag{8}$$

The extra factor of $1/2$ above arises from two issues: (1) there is a global restriction on the invariants q and d (see Remark 2.8), which occurs $1/4$ of the time, and is not taken into account by the local masses, and (2) the product of the local masses $E_v(q, d)$ determines the expected *weighted* number of D_4 -quartics with invariants q and d , where a D_4 -quartic L is weighted by $\#\text{Aut}(L)^{-1} = 1/2$.

3.2. *Predictions for the global distribution of D_4 -quartics using double Dirichlet series*

To determine the asymptotics of $\sum E(q, d)$, we study the behavior of the double Dirichlet series

$$\xi(s, t) := \sum_d \sum_q \frac{E(q, d)}{|q|^s |d|^t},$$

which converges absolutely for $s, t > 1$. Since there are three possible sign configurations for the pair (q, d) of integers, the archimedean contribution to $\xi(s, t)$ is exactly $3/4$. Additionally, $2 \cdot E(q, d)$ is multiplicative with respect to both q and d , and so it follows from Proposition 3.1 that $\xi(s, t)$ can be expressed as

$$\xi(s, t) = \frac{3}{8} \cdot \prod_p \xi_p(s, t),$$

where

$$\xi_p(s, t) = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^t} \left(1 + \frac{1}{p^s} \right)$$

when p is odd, and

$$\begin{aligned} \xi_2(s, t) = & 1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}} + \frac{2}{2^{4s}} + \frac{2}{2^{5s}} + \frac{4}{2^{6s}} + \frac{1}{2^{2t}} \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{4s}} + \frac{4}{2^{5s}} \right) \\ & + \frac{2}{2^{3t}} \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{4s}} + \frac{4}{2^{5s}} \right). \end{aligned}$$

Define the correction factor at 2 to be

$$\tilde{\xi}_2(s, t) := \xi_2(s, t) / \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^t} \left(1 + \frac{1}{2^s} \right) \right).$$

We can rewrite $\xi(s, t)$ as

$$\begin{aligned} \xi(s, t) = & \frac{3}{8} \cdot \tilde{\xi}_2(s, t) \cdot \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^t} \left(1 + \frac{1}{p^s} \right) \right) \\ = & \frac{3}{8} \cdot \tilde{\xi}_2(s, t) \cdot \zeta(s) \cdot \zeta(t) \cdot \prod_p (1 - p^{-2t} - p^{-t-2s} - p^{-3s} + p^{-2t-2s} + p^{-t-3s}). \end{aligned}$$

Therefore, the function $\xi(s, t)$ is holomorphic in the region $t > 1/2, s > 1/3$ aside from poles at the lines $s = 1$ and $t = 1$.

3.3. Heuristics

We now consider families of D_4 -quartics under different orderings. If X and Y are positive real numbers going to infinity, let $E_{q,d}(X, Y)$ denote the expected number of isomorphism classes of D_4 -quartics L such that $|q(L)| < X$ and $|d(L)| < Y$, i.e.

$$E_{q,d}(X, Y) := \sum_{\substack{|q| < X \\ |d| < Y}} E(q, d).$$

Then, by computing the residue of $\xi(s, t)$ at $(1, 1)$, we obtain the heuristic

$$E_{q,d}(X, Y) \sim \frac{3}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) \cdot X \cdot Y. \tag{9}$$

Here, the correction factor $\tilde{\xi}_2(1, 1)$ is 1. Note that this heuristic only relies on Assumption 3.2. If we were to take (8) as a definition, then we have completely verified the main term (9), and we can additionally obtain a power saving.

Heuristics for the family of D_4 -quartics ordered by conductor.

Next, we consider the family of D_4 -quartics ordered by conductor. Let $E_C(X)$ denote the expected number of isomorphism classes of D_4 -quartics L such that $|C(L)| < X$. If we let $E(C)$ denote the expected number of D_4 -quartics with conductor C , then

$$\sum_C \frac{E(C)}{|C|^s} = \xi(s, s)$$

since $C(L) = q(L)d(L)$. The function $\xi(s, s)$ has a double pole at 1 and, by computing its residue, we obtain

$$E_C(X) \sim \frac{3}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) \cdot X \log X. \tag{10}$$

The correction factor at 2 is again $\tilde{\xi}_2(1, 1) = 1$.

Heuristics for the family of D_4 -quartics ordered by discriminant. Finally, we consider the family of D_4 -quartics ordered by discriminant. Let $E_{\text{Disc}}(X)$ denote the expected number of isomorphism classes of D_4 -quartics L such that $|\text{Disc}(L)| < X$. If we let $E(\text{Disc})$ denote the expected number of D_4 -quartics L with discriminant Disc , then

$$\sum_{\text{Disc}} \frac{E(\text{Disc})}{|\text{Disc}|^s} = \xi(s, 2s)$$

since $\text{Disc}(L) = q(L)d(L)^2$. The function $\xi(s, 2s)$ has a simple pole at 1 and, by computing the residue, we obtain

$$E_{\text{Disc}}(X) \sim \frac{3 \cdot 11^2}{2^6 \cdot 17} \cdot \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4} \right) \cdot X. \tag{11}$$

In this case, the correction factor at 2 is $\tilde{\xi}_2(1, 2) = 11^2/(17 \cdot 2^3)$.

Cohen, Diaz y Diaz and Olivier showed in [9, Proposition 6.2] that the number of D_4 -quartics having discriminant bounded by X is $\sim cX$ where $c \approx 0.052$, whereas the constant on the right hand side of (11) is ≈ 0.406 . This implies that when ordering D_4 -quartics by discriminant, the completions of such fields at different primes do *not* behave independently of one another in the sense of [3], and so Assumption 3.2 does not hold.

4. Counting D_4 -quartics using analytic methods

In this section, we obtain asymptotics for the number of D_4 -quartics, ordered by conductor, whose quadratic subfield has small discriminant, following the methods of Cohen, Diaz y Diaz and Olivier [9] where similar asymptotics for the number of such D_4 -quartics ordered by discriminant are determined. By refining their arguments, we are able to count D_4 -quartics of bounded conductor whose quadratic subfields have small discriminant and satisfy a prescribed set of splitting conditions at a finite number of primes. We begin with a few definitions before giving the precise statement of the main theorem of the section.

Definition 4.1. If K is a quadratic field and L is a quadratic extension of K , define the *conductor* of the pair (L, K) as

$$C(L, K) := \frac{\text{Disc}(L)}{\text{Disc}(K)}. \tag{12}$$

If L is a D_4 -quartic and K denotes its (unique) quadratic subfield, then $C(L, K) = C(L)$.

We refine the notion of a collection of local specifications described in the introduction. Let $\Sigma_v^{\text{full}} = \{(\varsigma_v(L), \varsigma_v(K))\}$ be the set of all pairs consisting of a possible splitting type for a place v in a D_4 -quartic L and a consistent splitting type at v for its quadratic subfield K . We refer to a collection $\Sigma = (\Sigma_v)_v$ as a set of *local specifications* if $\Sigma_v \subseteq \Sigma_v^{\text{full}}$ for each v .

Definition 4.2. A set $\Sigma = (\Sigma_v)_v$ of local specifications is *stable* if for every prime p and every quadratic splitting type ς'_p (equal to either (11), (2), or (1^2)), the set Σ_p either contains all possible pairs $(*, \varsigma'_p)$ or none of them.

Additionally, we denote by $\mathcal{L}(\Sigma)$ the set of D_4 -quartics L with quadratic subfield K such that $(\varsigma_v(L), \varsigma_v(K)) \in \Sigma_v$ for all v . Similarly, let $\mathcal{K}(\Sigma)$ denote the set of quadratic subfields of $\mathcal{L}(\Sigma)$. Note that when Σ is stable, the set $\mathcal{L}(\Sigma)$ consists of all D_4 -quartics that are quadratic extensions of all the fields in $\mathcal{K}(\Sigma)$.

For a set Σ of local specifications, let $N_C(\Sigma; X, Y)$ be the number of isomorphism classes of D_4 -quartics $L \in \mathcal{L}(\Sigma)$ such that $|C(L)| < X$ and $|d(L)| < Y$. Additionally, set $N_C(X, Y) := N_C(\Sigma^{\text{full}}; X, Y)$. In this section, we compute asymptotics for $N_C(\Sigma; X, X^\beta)$ when Σ is stable and $\beta < 2/3$. More precisely, our goal is to prove the following theorem:

Theorem 4.3. *Let Σ be a stable set of local specifications. Then, for every $\beta < 2/3$, we have*

$$N_C(\Sigma; X, X^\beta) = \frac{1}{2\zeta(2)} \cdot \left(\sum_{\substack{K \in \mathcal{K}(\Sigma) \\ |Disc(K)| < X^\beta}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{2^{-r_2(K)}}{|Disc(K)|} \right) \cdot X + o_\beta(X),$$

We do so by first demonstrating that the number of quadratic extensions of quadratic number fields that are not D_4 -quartic fields is negligible, so we can compute $N_C(\Sigma; X, X^\beta)$ in terms of these towers of quadratic extensions. In [9], the authors define a Dirichlet series for each quadratic field K whose residue at $s = 1$ is shown to be the number of quadratic extensions of K . We then carry out a smooth count for the quartic fields in $\mathcal{L}(\Sigma)$ that are quadratic extensions of K and subsequently obtain the theorem by summing over all $K \in \mathcal{K}(\Sigma)$.

4.1. Quadratic extensions of quadratic number fields

If L is a quadratic extension of a quadratic field K , then either L is a D_4 -quartic or it is Galois with $\text{Gal}(L/\mathbb{Q}) = C_4$ or V_4 . In the following lemma, we prove a bound for the number of pairs (L, K) having bounded conductor, where L is a Galois quartic field and K is a quadratic subfield of L having small discriminant.

Lemma 4.4. *Let $\beta < 1$ be fixed. The number of pairs of (L, K) , where L is a Galois quartic field, K is a quadratic subfield of L , $C(L, K) < X$, and $|Disc(K)| < X^\beta$ is bounded by $O_\epsilon(X^{(1+\beta)/2+\epsilon})$.*

Proof. Let (L, K) be a pair satisfying the conditions of the lemma. By the relative discriminant formula, we have

$$|Disc(L)| = |Disc(K) \cdot C(L, K)| < X^{1+\beta}.$$

It is known from [10, §§2.4–2.5] that the number of Galois quartic fields whose discriminant has absolute value less than X is bounded by $O_\epsilon(X^{1/2+\epsilon})$. The lemma follows immediately. □

For stable Σ , we can thus prove Theorem 4.3 by counting the number of quadratic extensions over quadratic fields in $\mathcal{K}(\Sigma)$ whose relative discriminants have bounded norm. To this end, we consider the Dirichlet series $\Phi_{K,2}(s) = \Phi_{K,2}(C_2, s)$ defined in [9] for any number field K as

$$\Phi_{K,2}(s) := \sum_{[L:K]=2} \frac{1}{\text{Nm}_K(Disc(L/K))^s}.$$

It is proved in [9, Theorem 1.1] that

$$\Phi_{K,2}(s) = -1 + \frac{2^{-r_2(K)}}{\zeta_K(2s)} \cdot \sum_{\mathfrak{c}|2} \frac{\text{Nm}_K(2/\mathfrak{c})}{\text{Nm}_K(2/\mathfrak{c})^{2s}} \cdot \sum_{\chi \in \text{Cl}(K, \mathfrak{c}^2)^\vee} L_K(s, \chi),$$

where $r_2(K)$ denotes the number of pairs of complex embeddings of K , \mathfrak{c} runs over all integral ideals of K dividing 2, χ runs over all quadratic characters of the ray class group modulo \mathfrak{c}^2 , and $L_K(s, \chi)$ is the L -function of K for χ . It is also proven in [9, Corollary 1.2] that the rightmost pole of $\Phi_{K,2}(s)$ is at $s = 1$ with residue

$$\text{Res}_{s=1} \Phi_{K,2}(s) = \frac{2^{-r_2(K)}}{\zeta(2)} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})}. \tag{13}$$

We can then obtain “smooth counts” of the number of quadratic extensions of quadratic fields K :

Lemma 4.5. *Let φ be a smooth compactly supported function $\varphi : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$. If K is quadratic, then*

$$\begin{aligned} & \sum_{[L:K]=2} \varphi\left(\frac{|\text{Disc}(K) \cdot \text{Nm}_K(\text{Disc}(L/K))|}{X}\right) \\ &= \text{Vol}(\varphi) \cdot \text{Res}_{s=1} \Phi_{K,2}(s) \cdot \frac{X}{|\text{Disc}(K)|} + O_{\epsilon, \varphi}(2^{\omega(\text{Disc}(K))} |\text{Disc}(K)|^{-1/4+\epsilon} X^{1/2+\epsilon}), \end{aligned}$$

where $\omega(d)$ denotes the number of prime divisors of d , and $\text{Vol}(\varphi)$ denotes $\int \varphi(t) dt$.

Proof. Let $\tilde{\varphi}$ denote the Mellin transform of φ . By Mellin inversion, the left hand side of the above equation is equal to

$$\frac{1}{2\pi i} \int_{\text{Re}(s)=2} \tilde{\varphi}(s) \cdot \frac{X^s}{|\text{Disc}(K)|^s} \cdot \Phi_{K,2}(s) ds.$$

Shifting the line of integration to $\text{Re}(s) = 1/2 + \epsilon$, we pick up the main term from the pole at 1 since $\tilde{\varphi}(1) = \text{Vol}(\varphi)$. The error term follows by using the convexity bound of $O_\epsilon(|\text{Disc}(K)|^{1/4+\epsilon})$ near $s = 1/2$ at each of the $O(2^{\omega(\text{Disc}(K))})$ L -functions used to define $\Phi_{K,2}(s)$. □

The next lemma, whose proof is very similar to that of Lemma 4.5, gives a bound when imposing ramification on the quadratic extensions of a fixed quadratic field K and will only be used in §8:

Lemma 4.6. *If K is a quadratic field and \mathfrak{f} is a squarefree product of prime ideals in K , then the number of quadratic extensions L over K such that $\text{Nm}_K(\text{Disc}(L/K)) < X$ and every prime dividing \mathfrak{f} ramifies in L is bounded by*

$$O_\epsilon\left(\frac{L(1, K/\mathbb{Q})}{\text{Nm}(\mathfrak{f})} \cdot X + \frac{|\text{Disc}(K)|^{-1/4}}{\text{Nm}(\mathfrak{f})^{1/2}} \cdot X^{1/2+\epsilon}\right).$$

Proof. We can (and do) assume that f is odd. Since an upper bound for the number of quadratic extensions of K can be obtained with a smooth sum, we proceed as in the proof of Lemma 4.5. The only difference is that we use, instead of $\Phi_{K,2}(s)$, the Dirichlet series $\Phi_{K,2,f}(s)$ corresponding to extensions L of K that are ramified at every prime dividing f :

$$\begin{aligned} \Phi_{K,2,f}(s) &:= \sum_{\substack{[L:K]=2 \\ L \text{ ramified at } f}} \frac{1}{\text{Nm}_K(\text{Disc}(L/K))^s} \\ &= -1 + \frac{2^{-r_2(K)}}{\zeta_K(2s)} \cdot \sum_{c|2} \text{Nm}_K(c)^{2s-1} \cdot \sum_{\chi \in \text{Cl}(K, c^2)^\vee} \left(\sum_{\substack{a \text{ squarefree} \\ (a,c)=1, f|a}} \frac{\chi(a)}{\text{Nm}_K(a)^s} \right), \end{aligned}$$

where the notation is as in the definition of $\Phi_{K,2}(s)$. Since the residue of $\Phi_{K,2,f}(s)$ at 1, its rightmost pole, is $\ll L(1, K/\mathbb{Q})/\text{Nm}(f)$, the lemma follows from an argument identical to the proof of Lemma 4.5. □

4.2. Proof of Theorem 4.3

We are now ready to prove the main result of this section. From Lemma 4.4, it follows that we may estimate $N_C(\Sigma; X, X^\beta)$ by counting quadratic extensions L of quadratic fields K . Let $\chi_{[0,1]}$ denote the characteristic function of $[0, 1]$. Then

$$N_C(\Sigma; X, X^\beta) = \frac{1}{2} \sum_{\substack{K \in \mathcal{K}(\Sigma) \\ |\text{Disc}(K)| < X^\beta}} \sum_{[L:K]=2} \chi_{[0,1]} \left(\frac{|\text{Disc}(K) \cdot \text{Nm}_K(\text{Disc}(L/K))|}{X} \right). \tag{14}$$

The factor of 1/2 on the right hand side of (14) is to account for the fact that a D_4 -quartic L and its conjugate L' both contribute to the inner sum, while the left hand side of (14) counts D_4 -quartics up to conjugacy.

For $\epsilon > 0$, choose φ^\pm to be smooth compactly supported functions such that $\varphi^\pm - \chi_{[0,1]}$ takes values in \mathbb{R}^\pm and $\text{Vol}(\varphi^\pm) = 1 \pm \epsilon$. Lemma 4.5 together with (13) implies that

$$\begin{aligned} \sum_{\substack{K \in \mathcal{K}(\Sigma) \\ |\text{Disc}(K)| < X^\beta}} \sum_{[L:K]=2} \varphi^\pm \left(\frac{|\text{Disc}(K) \cdot \text{Nm}_K(\text{Disc}(L/K))|}{X} \right) \\ = \sum_{\substack{K \in \mathcal{K}(\Sigma) \\ |\text{Disc}(K)| < X^\beta}} \frac{1 \pm \epsilon}{\zeta(2)} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{2^{-r_2(K)}}{|\text{Disc}(K)|} \cdot X \\ + O_\epsilon \left(\sum_{\substack{K \in \mathcal{K}(\Sigma) \\ |\text{Disc}(K)| < X^\beta}} |\text{Disc}(K)|^{-1/4+\epsilon} X^{1/2+\epsilon} \right). \end{aligned}$$

In the above equation, the left hand side corresponding to φ^+ (resp. φ^-) is an upper bound (resp. lower bound) for $N_C(\Sigma; X, X^\beta)$. Meanwhile the error term on the right hand side is bounded by $O_\epsilon(X^{1/2+3\beta/4+\epsilon})$, which, when $\beta < 2/3$, is bounded by $o(X)$. Therefore, Theorem 4.3 follows by letting ϵ tend to 0. □

Remark 4.7. We note that standard analytic methods (namely, Perron’s formula in conjunction with hybrid (sub)convexity bounds on the growth of Hecke L -functions in the critical strip) yield a power saving in the error bound in Theorem 4.3. However, we do not include the arguments since they will not be necessary for the results of this paper.

5. Mass formulae for families of D_4 -quartics

We now turn to the proof of Theorem 2. In the previous section, the constant in the asymptotic number of D_4 -quartics with bounded conductor whose quadratic subfield has small discriminant was determined as a sum of L -values. In §§5.1–5.2, we prove an identity relating the constant in Theorem 4.3 to an Euler product matching the predicted mass formula described in §3.3 by proving that the main contribution to the sum on the right hand side of Theorem 4.3 comes from certain diagonal terms. Finally, in §5.3, we study the family of D_4 -quartics ordered by discriminant, and we prove an interesting identity between the analogous diagonal terms and the heuristic predicted by (11).

5.1. Isolating the diagonal terms in Theorem 4.3

We first prove a lemma that will be used in bounding the non-diagonal terms when we calculate the sum of L -values that appear in Theorem 4.3 in terms of a weighted Möbius sum.

Lemma 5.1. *For any $\epsilon > 0$,*

$$\sum_{\substack{0 < D < X \\ D \text{ squarefree}}} \frac{1}{D} \cdot \left(\sum_{m=1}^{\infty} \sum_{\substack{n=1 \\ mn \neq \square}}^{D^{1/2+\epsilon}} \frac{\mu(m)}{m^2 n} \left(\frac{D}{mn} \right) \right) = O_{\epsilon}(1),$$

where (\cdot) denotes the Legendre symbol.

Proof. The m -sum is absolutely convergent, so we will focus on the n - and D -sums. Interchanging the n - and D -sums yields

$$\sum_{\substack{0 < D < X \\ D \text{ squarefree}}} \frac{1}{D} \cdot \sum_{\substack{n < D^{1/2+\epsilon} \\ mn \neq \square}} \frac{1}{n} \left(\frac{D}{mn} \right) = \sum_{\substack{n < X^{1/2+\epsilon} \\ mn \neq \square}} \frac{1}{n} \cdot \sum_{\substack{n \frac{2}{1+2\epsilon} < D < X \\ D \text{ squarefree}}} \frac{1}{D} \left(\frac{D}{mn} \right). \tag{15}$$

We will now apply a simple squarefree sieve to complete the D -sum and then use the Pólya–Vinogradov inequality to finish the estimate. In particular, we can rewrite (15) as

$$\begin{aligned} & \sum_{\substack{n < X^{1/2+\epsilon} \\ mn \neq \square}} \frac{1}{n} \cdot \left(\sum_{\alpha < n \frac{1}{1+2\epsilon}} \left(\frac{\mu(\alpha)}{\alpha^2} \cdot \sum_{n \frac{2}{1+2\epsilon} \leq \alpha^2 d < X} \frac{1}{d} \cdot \left(\frac{\alpha^2 d}{mn} \right) \right) \right. \\ & \left. + \sum_{n \frac{1}{1+2\epsilon} \leq \alpha < X^{1/2}} \left(\frac{\mu(\alpha)}{\alpha^2} \cdot \sum_{n \frac{2}{1+2\epsilon} \leq \alpha^2 d < X} \frac{1}{d} \cdot \left(\frac{\alpha^2 d}{mn} \right) \right) \right). \end{aligned}$$

Thus, (15) is bounded by

$$\begin{aligned} &\ll \sum_{\substack{n < X^{1/2+\epsilon} \\ mn \neq \square}} \frac{1}{n} \cdot \left(\sum_{\alpha < n^{\frac{1}{1+2\epsilon}}} \frac{1}{\alpha^2} \cdot \left| \sum_{\alpha^{-2}n^{\frac{2}{1+2\epsilon}} \leq d < \alpha^{-2}X} \frac{1}{d} \cdot \left(\frac{\alpha^2 d}{mn} \right) \right| \right. \\ &\qquad \qquad \qquad \left. + \sum_{n^{\frac{1}{1+2\epsilon}} < \alpha < X^{1/2}} \frac{1}{\alpha^2} \cdot \left| \sum_{d < X/\alpha^2} \frac{1}{d} \cdot \left(\frac{\alpha^2 d}{mn} \right) \right| \right) \\ &\ll \sum_{\substack{n < X^{1/2+\epsilon} \\ mn \neq \square}} \frac{m^{1/2} \log(n)}{n^{1/2+\frac{1}{1+2\epsilon}}} = O_\epsilon(m^{1/2}). \end{aligned}$$

The last equality follows from the fact that for ϵ sufficiently small, $\frac{1}{2} + \frac{1}{1+2\epsilon} > \frac{3}{2} - \frac{1}{1000}$, so

$$\sum_{n=1}^\infty \frac{\log(n)}{n^{\frac{1}{2}+\frac{1}{1+2\epsilon}}} = O_\epsilon(1).$$

The lemma then follows from the absolute convergence of $\sum m^{-3/2}$. □

The next result is the key input in obtaining the mass formula. Using Lemma 5.1, we rewrite the sum of L -values appearing in Theorem 4.3 in terms of a weighted Möbius sum that we will later show is equal to an Euler product. When ordering D_4 -quartics by discriminant, there is no known analogue to Proposition 5.2.

Proposition 5.2. *We have*

$$\begin{aligned} &\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < X}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{1}{|\text{Disc}(K)|} \\ &\qquad = \sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < X}} \frac{1}{|\text{Disc}(K)|} \cdot \sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab)=1}} \frac{\mu(a)}{a^3 b^2} + O(1), \\ &\sum_{\substack{[K:\mathbb{Q}]=2 \\ -X < \text{Disc}(K) < 0}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{1}{|\text{Disc}(K)|} \\ &\qquad = \sum_{\substack{[K:\mathbb{Q}]=2 \\ -X < \text{Disc}(K) < 0}} \frac{1}{|\text{Disc}(K)|} \cdot \sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab)=1}} \frac{\mu(a)}{a^3 b^2} + O(1). \end{aligned} \tag{16}$$

Proof. Let χ_K denote the quadratic character associated with K by class field theory so that $L(1, K/\mathbb{Q}) = \sum_{n=1}^\infty \chi_K(n)/n$. From the absolutely convergent Euler product, it is straightforward to see that $L(2, K/\mathbb{Q}) > (\zeta(4)/\zeta(2))^2 > 0$, and hence $1/L(2, K/\mathbb{Q})$ is uniformly bounded independently of K . Using partial summation and the Pólya-Vinogradov inequality, for any $\epsilon > 0$ we get

$$\frac{1}{L(2, K/\mathbb{Q})} \cdot \sum_{n > |\text{Disc}(K)|^{1/2+\epsilon}} \frac{\chi_K(n)}{n} = O_\epsilon \left(\frac{\log |\text{Disc}(K)|}{|\text{Disc}(K)|^\epsilon} \right).$$

Thus, we can conclude that

$$\frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} = \frac{1}{L(2, K/\mathbb{Q})} \cdot \sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \frac{\chi_K(n)}{n} + O_\epsilon\left(\frac{\log |\text{Disc}(K)|}{|\text{Disc}(K)|^\epsilon}\right). \tag{17}$$

Using (17), the left hand sides of (16) are equal to

$$\begin{aligned} & \sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < X}} \frac{1}{|\text{Disc}(K)|} \cdot \left(\frac{1}{L(2, K/\mathbb{Q})} \cdot \sum_{n=1}^{\text{Disc}(K)^{1/2+\epsilon}} \frac{\chi_K(n)}{n} + O_\epsilon\left(\frac{\log \text{Disc}(K)}{\text{Disc}(K)^\epsilon}\right) \right), \\ & \sum_{\substack{[K:\mathbb{Q}]=2 \\ -X < \text{Disc}(K) < 0}} \frac{1}{|\text{Disc}(K)|} \cdot \left(\frac{1}{L(2, K/\mathbb{Q})} \cdot \sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \frac{\chi_K(n)}{n} + O_\epsilon\left(\frac{\log |\text{Disc}(K)|}{|\text{Disc}(K)|^\epsilon}\right) \right). \end{aligned} \tag{18}$$

In either case, the sum of the O_ϵ terms is itself $O_\epsilon(1)$, and so we focus on the remaining term. Using the absolute convergence of the Euler product of $L(2, K/\mathbb{Q})^{-1}$, we have

$$\frac{1}{L(2, K/\mathbb{Q})} \cdot \left(\sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \frac{\chi_K(n)}{n} \right) = \left(\sum_{m=1}^{\infty} \frac{\mu(m)\chi_K(m)}{m^2} \right) \cdot \left(\sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \frac{\chi_K(n)}{n} \right). \tag{19}$$

The key observation we make is that the main contribution to the right hand side of (19) comes from the “diagonal” terms, i.e., when mn is a square. By pulling out these terms, we may rewrite (19) as

$$\sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} + \sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \frac{\chi_K(n)}{n} \cdot \sum_{\substack{m=1 \\ mn \neq \square}}^{\infty} \frac{\mu(m)\chi_K(m)}{m^2}. \tag{20}$$

Substituting (20) back into (18) implies that the left hand sides of (16) are equal to

$$\begin{aligned} & \sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < X}} \frac{1}{\text{Disc}(K)} \cdot \left(\sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} + \sum_{n=1}^{\text{Disc}(K)^{1/2+\epsilon}} \sum_{\substack{m=1 \\ mn \neq \square}}^{\infty} \frac{\mu(m)\chi_K(mn)}{m^2 n} \right) + O_\epsilon(1), \\ & \sum_{\substack{[K:\mathbb{Q}]=2 \\ -X < \text{Disc}(K) < 0}} \frac{1}{|\text{Disc}(K)|} \left(\sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} + \sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \sum_{\substack{m=1 \\ mn \neq \square}}^{\infty} \frac{\mu(m)\chi_K(mn)}{m^2 n} \right) + O_\epsilon(1). \end{aligned}$$

By Lemma 5.1,

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ |\text{Disc}(K)| < X}} \frac{1}{|\text{Disc}(K)|} \cdot \left(\sum_{n=1}^{|\text{Disc}(K)|^{1/2+\epsilon}} \sum_{\substack{m=1 \\ mn \neq \square}}^{\infty} \frac{\mu(m)\chi_K(mn)}{m^2 n} \right) = O_\epsilon(1).$$

Noting that the remaining term does not depend on ϵ , we obtain the proposition. □

5.2. Proof of Theorem 2

We now turn to the proof of Theorem 2. From the identity

$$\sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} = \frac{\zeta(2)}{\zeta(3)} \cdot \prod_{p | \text{Disc}(K)} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}}, \tag{21}$$

we immediately obtain

$$\begin{aligned} & \sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < X}} \frac{1}{\text{Disc}(K)} \cdot \sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} \\ &= \frac{\zeta(2)}{\zeta(3)} \cdot \left(\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0 < \text{Disc}(K) < X}} \frac{1}{\text{Disc}(K)} \cdot \prod_{p | \text{Disc}(K)} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \right), \tag{22} \\ & \sum_{\substack{[K:\mathbb{Q}]=2 \\ -X < \text{Disc}(K) < 0}} \frac{1}{|\text{Disc}(K)|} \cdot \sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} \\ &= \frac{\zeta(2)}{\zeta(3)} \cdot \left(\sum_{\substack{[K:\mathbb{Q}]=2 \\ -X < \text{Disc}(K) < 0}} \frac{1}{|\text{Disc}(K)|} \cdot \prod_{p | \text{Disc}(K)} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \right). \end{aligned}$$

Decomposing the right hand sides of (22) into sums over squarefree integers in a fixed congruence class mod 4, we find that the left hand sides of (22) are equal to

$$\begin{aligned} & \frac{\zeta(2)}{\zeta(3)} \cdot \left(\sum_{\substack{1 < D < X \\ D \equiv 1 \pmod{4} \\ D \text{ squarefree}}} \frac{1}{D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} + \sum_{\substack{1 < D < X \\ D \equiv 3 \pmod{4} \\ D \text{ squarefree}}} \frac{3}{14D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \right. \\ & \qquad \qquad \qquad \left. + \sum_{\substack{1 < D < X \\ D \equiv 1 \pmod{2} \\ D \text{ squarefree}}} \frac{3}{28D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \right), \tag{23} \\ & \frac{\zeta(2)}{\zeta(3)} \cdot \left(\sum_{\substack{-X < D < -1 \\ D \equiv 1 \pmod{4} \\ D \text{ squarefree}}} \frac{1}{D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} + \sum_{\substack{-X < D < -1 \\ D \equiv 3 \pmod{4} \\ D \text{ squarefree}}} \frac{3}{14D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \right. \\ & \qquad \qquad \qquad \left. + \sum_{\substack{-X < D < -1 \\ D \equiv 1 \pmod{2} \\ D \text{ squarefree}}} \frac{3}{28D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \right). \end{aligned}$$

Consider the limit

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{\zeta(2)}{\zeta(3) \log(X)} \cdot \sum_{\substack{1 < D < X \\ D \text{ squarefree}}} \frac{1}{D} \cdot \prod_{p | D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} \\ &= \lim_{X \rightarrow \infty} \frac{\zeta(2)}{\zeta(3) \log(X)} \cdot \sum_{\substack{1 < D < X \\ D \text{ squarefree}}} \prod_{p | D} \frac{1}{p} \cdot \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}}. \tag{24} \end{aligned}$$

Using Perron’s formula, for $\Re(\sigma) > 0$, we can rewrite the right hand side of (24) as

$$\lim_{X \rightarrow \infty} \frac{\zeta(2)}{\zeta(3) \log(X)} \cdot \frac{1}{2\pi i} \cdot \int_{\sigma} \left(\prod_p \left(1 + \frac{1}{p^{s+1}} \cdot \frac{1-p^{-2}}{1-p^{-3}} \right) \right) \cdot X^s \cdot \frac{ds}{s}.$$

The Euler product, for $\sigma > 0$, is equal to

$$\prod_p \left(1 + \frac{1}{p^{s+1}} \cdot \frac{1-p^{-2}}{1-p^{-3}} \right) = \zeta(s+1) \cdot \prod_p \left(1 - \frac{1}{p^{2s+2}} \cdot \frac{1-p^{-2}}{1-p^{-3}} - \frac{1}{p^{s+3}} \cdot \frac{1-p^{-1}}{1-p^{-3}} \right).$$

Note that

$$\prod_p \left(1 - \frac{1}{p^{2s+2}} \cdot \frac{1-p^{-2}}{1-p^{-3}} - \frac{1}{p^{s+3}} \cdot \frac{1-p^{-1}}{1-p^{-3}} \right) = \prod_p \left(1 + O\left(\frac{1}{p^{2s+2}} + \frac{1}{p^{s+3}} \right) \right).$$

Hence, moving the σ contour to the left of $\Re(\sigma) = 0$ and using the Cauchy integral formula, we get³

$$\int_{\sigma} \left(\prod_p \left(1 + \frac{1}{p^{s+1}} \cdot \frac{1-p^{-2}}{1-p^{-3}} \right) \right) \cdot X^s \cdot \frac{ds}{s} = (\log X) \cdot \prod_p \left(1 - \frac{1}{p^2} \cdot \frac{1-p^{-2}}{1-p^{-3}} - \frac{1}{p^3} \cdot \frac{1-p^{-1}}{1-p^{-3}} \right) + o(\log X). \tag{25}$$

The main term on the right hand side of (25) simplifies to

$$\zeta(2)\zeta(3)(\log X) \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right)$$

This shows in particular that we can rewrite the limit in (24) as

$$\lim_{X \rightarrow \infty} \frac{\zeta(2)}{\zeta(3) \log X} \cdot \sum_{\substack{1 < D < X \\ D \text{ squarefree}}} \frac{1}{D} \cdot \prod_{p|D} \frac{1 - \frac{1}{p^2}}{1 - \frac{1}{p^3}} = \zeta(2) \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right).$$

Carrying out the analogous computation for each term in both equations of (23) yields Theorem 2. □

Theorems 2 and 4.3 immediately imply the following result.

Theorem 5.3. *Let $\beta < 2/3$ be fixed. For the family of all D_4 -quartics,*

$$N_C(X, X^\beta) = \frac{3\beta}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4} \right) \cdot X \log X + O(X).$$

It follows from the heuristics of §3.3 that the family of D_4 -quartics L satisfying $|d(L)| \leq |C(L)|^{2/3}$ satisfies the mass formula (10) when such fields are ordered by their conductors. In §§6–8, we prove a refinement of Theorem 5.3 by adapting the arguments in [2] in conjunction with the analytic techniques used in Section 4.

³ One can in fact obtain a better error term, but it is unnecessary for establishing the results of the current article.

5.3. Diagonal terms for the family of D_4 -quartics ordered by discriminant

We would like to conclude this section by considering asymptotics for the analogous “diagonal terms” that arise when counting the number of D_4 -quartics having bounded discriminants. Let $N_{\text{Disc}}(X)$ denote the number of isomorphism classes of D_4 -quartics L with $|\text{Disc}(L)| < X$. By [9, Corollary 1.4] (or following the proof of Theorem 4.3 with discriminant in place of conductor), we have

$$N_{\text{Disc}}(X) = \frac{X}{2\zeta(2)} \cdot \sum_{\substack{[K:\mathbb{Q}]=2 \\ |\text{Disc}(K)| < X}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{2^{-r_2(K)}}{|\text{Disc}(K)|^2} + o(X). \tag{26}$$

Applying the reasoning in the proof of Proposition 5.2, we find that combining (19) and (26) implies

$$N_{\text{Disc}}(X) = \frac{X}{2\zeta(2)} \cdot \sum_{\substack{[K:\mathbb{Q}]=2 \\ |\text{Disc}(K)| < X}} \left(\sum_{m=1}^{\infty} \frac{\mu(m)\chi_K(m)}{m^2} \right) \cdot \left(\sum_{n=1}^{\infty} \frac{\chi_K(n)}{n} \right) \cdot \frac{2^{-r_2(K)}}{|\text{Disc}(K)|^2} + o(X).$$

We replace the product of sums

$$\left(\sum_{m=1}^{\infty} \frac{\mu(m)\chi_K(m)}{m^2} \right) \cdot \left(\sum_{n=1}^{\infty} \frac{\chi_K(n)}{n} \right)$$

with simply the “diagonal” terms (i.e., the terms where mn is a square).

Theorem 5.4. *We have*

$$\begin{aligned} & \frac{1}{2\zeta(2)} \cdot \sum_{\substack{[K:\mathbb{Q}]=2 \\ |\text{Disc}(K)| < X}} \frac{2^{-r(K)}}{|\text{Disc}(K)|^2} \cdot \left(\sum_{\substack{0 < a, b < \infty \\ (\text{Disc}(K), ab) = 1}} \frac{\mu(a)}{a^3 b^2} \right) \cdot X \\ & \sim \frac{3 \cdot 11^2}{2^6 \cdot 17} \cdot \prod_p \left(1 + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^4} \right) \cdot X. \end{aligned} \tag{27}$$

Proof. This follows from an argument analogous to the proof of Theorem 2. □

The right hand side of (27) agrees exactly with the heuristic in (11)! The non-diagonal terms, as in §5.2, again give an error term of $O(X)$. In the case when D_4 -quartics were ordered by conductor, this error term was negligible compared to the main term of order $X \log X$. This time, however, the main term of $\asymp X$ does not automatically dominate the error term. In fact, the comparison of the constant $c \approx 0.0523$ from [9] and the constant ≈ 0.406 on the right hand side of (27) implies that the non-diagonal terms do make a non-negligible contribution.

6. Parametrizing D_4 -quartics via pairs of ternary quadratic forms

We next give a proof using geometry-of-numbers techniques in conjunction with arithmetic invariant theory methods for determining asymptotics of the number of D_4 -quartics with $|q| < X$ and $|d| \ll X$. We obtain worse error estimates in this second proof, but we are able to prove more refined statements for a wider class of collections of local specifications. We begin with a parametrization of D_4 -quartics via certain pairs of ternary quadratic forms, following Bhargava [1] and Wood [30]. In §6.1, we describe the arithmetic invariant theory for orbits of such pairs of ternary quadratic forms and compare it to the invariants defined in Definitions 2.7 and 2.5 for the corresponding D_4 -quartics. We additionally define splitting types, and we compute the p -adic densities for pairs of ternary quadratic forms corresponding to D_4 -quartics with fixed splitting type at p . These results allow us to employ geometry-of-numbers methods carried out in Section 7 to count the relevant orbits parametrizing D_4 -quartics with $|q| < X$ and $|d| \ll X$.

In [1], Bhargava proved that isomorphism classes of pairs (Q, C) , where Q is a quartic ring and C is a cubic resolvent ring of Q are in bijection with $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ -orbits on $\mathbb{Z}^2 \otimes \text{Sym}^2(\mathbb{Z}^3)$, the space of pairs of integral ternary quadratic forms. If Q is a maximal quartic ring, then it has a unique cubic resolvent ring, so this bijection (when restricted to maximal rings) can be viewed as a parametrization of quartic fields. We write a pair of ternary quadratic forms as a pair (A, B) of symmetric 3×3 matrices whose diagonal entries are integers and non-diagonal entries are half-integers. The group $GL_2 \times SL_3$ acts on pairs of ternary quadratic forms as follows:

$$(g_2, g_3) \cdot (A, B) = (g_3 A g_3^t, g_3 B g_3^t) \cdot g_2^t.$$

For quartic rings Q containing a quadratic subring, Wood [30] gives a more specialized bijection: For any ring R , let $V'(R) \subset R^2 \otimes \text{Sym}^2(R^3)$ denote the space of pairs (A, B) of ternary quadratic forms satisfying

$$(A, B) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & a_{22} & a_{23}/2 \\ 0 & a_{23}/2 & a_{33} \end{bmatrix}, \begin{bmatrix} b_{11} & b_{12}/2 & b_{13}/2 \\ b_{12}/2 & b_{22} & b_{23}/2 \\ b_{13}/2 & b_{23}/2 & b_{33} \end{bmatrix} \right),$$

where $a_{22}, a_{23}, a_{33}, b_{11}, b_{12}, b_{22}, b_{23}$, and b_{33} are elements of R with $b_{11} \neq 0$. The subgroup $G'(R)$ of $GL_2(R) \times SL_3(R)$ consisting of elements (g_2, g_3) such that

$$g_2 = \begin{bmatrix} \pm 1 & 0 \\ * & \pm 1 \end{bmatrix} \quad \text{and} \quad g_3 = \begin{bmatrix} \pm 1 & 0 & 0 \\ * & * & * \\ * & * & * \end{bmatrix}$$

acts on $V'(R)$. Then the $G'(\mathbb{Z})$ -orbits on $V'(\mathbb{Z})$ are in bijection with triples (Q, C, T) consisting of a quartic ring Q , a cubic resolvent C of Q , and a quadratic subring $T \subset Q$. More precisely:

Theorem 6.1 ([30, Thm. 7.3.5]). *For any principal ideal domain R of characteristic different from 2, there is a bijection between $G'(R)$ -equivalence classes of elements of $V'(R)$ with isomorphism classes of triples (Q, C, T) where*

- Q is a quartic ring over R ,
- C is a cubic resolvent of Q with map $\varphi : Q \rightarrow C$, and
- $T \subset Q$ is a primitive quadratic subalgebra such that $\varphi(T) \neq 0$.

In order to obtain a parametrization of maximal orders in D_4 -quartics, we first make a few definitions.

Definition 6.2. An element of $v \in V'(\mathbb{Z})$ is *generic* if the quartic ring corresponding to v under Theorem 6.1 is a D_4 -quartic order, i.e., an order in a D_4 -quartic. Additionally, an element $V'(\mathbb{Z})$ is said to be *maximal* if it corresponds to a maximal quartic ring. A collection of elements of $V'(\mathbb{Z})$ is said to be maximal or generic if each element is the same.

Let (A, B) be an element of $V'(\mathbb{Z})$ and let Q be the quartic ring corresponding to it. It follows from [1, Lemma 22] that Q is non-maximal at every prime dividing b_{11} . Hence Q is maximal only when $b_{11} = \pm 1$. Furthermore, by replacing (A, B) with $(-\text{Id}, \text{Id}) \cdot (A, B) = (-A, -B)$ if necessary, we may assume that $b_{11} = 1$. We define $V(\mathbb{Z}) \subset V'(\mathbb{Z})$ to be the subspace of pairs

$$(A, B) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & a_{22} & a_{23}/2 \\ 0 & a_{23}/2 & a_{33} \end{bmatrix}, \begin{bmatrix} 1 & b_{12}/2 & b_{13}/2 \\ b_{12}/2 & b_{22} & b_{23}/2 \\ b_{13}/2 & b_{23}/2 & b_{33} \end{bmatrix} \right), \tag{28}$$

and we define the subgroup $G(\mathbb{Z}) \subset G'(\mathbb{Z})$ to be the set of pairs $(g_2, g_3) \in G'(\mathbb{Z})$ such that

$$g_2 = \begin{bmatrix} \pm 1 & 0 \\ * & 1 \end{bmatrix} \quad \text{and} \quad g_3 = \begin{bmatrix} \pm 1 & 0 & 0 \\ * & * & * \\ * & * & * \end{bmatrix}.$$

Moreover, for any ring R , we analogously define the space $V(R)$ and the group $G(R)$. We have the following proposition:

Proposition 6.3. *There is a bijection between (isomorphism classes of) D_4 -quartics and maximal generic $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$.*

Proof. Recall that every D_4 -quartic field L has a unique maximal order and that a maximal order has a unique cubic resolvent ring as well as a unique primitive quadratic subalgebra. Thus, there is exactly one $G'(\mathbb{Z})$ -orbit in $V'(\mathbb{Z})$ corresponding to L by Theorem 6.1. The above discussion shows that each generic, maximal $G'(\mathbb{Z})$ -orbit in $V'(\mathbb{Z})$ contains an element of $V(\mathbb{Z})$. Moreover, if $(A', B') = (g_2, g_3) \cdot (A, B)$ for some $(A, B) \in V(\mathbb{Z})$ and $(g_2, g_3) \in G'(\mathbb{Z})$ then $B'_{11} = g_{2,22} = 1$ and thus $(g_2, g_3) \in G(\mathbb{Z})$. Since we only make a claim about maximal orders, this completes the proof. \square

6.1. Invariant theory

We next discuss the invariant theory for the action of G on V . The action of $G(\mathbb{C}) \cap \text{SL}_3(\mathbb{C})$ on $V(\mathbb{C})$ turns out to have ring of invariants freely generated by three elements.

We can describe these invariants in terms of the *cubic resolvent* of (A, B) , i.e., the binary cubic form $\det(Ax + By)$. It is straightforward to check that if (A, B) is as in (28), then the coefficient of x^3 in $\det(Ax + By)$ is zero. For a ring R , let $U(R)$ denote the subspace of the space of binary cubic forms consisting of elements

$$f(x, y) = bx^2y + cxy^2 + dy^3,$$

where $b, c, d \in R$. Define N_1 to be the group of lower triangular 2×2 matrices with top left entry ± 1 and bottom right entry 1. Then N_1 acts on U via

$$g \cdot f(x, y) = f((x, y) \cdot g^t).$$

Additionally, if $\pi : V(R) \rightarrow U(R)$ denotes the resolvent map $(A, B) \mapsto 4\det(Ax + By)$, then for $(g_2, g_3) \in G(R)$,

$$\pi((g_2, g_3) \cdot (A, B)) = g_2 \cdot \pi(A, B).$$

The coefficients b, c , and d of the binary cubic form $\pi(A, B)$ are the invariants for the action of $G(\mathbb{C}) \cap \text{SL}_3(\mathbb{C})$ on $V(\mathbb{C})$. Therefore, the ring of invariants for the action of all of $G(\mathbb{C})$ on $V(\mathbb{C})$ is the same as the ring of invariants for the action of $N_1(\mathbb{C})$ on $U(\mathbb{C})$. The latter ring is freely generated by two elements d and q , which can be associated to an element of V as follows:

Definition 6.4. If $(A, B) \in V(R)$ has resolvent $f(x, y) = bx^2y + cxy^2 + dy^3$, then

$$d(A, B) := d(f) := -b, \quad q(A, B) := q(f) := c^2 - 4bd.$$

Additionally, we set

$$C(A, B) := d(A, B) \cdot q(A, B) \quad \text{and} \quad \text{Disc}(A, B) := d(A, B)^2 \cdot q(A, B).$$

We now relate the invariants d and q of an element $(A, B) \in V(\mathbb{Z})$ to the invariants of the quartic ring corresponding to the $G(\mathbb{Z})$ -orbit of (A, B) in Theorem 6.1.

Proposition 6.5. *Let $(A, B) \in V(\mathbb{Z})$ with non-zero invariants $d(A, B)$ and $q(A, B)$. Let Q denote the quartic ring corresponding to (A, B) and let T be its quadratic subalgebra. Then $\text{Disc}(T) = d(A, B)$ and $\text{Nm}_T(\text{Disc}(Q/T)) = |q(A, B)|$.*

Proof. Let (A, B) be as in (28) with resolvent $f(x, y) = bx^2y + cxy^2 + dy^3$, and assume that $d(A, B)$ and $q(A, B)$ are non-zero. As described in [1, Section 3], one can describe the multiplicative structure on a (normal) \mathbb{Z} -basis of Q using the matrix coefficients of (A, B) . Indeed, if $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$ is a \mathbb{Z} -basis for Q , we can write its multiplication table as

$$\alpha_i \alpha_j = c_{ij}^0 + c_{ij}^1 \alpha_1 + c_{ij}^2 \alpha_2 + c_{ij}^3 \alpha_3,$$

where $c_{ij}^k \in \mathbb{Z}$ for $1 \leq i, j \leq 3$ and $k \in \{0, 1, 2, 3\}$ are completely determined by a_{ij} and b_{ij} . Equations (20)–(22) of [1] with $a_{11} = a_{12} = a_{13} = 0$ and $b_{11} = 1$ imply that $c_{11}^2 = c_{11}^3 = 0$. Additionally, we obtain $c_{11}^0 = -a_{33}a_{22}$ and $c_{11}^1 = a_{23}$, i.e.,

$$\alpha_1^2 = -a_{33}a_{22} + a_{23}\alpha_1,$$

and so $\mathbb{Z}[\alpha_1] = \langle 1, \alpha_1 \rangle$ is a quadratic subalgebra of Q . By the description of T given in [30, proof of Corollary 7.2.2], we have $T = \mathbb{Z}[\alpha_1]$, and

$$\text{Disc}(T) = \text{Disc}(\alpha_1) = a_{23}^2 - 4a_{33}a_{22}.$$

Using the resolvent map $\pi(A, B) = 4 \det(Ax + By) = bx^2y + cxy^2 + dy^3$, we deduce that

$$b = 4a_{22}a_{33} - a_{23}^2.$$

Thus, $\text{Disc}(T) = d(A, B)$, as desired.

Furthermore, by [1, Proposition 10] and since $\text{Disc}(A, B) = \text{Disc}(\pi(A, B))$, we have

$$\text{Disc}(Q) = \text{Disc}(A, B) = \text{Disc}(bx^2y + cxy^2 + dy^3) = b^2c^2 - 4b^3d.$$

The relative discriminant formula implies that $|\text{Disc}(Q)| = |\text{Disc}(T)^2 \cdot \text{Nm}_T(\text{Disc}(Q/T))|$, and so we conclude that

$$\text{Nm}_T(\text{Disc}(Q/T)) = \left| \frac{\text{Disc}(Q)}{\text{Disc}(T)^2} \right| = |c^2 - 4bd|.$$

The proposition follows. □

We slightly generalize the notion of conductor given in the introduction for étale quartic algebras over R . For a pair (Q, T) , where Q is a étale quartic algebra over R and T is a primitive quadratic subalgebra of Q , we set $C(Q, T) := \text{Disc}(Q)/\text{Disc}(T)$. The following lemma will be useful in obtaining a bound on the number of $G(\mathbb{Z})$ -orbits that correspond to non-maximal D_4 -quartic orders in Section 8.

Lemma 6.6. *Let p be an odd prime. If $(A, B) \in V(\mathbb{Z}_p)$ corresponds to a non-maximal quartic order Q contained in a degree-4 étale extension L_p of \mathbb{Q}_p and a quartic subalgebra T contained in a quadratic subextension K_p of L_p , then*

$$p^2 \mid \frac{C(A, B)}{C(L_p, K_p)}.$$

Proof. Since the index of Q in the maximal order of L is a multiple of p , it follows that the discriminant of (A, B) differs from the discriminant of L by a factor of at least p^2 . Since $C(A, B) = \text{Disc}(A, B)/\text{Disc}(T)$ and $C(L_p, K_p) = \text{Disc}(L_p)/\text{Disc}(K_p)$, the lemma follows unless $\text{Disc}(T)/\text{Disc}(K_p)$ is divisible by p , or equivalently, unless T is not maximal in the ring of integers of K_p .

Assume that T is not maximal in the ring of integers of K_p , and thus has discriminant divisible by p^2 . We know from Proposition 6.5 that $-\text{Disc}(T)$ is the discriminant of the quadratic form $a_{22}y^2 + a_{23}yz + a_{33}z^2$ corresponding to A . Hence, either A is a multiple of p or, after a change of variables, we may assume that $p^2 \mid a_{22}$ and $p \mid a_{23}$. In the first case, the pair of rings (Q_1, T_1) corresponding to $(A/p, B) \in V(\mathbb{Z})$ are over-orders of Q and T such that $p^4 \mid C(Q, T)/C(Q_1, T_1)$. In the second case, the argument is similar: we use the pair (A_2, B_2) obtained by multiplying the third row and column of A and B by p , and dividing A by p^2 , which yield a pair (Q_2, T_2) of over-orders of (Q, T) such that $p^2 \mid C(Q, T)/C(Q_1, T_1)$. The lemma follows. □

6.2. *Splitting types of pairs of ternary quadratic forms*

Let p be a fixed prime. We say that a pair $(A, B) \in V(\mathbb{F}_p)$ is *non-degenerate* if the zero sets in $\mathbb{P}^2(\mathbb{F}_p)$ of the two ternary quadratic forms corresponding to A and B intersect at four points counted with multiplicity. For non-degenerate elements $(A, B) \in V(\mathbb{F}_p)$ such that A is non-zero, we define the *quartic splitting type* at p to be

$$\zeta_p(A, B) = (f_1^{e_1} f_2^{e_2} \dots),$$

where the f_i 's are the degrees over \mathbb{F}_p of the field of definition of these points, and the e_i 's are their multiplicities. Furthermore, recall that the top row and column of A is 0, and so in the notation of (28), A corresponds to a quadratic form $g(y, z) = a_{22}y^2 + a_{23}yz + a_{33}z^2$. We define the *quadratic splitting type* $\zeta'_p(A, B)$ of (A, B) to be (11) if $g(x, y)$ has two distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$, to be (2) if $g(x, y)$ has a pair of conjugate roots defined over a quadratic extension of \mathbb{F}_p , and (1²) if $g(x, y)$ has a double root. We then say that the pair $(\zeta_p(A, B), \zeta'_p(A, B))$ is the *splitting type* of (A, B) at p .

If (A, B) is an element in $V(\mathbb{Z})$ or $V(\mathbb{Z}_p)$, we define the splitting type of (A, B) at p to be the splitting type of the reduction modulo p of (A, B) , assuming it is non-degenerate. Let Q be the quartic ring corresponding to (A, B) , and let T denote the quadratic subring of Q arising from Theorem 6.1. It follows from [1, §4.1] that the quartic splitting type of (A, B) is equal to the splitting type of Q . We have seen that the quadratic subring T of Q corresponding to the pair (A, B) is the quadratic ring whose discriminant is the same as that of the binary quadratic form corresponding to A . Hence, the quadratic splitting type of (A, B) is the same as the splitting type of T .

Given a pair (L_p, K_p) of extensions of \mathbb{Q}_p , whose rings of integers correspond to a pair $(A, B) \in V(\mathbb{Z}_p)$, we define $\zeta_p(L_p, K_p)$ to equal the splitting type of (A, B) . Additionally, there are four possible splitting types $\zeta = (\zeta_\infty, \zeta'_\infty)$ at ∞ for an element in $V(\mathbb{R})$ having non-zero discriminant. The invariants (d, q) of an element $v \in V(\mathbb{R})^{(\zeta)}$ are constrained in the following way:

$$\begin{aligned} \zeta = ((1111), (11)) &\implies q > 0, d > 0; \\ \zeta = ((112), (11)) &\implies q < 0, d > 0; \\ \zeta = ((22), (11)) &\implies q > 0, d > 0; \\ \zeta = ((22), (2)) &\implies q > 0, d < 0. \end{aligned}$$

We denote the set of elements in $V(\mathbb{R})$ having splitting type ζ by $V(\mathbb{R})^{(\zeta)}$ and set $V(\mathbb{Z})^{(\zeta)} = V(\mathbb{Z}) \cap V(\mathbb{R})^{(\zeta)}$.

6.3. *The density of maximal elements*

For a prime p and splitting type (ζ_p, ζ'_p) , let $T_p(\zeta_p, \zeta'_p)$ denote the set of elements $(A, B) \in V(\mathbb{Z}_p)$ whose splitting type at p is (ζ_p, ζ'_p) and let $M_p(\zeta_p, \zeta'_p)$ denote the set of elements $(A, B) \in T_p(\zeta_p, \zeta'_p)$ that correspond to quartic rings under Theorem 6.1 that are maximal at p . Identifying $V(\mathbb{Z}_p) \cong \mathbb{Z}_p^8$ by regarding the non-fixed entries of (28) as a vector, let μ denote the Haar measure normalized so that $V(\mathbb{Z}_p)$ has volume 1. We have the following result which gives the volumes of the sets $M_p(\zeta_p, \zeta'_p)$.

Proposition 6.7. *We have*

$$\begin{aligned} \mu(M_p((1111), (11))) &= \frac{1}{8}(p - 1)^3(p + 1)/p^4, \\ \mu(M_p((22), (11))) &= \frac{1}{8}(p - 1)^3(p + 1)/p^4, \\ \mu(M_p((22), (2))) &= \frac{1}{4}(p - 1)^3(p + 1)/p^4, \\ \mu(M_p((112), (11))) &= \frac{1}{4}(p - 1)^3(p + 1)/p^4, \\ \mu(M_p((4), (2))) &= \frac{1}{4}(p - 1)^3(p + 1)/p^4, \\ \mu(M_p((1^211), (11))) &= \frac{1}{2}(p - 1)^3(p + 1)/p^5, \\ \mu(M_p((1^22), (11))) &= \frac{1}{2}(p - 1)^3(p + 1)/p^5, \\ \mu(M_p((1^21^2), (1^2))) &= \frac{1}{2}(p - 1)^3(p + 1)/p^5, \\ \mu(M_p((2^2), (1^2))) &= \frac{1}{2}(p - 1)^3(p + 1)/p^5, \\ \mu(M_p((1^4), (1^2))) &= (p - 1)^3(p + 1)/p^6, \\ \mu(M_p((1^21^2), (11))) &= \frac{1}{2}(p - 1)^3(p + 1)/p^6, \\ \mu(M_p((2^2), (2))) &= \frac{1}{2}(p - 1)^3(p + 1)/p^6. \end{aligned}$$

Proof. First note that the splitting type of $v \in V(\mathbb{Z}_p)$ depends only on the reduction of v modulo p . It follows that the densities of the sets $T_p(\zeta_p, \zeta'_p)$ can be computed by counting elements in $V(\mathbb{F}_p)$. The conditions that ensure the maximality of v are listed in [1, §4.2]. We prove Proposition 6.7 by computing the densities of $T_p(\zeta_p, \zeta'_p)$ and then, for each ζ_p , determining the probability that $v \in T_p(\zeta_p, \zeta'_p)$ is maximal.

Let (A, B) be an element of $V(\mathbb{Z}_p)$ having quadratic splitting type (11). It follows that the quadratic form corresponding to A has two distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$. The number of possibilities for \bar{A} , the reduction of A modulo p , is thus equal to $(p + 1)p(p - 1)/2$ giving a density of $(p + 1)p(p - 1)/(2p^3)$ for the possibilities of A . By a change of variables, we may assume that (A, B) is of the form

$$(\bar{A}, \bar{B}) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & t \end{bmatrix} \right) \tag{29}$$

when p is odd, and

$$(\bar{A}, \bar{B}) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & \alpha/2 & \beta/2 \\ \alpha/2 & s & 0 \\ \beta/2 & 0 & t \end{bmatrix} \right) \tag{30}$$

when $p = 2$. The quartic splitting type of (A, B) then has six options: (1111), (112), (22), (1^211) , (1^22) , and (1^21^2) . When p is odd, this splitting type depends on whether s and t are residues modulo p , non-residues modulo p , or 0. Their relative densities can be computed directly. To obtain the splitting type (1111), both s and t must be residues modulo p which occurs with relative density $(p - 1)^2/(4p^2)$. It is a straightforward computation to check that for $p = 2$, the relative density of elements with quartic splitting

type (1111) is again $1/16 = (p - 1)^2/(4p^2)$. Multiplying with the density $(p^2 - 1)/(2p^2)$ of split quadratic forms arising from A yields the density of $T_p((1111), (11))$. Since every element with unramified splitting type is automatically maximal, it follows that $T_p((1111), (11)) = M_p((1111), (11))$, yielding the first part of the proposition.

We now compute the density of $M_p((1^2 1^2), (11))$. Again, we may assume that (\bar{A}, \bar{B}) is of the form (29) when p is odd and of the form (30) when $p = 2$. When p is odd, such a pair (A, B) has quartic splitting type $(1^2 1^2)$ when $s = t = 0$, and when $p = 2$ such a form has splitting type $(1^2 1^2)$ when $\alpha = \beta = 0$. The relative density of such (A, B) is $1/p^2$, and we therefore see that the density of $T_p((1^2 1^2), (11))$ is $\frac{1}{2}(p - 1)(p + 1)/p^4$. We now compute the probability that an element $(A, B) \in T_p((1^2 1^2), (11))$ is maximal at p . Let (A, B) in $T_p((1^2 1^2), (11))$ be fixed. By a change of variables, we may assume (for both p odd and $p = 2$) that the reduction of (A, B) modulo p is equal to

$$(\bar{A}, \bar{B}) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right). \tag{31}$$

From [1, Lemma 23], it follows that (A, B) is maximal if and only if neither b_{22} nor b_{23} is divisible by p^2 . Hence the relative density of $M_p((1^2 1^2), (11))$ in $T_p((1^2 1^2), (11))$ is $(1 - 1/p)^2$. In conjunction with the previously computed density of $T_p((1^2 1^2), (11))$, it follows that the density of $M_p((1^2 1^2), (11))$ is as stated in the proposition. The computations of the densities of the $M_p(\varsigma_p, \varsigma'_p)$ for other splitting types $(\varsigma_p, \varsigma'_p)$ are very similar to the above two computations and so we omit them. \square

Proposition 6.7 gives the p -adic splitting densities in V . However, it is possible to extract densities that are more refined. From the splitting types with central inertia in Table 1, it is evident that the splitting type of a D_4 -quartic L at a prime p is not enough to determine the decomposition groups of L at p . However, if $v \in V(\mathbb{Z})$ corresponds to \mathcal{O}_L , then the $G(\mathbb{Z}_p)$ -orbit of v in $V(\mathbb{Z}_p)$ determines $\mathcal{O}_L \otimes \mathbb{Z}_p$, and hence determines the decomposition groups of L at p . In the following lemma, we compute some of these more refined densities.

If p is an odd prime with splitting type $((1^2 1^2), (11))$ (resp. $((2^2), (2))$) in a D_4 -quartic L with quadratic subfield K , then there are two possibilities for the splitting type $(\varsigma_p(\phi(L)), \varsigma_p(\phi(K)))$ of $\phi(L)$ at p (see Definition 2.1), namely $((1111), (11))$ (resp. $((22), (11))$) or $((22), (2))$. Let $M_p^{(11)}(\varsigma_p, \varsigma'_p)$ (resp. $M_p^{(2)}(\varsigma_p, \varsigma'_p)$) denote the subset of elements $(A, B) \in M_p(\varsigma_p, \varsigma'_p)$ corresponding to (Q, T) under Theorem 6.1 such that $\phi(\text{Frac}(T))$ has splitting type (11) (resp. (2)) at p .

Lemma 6.8. *Let p be an odd prime and let $(\varsigma_p, \varsigma'_p)$ be one of $((1^2 1^2), (11))$ or $((2^2), (2))$. Then with the notation of the previous paragraph,*

$$\mu(M_p^{(2)}(\varsigma_p, \varsigma'_p)) = \mu(M_p^{(11)}(\varsigma_p, \varsigma'_p)).$$

Proof. We prove the lemma only for the splitting type $((1^2 1^2), (11))$, since the proof is very similar for $((2^2), (2))$. Let $(A, B) \in V(\mathbb{Z}_p)$ be a maximal element, corresponding to a degree-4 étale \mathbb{Z}_p -algebra Q and a quadratic subalgebra T , and let L (respectively, K)

denote the fraction field of Q (respectively, T). Assume that the splitting type of (A, B) is $((1^2 1^2), (11))$, and let $f(x, y) = 4 \det(Ax + By)$ denote the cubic resolvent polynomial of (A, B) . Then the x^3 -coefficient of f is 0, and dividing f by y yields a binary quadratic form. A direct computation, in conjunction with Propositions 2.6 and 6.5, implies that

$$\text{Disc}_p(f(x, y)/y)/p^2 = \text{Disc}_p(\phi(K)), \tag{32}$$

where Disc_p means the p -part of the discriminant, and hence sign issues do not arise. Since the two possible decomposition groups for the splitting type $((1^2 1^2), (11))$ are determined by the splitting behavior of p at $\phi(K)$ (see Table 1), it follows that the relative densities of these decomposition groups can be found by computing the relative densities of the different possible splitting behaviors of p in the quadratic order whose discriminant is $\text{Disc}_p(f(x, y)/y)/p^2$.

Since p is odd, from the discussion surrounding (31), it follows that we may assume (A, B) satisfies

$$\begin{aligned} a_{11} = a_{12} = a_{13} = b_{12} = b_{13} = 0, \quad b_{11} = 1, \quad a_{23} \equiv 1 \pmod{p}, \\ a_{22} \equiv b_{22} \equiv b_{23} \equiv b_{33} \equiv 0 \pmod{p}. \end{aligned}$$

Consider the pair (A, B_1) , where the B_1 is obtained from B by dividing the b_{22}, b_{23} , and b_{33} by p . Let f_1 denote the cubic resolvent form of (A, B_1) . By a direct computation and applying (32), the discriminant of $f_1(x, y)/y$ is exactly the same as the discriminant of $\phi(K)$. Hence the decomposition group of L is determined by the splitting of p in $f_1(x, y)/y$. Since (A, B) was assumed to be maximal, it follows that p does not divide the discriminant of $f_1(x, y)/y$, because, by Table 1, for the splitting types under consideration, $\phi(K)$ is unramified at p . It is a direct computation to check that the density of elements (A, B_1) such that $f_1(x, y)/y$ has splitting type (11) (resp. (2)) is exactly $1/2$, yielding the lemma. □

Let \mathcal{M}_p denote the set of elements $(A, B) \in V(\mathbb{Z}_p)$ that are maximal at p , and let \mathcal{U}_p denote the set of elements (A, B) in \mathcal{M}_p that do not have central inertia, i.e., the splitting type of any $(A, B) \in \mathcal{U}_p$ at p is not equal to $((1^4), (1^2)), ((1^2 1^2), (11))$, or $((2^2), (2))$. Summing the values obtained in Proposition 6.7 we can compute the density of \mathcal{M}_p . To determine the density of \mathcal{U}_p , we add up the values of the first nine rows.

Theorem 6.9. *We have*

$$\begin{aligned} \mu(\mathcal{M}_p) &= \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right), \\ \mu(\mathcal{U}_p) &= \left(1 - \frac{1}{p^2}\right) \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p}\right). \end{aligned}$$

7. Counting D_4 -quartics using geometry-of-numbers methods

In the previous section, we defined an injective map from D_4 -quartics to $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$ and determined generators d and q for the ring of invariants for the action of G on V . In this section, our goal is to count generic $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$ having bounded invariants.

Recall that an element $v \in V(\mathbb{Z})$ is said to be generic if v corresponds to an order in a D_4 -quartic, and the subset of elements in $V(\mathbb{Z})$ with infinite splitting type ζ is denoted by $V(\mathbb{Z})^{(\zeta)}$. For any $G(\mathbb{Z})$ -invariant set $\mathcal{L} \subset V(\mathbb{Z})$ and for any $\delta > 0$, let $\mathcal{N}_q^{(\delta)}(\mathcal{L}; X, Y)$ denote the number of generic $G(\mathbb{Z})$ -orbits v on \mathcal{L} such that $X < |q(v)| \leq (1 + \delta)X$ and $Y < |d(v)| \leq (1 + \delta)Y$. Our goal in this section is to prove the following theorem:

Theorem 7.1. *Let X and Y be positive real numbers going to infinity such that $Y(\log Y)^2 = o(X)$. Then*

$$\mathcal{N}_q^{(\delta)}(V(\mathbb{Z})^{(\zeta)}; X, Y) = \frac{\zeta(2)}{2\tau_\zeta} \delta^2 XY + o_\delta(XY),$$

where $\tau_\zeta = 8$ when $\zeta = ((1111), (11))$ or $\zeta = ((22), (11))$ and $\tau_\zeta = 4$ otherwise.

To do so, we study the fundamental domain for the action of the non-reductive group $G(\mathbb{Z})$ on $V(\mathbb{R})$. We then compute the volume of a cover of this fundamental set after cutting off the cusps in terms of an Euler product of local densities.

7.1. Construction of fundamental domains

In this section, our goal is to construct a finite cover for a fundamental domain for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})$. As a first step, we describe the $G(\mathbb{R})$ -orbits on $V(\mathbb{R})$, and the sizes of the stabilizers in $G(\mathbb{R})$ of elements in each orbit. Before we do so, it will be convenient to introduce the following group and space: For any ring R , let $V_{\text{red}}(R) \subset V(R)$ consist of all pairs (A, B) of the form

$$(A, B) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & a_{22} & a_{23}/2 \\ 0 & a_{23}/2 & a_{33} \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & b_{22} & b_{23}/2 \\ 0 & b_{23}/2 & b_{33} \end{bmatrix} \right). \tag{33}$$

The subgroup $G_{\text{red}}(R)$ of $G(R)$ acts on $V_{\text{red}}(R)$, where $G_{\text{red}}(R)$ consists of elements $(g_2, g_3) \in \text{GL}_2(R) \times \text{SL}_3(R)$ such that

$$g_2 = \begin{bmatrix} \pm 1 & 0 \\ * & 1 \end{bmatrix} \quad \text{and} \quad g_3 = \begin{bmatrix} \pm 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{bmatrix}. \tag{34}$$

Proposition 7.2. *The orbits for the action of $G(\mathbb{R})$ on the set of elements in $V(\mathbb{R})$ having non-zero invariants q and d correspond to a pair (L_∞, K_∞) of étale algebras with splitting types and invariants as follows:*

- (1) *When $q > 0$ and $d > 0$, there are two orbits, one with splitting type $((1111), (11))$ and one with splitting type $((22), (11))$.*
- (2) *When $q < 0$ and $d > 0$, there is one orbit with splitting type $((112), (11))$.*
- (3) *When $q > 0$ and $d < 0$, there is one orbit with splitting type $((22), (2))$.*

The respective sizes of the stabilizers in $G(\mathbb{R})$ of elements in these orbits are 8 in the first case, and 4 in the second and third cases, and we denote these stabilizer quantities by $\tau_\zeta(L_\infty, K_\infty)$.

Proof. We start with a few observations. First note that $G(\mathbb{R})$ -orbits on $V(\mathbb{R})$ having fixed invariants d and q are in bijection with $G_{\text{red}}(\mathbb{R})$ -orbits on $V_{\text{red}}(\mathbb{R})$ having invariants q and d . This is because $(A, B) \in V(\mathbb{R})$ is $G(\mathbb{R})$ -equivalent to some $(A_{\text{red}}, B_{\text{red}}) \in V_{\text{red}}(\mathbb{R})$. Furthermore, if two elements in $V_{\text{red}}(\mathbb{R})$ are $G(\mathbb{R})$ -equivalent via some $g \in G(\mathbb{R})$, then g must in fact belong to $G_{\text{red}}(\mathbb{R})$. This latter fact also implies that the stabilizer in $G(\mathbb{R})$ of any element in $V_{\text{red}}(\mathbb{R})$ is contained in $G_{\text{red}}(\mathbb{R})$. Also note that $G_{\text{red}}(\mathbb{R})$ -orbits on $V_{\text{red}}(\mathbb{R})$ having non-zero invariants d and q are in bijection with $G_{\text{red}}(\mathbb{R})$ -orbits on $V_{\text{red}}(\mathbb{R})$ having invariants $q/|q|$ and $d/|d|$. Indeed, if $(A, B) \in V_{\text{red}}(\mathbb{R})$ has invariants q and d , then dividing A by $\sqrt{|d|}$ and dividing the lower 2×2 submatrix of B by $\sqrt{|q|/|d|}$ yields the necessary bijection. Moreover, a direct computation shows that the stabilizers in $G_{\text{red}}(\mathbb{R})$ of these two elements are the same. Therefore, it suffices to prove the proposition in the case when q and d are ± 1 .

Consider the case $q = d = 1$. Let $(A, B) \in V_{\text{red}}(\mathbb{R})$ have such invariants. By replacing (A, B) with a $G_{\text{red}}(\mathbb{R})$ -translate, we transform it as follows: first, we ensure that $a_{22} = a_{33} = 0$; next, we subtract an appropriate multiple of A from B to ensure that its off-diagonal entries are 0; finally, we use an element of $SL_2(\mathbb{R}) \subset G_{\text{red}}(\mathbb{R})$ to ensure that $|b_{22}| = |b_{33}|$. From the fact that $q = d = 1$, it follows that we have transformed (A, B) into the form

$$\left(\begin{bmatrix} 0 & & \\ & \frac{1}{2} & \\ & & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 1 & & \\ & \frac{\pm 1}{4} & \\ & & \frac{\pm 1}{4} \end{bmatrix} \right),$$

where b_{22} and b_{33} are either both positive or both negative. It is a direct computation to check that (A, B) has splitting type $((22), (11))$ in the former case and $((1111), (11))$ in the latter case. Furthermore, the stabilizer in $G_{\text{red}}(\mathbb{R})$ of (A, B) in either case is seen to consist of the following eight elements:

$$\begin{aligned} & \left(\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \right), \quad \left(\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix} \right), \quad \left(\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} -1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \right), \\ & \left(\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & -1 & \\ & & 1 \end{bmatrix} \right), \quad \left(\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix} \right), \quad \left(\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} -1 & & \\ & -1 & \\ & & 1 \end{bmatrix} \right), \\ & \left(\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} -1 & & \\ & -1 & \\ & & -1 \end{bmatrix} \right), \quad \left(\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & 1 & \\ & & -1 \end{bmatrix} \right). \end{aligned}$$

This concludes the proof of the first item in Proposition 7.2. We omit the proofs of the other two items since they are very similar. □

Recall that the set of elements in $V(\mathbb{R})$ with infinite splitting type ζ is denoted by $V(\mathbb{R})^{(\zeta)}$. Given a splitting type ζ , let $(A_\zeta, B_\zeta) \in V(\mathbb{R})^{(\zeta)} \cap V_{\text{red}}(\mathbb{R})$ be an element whose invariants have absolute value 1. By multiplying A_ζ by $\sqrt{|d|}$ and multiplying the bottom 2×2 submatrix of B by $\sqrt{|q|/|d|}$, we obtain an element with invariants q and d , for any pair $(q, d) \in \mathbb{R}^2$ having appropriate signs. We thus obtain the following result which follows

immediately from Proposition 7.2. Note that the set of such pairs (A, B) is bounded (since q and d are) and semialgebraic (indeed, they are defined by linear conditions.)

Proposition 7.3. *Fix an infinite splitting type ζ . There exists a fundamental set $\mathcal{R}^{(\zeta)}$ for the action of $G(\mathbb{R})$ on $V(\mathbb{R})^{(\zeta)}$ such that $\mathcal{R}^{(\zeta)}$ contains one element (A, B) having invariants q and d for any $(q, d) \in \mathbb{R}^2$ having appropriate signs. Moreover, $\mathcal{R}^{(\zeta)}$ may be constructed so that the element $(A, B) \in \mathcal{R}^{(\zeta)}$ having invariants q and d is such that the coefficients of A are bounded by $O_\delta(|d|^{1/2})$ and the coefficients of B are bounded by $O_\delta(|q|^{1/2}|d|^{-1/2})$.*

Let \mathcal{F} be a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$. We may assume that \mathcal{F} is contained in the Siegel domain $\mathcal{S} = \mathcal{S}_1\mathcal{S}_2$, where

$$\begin{aligned} \mathcal{S}_1 &= \left\{ \left(\begin{bmatrix} 1 & \\ n & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ & m_3 \ 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & t^{-1} \ t \end{bmatrix} \begin{bmatrix} 1 & \cos \theta & \sin \theta \\ & -\sin \theta & \cos \theta \end{bmatrix} \right) : n, m_3 \in [0, 1), t > \frac{1}{2} \right\}, \\ \mathcal{S}_2 &= \left\{ \left(\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ m_1 & 1 \\ m_2 & & 1 \end{bmatrix} \right) : m_1, m_2 \in [0, 1) \right\}. \end{aligned} \tag{35}$$

We have $\mathcal{F} = \mathcal{F}_2\mathcal{F}_1$, where $\mathcal{F}_1 \subset \mathcal{S}_1$ and $\mathcal{F}_2 = \mathcal{S}_2$. From an argument identical to that in [5, §2.1], it follows that $\mathcal{F} \cdot \mathcal{R}^{(\zeta)}$ is a cover of a fundamental domain for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{(\zeta)}$, where the $G(\mathbb{Z})$ -orbit of v is represented $m(v)$ times. Here $m(v)$ is given by

$$m(v) = \# \text{Stab}_{G(\mathbb{R})}(v) / \# \text{Stab}_{G(\mathbb{Z})}(v).$$

Every element in $V(\mathbb{R})$ is fixed by the element $(\text{Id}, g_3) \in G(\mathbb{Z})$, where g_3 is the diagonal 3×3 matrix whose diagonal entries are $1, -1$, and -1 . Conversely, every non-trivial element $\gamma \in G(\mathbb{Z})$ not equal to $(\text{Id}, g_3) \in G(\mathbb{Z})$, acts non-trivially on $V(\mathbb{R})$. Hence the set of points in $V(\mathbb{R})$ fixed by γ has lower dimension and thus has measure 0. Since there are only countable many elements in $G(\mathbb{Z})$, it follows that the set of elements in $V(\mathbb{R})$ that have a stabilizer in $G(\mathbb{Z})$ of size greater than 2 has measure 0. We thus obtain the following theorem.

Theorem 7.4. *The multiset $\mathcal{F} \cdot \mathcal{R}^{(\zeta)}$ is a $\tau_\zeta/2$ -fold cover of a fundamental domain for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{(\zeta)}$, where $\tau_\zeta = 8$ for $\zeta = ((1111), (11))$ or $((22), (11))$ and $\tau_\zeta = 4$ for $\zeta = ((112), (11))$ or $((22), (2))$.*

7.2. Averaging and cutting off the cusp

Let $\mathcal{L} \subset V(\mathbb{R})^{(\zeta)}$ be a $G(\mathbb{Z})$ -invariant lattice, and denote the set of generic elements in \mathcal{L} by \mathcal{L}^{gen} . Given a subset W of $V(\mathbb{R})$ and a constant $\delta > 0$, we denote by $W_{X\delta}$ the set of

elements $w \in W$ with $X \leq |q(w)| < (1 + \delta)X$ and $Y \leq |d(w)| < (1 + \delta)Y$. Since the stabilizer in $G(\mathbb{Z})$ of a generic element in $V(\mathbb{Z})$ has size 2, Theorem 7.4 implies that

$$\mathcal{N}_q^{(\delta)}(\mathcal{L}; X, Y) = \frac{2}{\tau_\zeta} \#\{\mathcal{F} \cdot \mathcal{R}_{XY}^{(\zeta)} \cap \mathcal{L}^{\text{gen}}\}, \tag{36}$$

From Proposition 7.3, it follows that the coefficients a_{ij} and b_{ij} of any element $(A, B) \in \mathcal{R}_{XY}^{(\zeta)}$ satisfy the bounds

$$|a_{ij}| \ll Y^{1/2}, \quad |b_{ij}| \ll X^{1/2}/Y^{1/2}. \tag{37}$$

We now pick the following bounded open non-empty subset G_0 of $G_{\text{red}}(\mathbb{R})$:

$$G_0 := \left\{ \left(\begin{bmatrix} 1 & & & \\ & n & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & a & b & \\ & c & d & \end{bmatrix} \right) : n \in (0, \sqrt{X}/Y), \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_1 \subset \text{SL}_2(\mathbb{R}) \right\},$$

where G_1 is a bounded open non-empty $\text{SO}_2(\mathbb{R})$ -invariant subset of $\text{SL}_2(\mathbb{R})$. The reason for the choice of the range of n is that the coefficients of every element in $G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$ satisfy the bounds (37). Write the fundamental domain \mathcal{F} in (36) as $\mathcal{F}_2 \mathcal{F}_1 g$. Using coordinates from (35), we write an element in \mathcal{F}_1 as (n, m_3, t, θ) . In these coordinates,

$$dg = t^{-2} dndm_3 d^\times t d\theta$$

is a Haar measure on $G_{\text{red}}(\mathbb{R})$. The proof of the following lemma follows the argument in [5, proof of Theorem 2.5].

Lemma 7.5. *We have*

$$\mathcal{N}_q^{(\delta)}(\mathcal{L}; X, Y) = \frac{2}{\tau_\zeta \text{Vol}(G_0)} \int_{g \in \mathcal{F}_1} \#\{\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap \mathcal{L}^{\text{gen}}\} dg.$$

Proof. For every $g \in G_{\text{red}}(\mathbb{R})$, the set $g \cdot \mathcal{R}^{(\zeta)}$ is a fundamental set for the action of $G(\mathbb{R})$ on $V(\mathbb{R})^\zeta$. Therefore, averaging (36), with $\mathcal{R}^{(\zeta)}$ replaced with $g \cdot \mathcal{R}^{(\zeta)}$, over $g \in G_0$, we obtain

$$\mathcal{N}_q^{(\delta)}(\mathcal{L}; X, Y) = \frac{2}{\tau_\zeta \text{Vol}(G_0)} \int_{g \in G_0} \#\{\mathcal{F}_2 \mathcal{F}_1 g \cdot \mathcal{R}_{XY}^{(\zeta)} \cap \mathcal{L}^{\text{gen}}\} dg.$$

Pick $v \in \mathcal{L}^{\text{gen}}$, and let $v_0 \in \mathcal{R}^{(\zeta)}$ denote the unique element that is $G(\mathbb{R})$ -equivalent to v . Since $G_{\text{red}}(\mathbb{R}) \cdot \mathcal{R}^{(\zeta)}$ is contained in $V_{\text{red}}(\mathbb{R})$, and there exists at most one element in \mathcal{F}_2^{-1} , such that $\gamma_2 \cdot v \in V_{\text{red}}(\mathbb{R})$, it follows that the set S_v of elements $\gamma \in G_{\text{red}}(\mathbb{R})$ such that $\gamma \cdot v_0 \in \mathcal{F}_2^{-1} v$ is finite. Therefore,

$$\begin{aligned} \int_{g \in G_0} \#\{\mathcal{F}_2 \mathcal{F}_1 g \cdot \mathcal{R}_{XY}^{(\zeta)} \cap \mathcal{L}^{\text{gen}}\} dg &= \sum_{v \in \mathcal{L}^{\text{gen}}} \sum_{\gamma \in S_v} \text{Vol}(\{g \in G_0 : \gamma \in \mathcal{F}_1 g\}), \\ \int_{g \in \mathcal{F}_1} \#\{\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap \mathcal{L}^{\text{gen}}\} dg &= \sum_{v \in \mathcal{L}^{\text{gen}}} \sum_{\gamma \in S_v} \text{Vol}(\{g \in \mathcal{F}_1 : \gamma \in g G_0\}). \end{aligned}$$

Since

$$\begin{aligned} \text{Vol}(\{g \in G_0 : \gamma \in \mathcal{F}_1 g\}) &= \text{Vol}(G_0 \cap \mathcal{F}_1^{-1} \gamma) = \text{Vol}(\gamma G_0^{-1} \cap \mathcal{F}_1) \\ &= \text{Vol}(\{g \in \mathcal{F}_1 : \gamma \in g G_0\}), \end{aligned}$$

the lemma follows. □

In the next lemma we show that $\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$ has no integral generic points if t is too large.

Lemma 7.6. *Suppose $\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap V(\mathbb{Z})^{\text{gen}}$ is non-empty for $g = (n, m_3, t, \theta)$. Then $t \ll Y^{1/4}$.*

Proof. Let $(A, B) \in \mathcal{R}^{(\zeta)}$. Then $|a_{22}| \ll Y^{1/2}$. Therefore, there exists a constant C such that if $t > CY^{1/4}$, then $|a_{22}| < 1$ for every $(A, B) \in t\theta G_0 \mathcal{R}^{(\zeta)}$. The action of m_3, n , and \mathcal{F}_2 does not change the value of a_{22} , and it follows that $a_{22} = 0$ for every $(A, B) \in \mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap V(\mathbb{Z})$. We claim that such an (A, B) is not generic. Indeed, the conic in \mathbb{P}^2 cut out by A consists of a pair of lines, each of which is defined over \mathbb{Q} . Therefore, the intersection points of the conics corresponding to A and B are defined over a degree-2 extension of \mathbb{Q} , and so (A, B) cannot correspond to a D_4 field. The lemma thus follows. □

We let $\mathcal{F}' = \mathcal{F}_2 \mathcal{F}'_1 \subset \mathcal{F}$ consist of all elements $g_2 g_1$ with $g_2 \in \mathcal{F}_2$ and $g_1 = (n, m_3, t, \theta)$, where $t \leq CY^{1/4}$ for the C in the proof of the above lemma. For any lattice \mathcal{L} of $V(\mathbb{Z})$, define

$$\mathcal{N}_q^*(\mathcal{L}; X, Y) := \frac{2}{\tau_\zeta \text{Vol}(G_0)} \int_{g \in \mathcal{F}'_1} \#\{(\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap \mathcal{L})\} dg. \tag{38}$$

We use the following result of Davenport [13] to estimate $\mathcal{N}_q^*(\mathcal{L}; X, Y)$:

Proposition 7.7. *Let \mathcal{R} be a bounded, semi-algebraic multiset in \mathbb{R}^n having maximum multiplicity m , and that is defined by at most k polynomial inequalities each having degree at most ℓ . Then the number of integral lattice points (counted with multiplicity) contained in \mathcal{R} is*

$$\text{Vol}(\mathcal{R}) + O(\max\{\text{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\text{Vol}(\bar{\mathcal{R}})$ denotes the greatest d -dimensional volume of any projection of \mathcal{R} onto a coordinate subspace obtained by equating $n - d$ coordinates to zero, where d takes all values from 1 to $n - 1$. The implied constant in the second summand depends only on n, m, k , and ℓ .

In fact, the proof of the above proposition implies that we may replace $\text{Vol}(\bar{\mathcal{R}})$ by the maximum of the d -dimensional volumes of the projections of any unipotent translate of \mathcal{R} .

Now, for $g \in \mathcal{F}_1$, the set $g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$ is a bounded set contained in $V_{\text{red}}(\mathbb{R})$. Hence, the b_{12} - and b_{13} -coefficients of elements in $\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$ must lie in $[0, 2)$. They can only be integral when they are 0 or 1. Therefore, every integral point in $\mathcal{F}_2 g G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$ lies on one of four hyperplanes in $V(\mathbb{R})$: the hyperplanes corresponding to $(b_{12}, b_{13}) = (0, 0), (0, 1),$

(1, 0), and (1, 1). Moreover, these hyperplanes are unipotent translates of each other, in fact, by the elements in \mathcal{F}_2 with $m_1, m_2 \in \{0, 1/2\}$. It follows that the four hyperplane sections have the same volume, and Proposition 7.7 applied to them yields the same error estimates. Therefore,

$$\mathcal{N}_q^*(\mathcal{L}; X, Y) = \frac{8}{\tau_\zeta \text{Vol}(G_0)} \int_{g \in \mathcal{F}'_1} \text{Vol}_{\mathcal{L}}(gG_0 \cdot \mathcal{R}_{XY}^{(\zeta)}) dg + O(\mathcal{E}(X, Y)), \tag{39}$$

where $\text{Vol}_{\mathcal{L}}$ is computed with Euclidean measure normalized so that \mathcal{L} has covolume 1, and

$$\mathcal{E}(X, Y) = \frac{1}{\text{Vol}(G_0)} \int_{g=(0,0,t,0) \in \mathcal{F}'_1} \text{MP}(gG_0 \cdot \mathcal{R}_{XY}^{(\zeta)}) t^{-2} d^\times t.$$

The quantity $\text{MP}(g)$ denotes the maximal volume of the projections of $gG_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$ onto its coordinate hyperplanes. Every element (A, B) in $\mathcal{R}^{(\zeta)}$ is such that the coefficients of A are bounded by $Y^{1/2}$ and the coefficients of B are bounded by $X^{1/2}/Y^{1/2}$. By construction of G_0 , the same is true for every element in $G_0 \cdot \mathcal{R}^{(\zeta)}$. Then the error integral is easily bounded: as long as $Y \ll X$, the maximum projection is onto the coordinate subspace obtained by setting b_{22} to 0 since the ranges of the other coordinates are $\gg 1$ for every value of $g \in \mathcal{F}'_1$. Therefore, for $g = (0, 0, t, 0)$, we have

$$\text{MP}(gG_0 \cdot \mathcal{R}_{XY}^{(\zeta)}) \ll t^2 Y^{3/2} \frac{X}{Y} = t^2 XY^{1/2}.$$

Therefore,

$$\mathcal{E}(X, Y) \ll \frac{1}{\text{Vol}(G_0)} \int_{t=1}^{Y^{1/4}} XY^{1/2} d^\times t \ll Y^{3/2} X^{1/2} \log Y, \tag{40}$$

since $\text{Vol}(G_0)$ is easily seen to be $\asymp X^{1/2}/Y$.

We next have the following bound on the number of non-generic $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$.

Proposition 7.8. *We have*

$$\frac{1}{\text{Vol}(G_0)} \int_{g \in \mathcal{F}'_1} \#\{gG_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap V(\mathbb{Z}) \setminus V(\mathbb{Z})^{\text{gen}}\} dg = o(XY).$$

Proof. If $v \in V(\mathbb{Z})$ is not generic, then there exists unramified splitting types $\zeta'' = (\zeta''_p, \zeta'''_p)_p$ for all primes p such that $(\zeta_p(v), \zeta'_p(v)) \neq (\zeta''_p, \zeta'''_p)$ for all primes p . Given any unramified splitting type, there exists a constant $c < 1$ such that the density of elements in $V(\mathbb{Z}_p)$ that do not have splitting type (ζ''_p, ζ'''_p) is bounded above by c . From (41) we therefore obtain, for any fixed integer M ,

$$\begin{aligned} & \frac{1}{\text{Vol}(G_0)} \int_{g \in \mathcal{F}'_1} \#\{gG_0 \cdot \mathcal{R}_{XY}^{(\zeta)} \cap V(\mathbb{Z}) \setminus V(\mathbb{Z})^{\text{gen}}\} dg \\ & \ll \frac{\text{Vol}(G_0 \cdot \mathcal{R}_{XY}^{(\zeta)})}{\text{Vol}(G_0)} \cdot \prod_{p < M} c(\zeta''_p, \zeta'''_p) + \mathcal{E}(X, Y) \ll XY \cdot \prod_{p < M} c + X^{1/2} Y^{3/2} \log Y, \end{aligned}$$

where the second estimate follows since the ratio of volumes is $\asymp XY$. Note that by assumption, we have $X^{1/2}Y^{3/2} \log Y = o(XY)$. Therefore, by letting M tend to infinity, we obtain the result. \square

From (39), (40) and Proposition 7.8, we see that if X and Y go to infinity such that $Y(\log Y)^2 = o(X)$, then

$$\begin{aligned} \mathcal{N}_q^{(\delta)}(\mathcal{L}; X, Y) &= \frac{8X^{-1/2}Y}{\tau_\zeta \text{Vol}(G_1)} \text{Vol}(\mathcal{F}_1) \text{Vol}_{\mathcal{L}}(G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}) + o(XY) \\ &= \frac{8}{\tau_\zeta \text{Vol}(G_0)} \text{Vol}(\mathcal{F}_1) \text{Vol}_{\mathcal{L}}(G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}) + o(XY). \end{aligned} \tag{41}$$

To compute the volumes of $G_0 \cdot \mathcal{R}_{XY}^{(\zeta)}$, we have the following result, which follows immediately from a Jacobian change of variables computation.

Proposition 7.9. *Let dv_i be the standard Euclidean measures on $V_{\text{red}}(\mathbb{R})$, let dh denote the Haar measure on $G_{\text{red}}(\mathbb{R})$ obtained from the $\bar{N}AN$ decomposition of $\text{SL}_2(\mathbb{R})$, and pick the measure $dd \, dq$ on $\mathcal{R}^{(\zeta)}$. We have a natural map $G_{\text{red}}(\mathbb{R}) \times \mathcal{R}^{(\zeta)} \rightarrow V_{\text{red}}(\mathbb{R})$. Then the Jacobian of the change of variables is $1/16$, i.e., for any measurable function φ on $V_{\text{red}}(\mathbb{R})$, we have*

$$\int_{v \in G_{\text{red}}(\mathbb{R}) \cdot \mathcal{R}^{(\zeta)}} \varphi(v) \, dv = \frac{1}{16} \int_{r \in \mathcal{R}^{(\zeta)}} \int_{h \in G_{\text{red}}(\mathbb{R})} \varphi(g \cdot r) \, dh \, dd(r) \, dq(r). \tag{42}$$

Therefore, we obtain the following theorem from which Theorem 7.1 follows immediately.

Theorem 7.10. *Let \mathcal{L} denote a finite union of $G(\mathbb{Z})$ -invariant lattices in $V(\mathbb{R})^{(\zeta)}$. Then, for positive real numbers X, Y going to infinity such that $Y(\log Y)^2 = o(X)$, we have*

$$\mathcal{N}_q^{(\delta)}(\mathcal{L}; X, Y) = \frac{\zeta(2)}{2\tau_\zeta} \delta^2 XY \prod_p \text{Vol}(\mathcal{L}_p) + o_\delta(XY),$$

where \mathcal{L}_p denotes the closure of \mathcal{L} in $V(\mathbb{Z}_p)$, the volumes of sets in $V(\mathbb{Z}_p)$ are taken with respect to the usual Euclidean measure, and τ_ζ is as in Theorem 7.1.

Proof. The set $\mathcal{R}_{XY}^{(\zeta)}$ contains exactly one point with invariants q and d , for every $X \leq q < (1 + \delta)X$ and $Y \leq d < (1 + \delta)Y$. Hence, the volume of $\mathcal{R}_{XY}^{(\zeta)}$ is $\delta^2 XY$. The theorem now follows from (41) and Proposition 7.9 since the volume of \mathcal{F}_1 under the measure dh is $\zeta(2)$, and $\text{Vol}_{\mathcal{L}}$ differs from normal Euclidean measure by a factor of $\prod_p \text{Vol}(\mathcal{L}_p)$. \square

8. Uniformity estimates and sieving to D_4 -quartics

In order to use our results from §§4–5 and §§6–7 to prove our main theorems, we will employ simple sieves. In this section, we start by collecting the requisite tail estimates. First, we need a bound on the number of D_4 -quartics having central inertia at some large

prime, which is established in §8.1. On the other hand, in §8.2 we obtain an estimate on the number of $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$ that are non-maximal at some large prime. It is interesting to note that the results in §7 are not strong enough for these estimates, and so we employ techniques from §4.

8.1. Bounding the number of D_4 -quartics with large central inertia

We start with a preliminary lemma bounding the number of D_4 -quartics with fixed conductor.

Lemma 8.1. *For any positive integer N , the number of D_4 -quartics with conductor N is bounded by $O_\epsilon(N^\epsilon)$.*

Proof. Let L be a D_4 -quartic with conductor N , and let K be the quadratic subfield of L . Then the discriminant of K divides N . Hence the number of choices for K is bounded by twice the number of divisors of N . Given a fixed quadratic field K whose discriminant D divides N , the number of D_4 -quartics of conductor N whose quadratic subfield is K is bounded by $4 \cdot \#\text{Cl}_2(K)$ times the number of squarefree ideals dividing $4N$ (see [9, §3]). But $4 \cdot \#\text{Cl}_2(K) \ll_\epsilon D^\epsilon$ and the number of divisors of $4N$ is $\ll_\epsilon N^\epsilon$. Combining these estimates yields the lemma. \square

Next, we prove the required estimate on D_4 -quartics having specified central inertia by combining the previous lemma with Lemma 4.6.

Proposition 8.2. *Let X and Y be integers such that $X \geq Y$. Then the number of D_4 -quartics L such that $X \leq q(L) < 2X$, $Y \leq d(L) < 2Y$, and L has central inertia every prime dividing a positive squarefree integer n is bounded by $O_\epsilon(XY/n^{2-\epsilon})$.*

Proof. We consider two ranges of n . We fix a large positive real number M (any $M > 16$ will suffice). When $n \geq X^{1/M}$, we have $n \geq (XY)^{1/2M}$. The number of possible conductors for a D_4 -quartics L satisfying the conditions of the proposition is bounded by $O(XY/n^2)$, since the conductor is bounded by $4XY$ and is divisible by n^2 . Hence, from Lemma 8.1, it follows that the number of such fields L is bounded by $O_\epsilon((XY)^{1+\epsilon}/n^2) = O_\epsilon(XY/n^{2-\epsilon})$.

For $n \leq X^{1/M}$, we see from Lemma 4.6 that the number of D_4 -quartics satisfying the conditions of the proposition and having splitting type $((1^2 1^2), (11))$ or $((2^2), (2))$ at every prime dividing n is bounded by

$$O\left(\frac{X}{n^{2-\epsilon}} \cdot \sum_{\substack{[K:\mathbb{Q}]=2 \\ |\text{Disc}(K)| < Y}} L(1, K/\mathbb{Q})\right).$$

By [28, §3], the sum above is $\ll Y$ and so the total displayed quantity is bounded by $O(XY/n^{2-\epsilon})$. Similarly, the number of D_4 -quartics satisfying the conditions of the proposition and having splitting type $((1^4), (1^2))$ at every prime dividing n is bounded by

$$O\left(\frac{X}{n^{1-\epsilon}} \cdot \sum_{\substack{[K:\mathbb{Q}]=2 \\ n|\text{Disc}(K) \\ |\text{Disc}(K)| < Y}} L(1, K/\mathbb{Q})\right).$$

If $Y \geq n^M$, the sum of L -values is bounded by $O(Y/n)$ by arguments identical to those in [28, §3], yielding a total bound of $O(XY/n^{2-\epsilon})$. When instead $Y < n^M$, the classical bound of $O_\epsilon(\text{Disc}(K)^\epsilon)$ on $L(1, K/\mathbb{Q})$ yields the proposition. \square

8.2. Bounding the number of non-maximal $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$

For a fixed prime p , let \mathcal{W}_p denote the set of generic elements in $V(\mathbb{Z})$ that correspond to non-maximal orders in D_4 -quartics. Our next goal is to prove a uniform tail estimate for the number of $G(\mathbb{Z})$ -orbits on \mathcal{W}_p having bounded invariants. We start with the following lemmas.

Lemma 8.3. *The number of D_4 -quartics L with $|q(L)| < X$ and $|d(L)| < Y$ is bounded by $O(XY)$.*

Proof. From Lemma 4.5, we see that for $X \geq Y$ (in fact for $Y \ll_\epsilon X^{3-\epsilon}$), the number of D_4 -quartics with invariants q and d less than X and Y , respectively, is bounded by

$$O\left(X \cdot \sum_{|\text{Disc}(K)| < Y} L(1, K/\mathbb{Q})\right),$$

which is $O(XY)$ by the results in [28, §3].

When $X < Y$, we bound the number of D_4 -quartics L by instead bounding the number of fields $\phi(L)$ (see Definition 2.1). To do so, it suffices to show that, when $X < Y$ the number of fields L with $X < q(L) < 2X$ and $Y < d(L) < 2Y$ is $O(XY)$ since $\sum 2^{-m}$ converges. But recall from (7) that $J(L)d(\phi(L)) = q(L)$. Then under this assumption,

$$Y \cdot J(L) < q(\phi(L)) < 2Y \cdot J(L), \quad \frac{X}{J(L)} < d(\phi(L)) < \frac{2X}{J(L)}.$$

By Proposition 8.2, since $Y \cdot J(L) \geq Y > X \geq X/J(L)$, we find that the number of such D_4 -quartics $\phi(L)$ in this range with $J(\phi(L)) = J(L) = n$ is $O_\epsilon(XY/n^{2-\epsilon})$, so it suffices to sum $O_\epsilon(XY/n^{2-\epsilon})$ over all valid n . Since $\sum 1/n^{2-\epsilon}$ over integers n converges, this completes the proof. \square

We now prove the following uniform bound on the number of $G(\mathbb{Z})$ -orbits on \mathcal{W}_p , the set of generic elements in $V(\mathbb{Z})$ that are not maximal at p .

Proposition 8.4. *The number of $G(\mathbb{Z})$ -orbits v on \mathcal{W}_p with $X \leq q(v) < 2X$ and $Y \leq d(v) < 2Y$ is bounded by $O_\epsilon(XY/p^{2-\epsilon})$.*

Proof. Note that since this is an asymptotic statement as p grows, we may assume that p is sufficiently large, and in particular that p is odd. An element $v \in \mathcal{W}_p$ gives a quartic ring Q whose field of fractions L is a D_4 -quartic. Let $i(v)$ denote $C(v)/C(L)$, the ratio of the conductors of v and L . From Lemma 6.6, it follows that $i(v)$ is divisible by p^2 . From Lemma 8.3, it follows that the number of possible fields L that occur this way is bounded by $O(XY/i(v)^{1-\epsilon})$. Next, note that the index of Q in the ring of integers of L

divides $i(v)$. The methods of [26] imply that the number of suborders of index $k = \prod p_i^{e_i}$ of a maximal quartic ring is bounded by

$$j(k) := \prod p_i^{(2+\epsilon)\lfloor e_i/4 \rfloor}.$$

Once the order Q has been determined, there are $O(1)$ choices for the quadratic subring T of Q corresponding to v under Theorem 6.1. Finally, Corollary 4 of [1] asserts that the number of cubic resolvents of ring Q is $d(c)$, the sum of the divisors of the content c of Q . Furthermore, the content c of the quartic ring corresponding to $v = (A, B)$ is equal to the gcd of the coefficients of A (see [1, §3.6]), which implies that $i(v)$ is a multiple of c^4 .

Therefore, the number of $G(\mathbb{Z})$ -orbits on \mathcal{W}_p satisfying the conditions of the proposition is bounded by

$$\sum_{p^2|m} \sum_{c^4|m} \sum_{k|m} j(k)d(c)(X/m^{1-\epsilon}), \tag{43}$$

where m runs over all integers divisible by p^2 . Using the multiplicativity of j and d , the expression (43) is easily seen to be $\ll_\epsilon X/p^{2-\epsilon}$ and the proposition follows. \square

9. Proof of the main theorems

In this section, we conclude the proof of the generalization of Theorem 5.3 that allows for imposing certain local specifications (see Theorem 9.3). First, we define p -adic densities and determine the number of étale algebras along with their automorphism groups for each splitting type. As a byproduct of the two asymptotics obtained for $N_C(\Sigma; X, X^{1/2})$ by Theorem 4.3 and in §9.2, we prove Theorem 6.

Theorems 1 and 3 are proved in §9.3. First, we obtain asymptotics for $N_C(\Sigma; X, Y)$ when $Y > X^{1/2}$ from counting D_4 -quartics $\phi(L)$ with conductor bounded by X and small quadratic discriminant, where $L \in \mathcal{L}(\Sigma)$. We then prove Theorem 3 after employing a bound that follows from the analytic methods in Sections 4 and 5. Finally, in §9.4 we prove a refinement of Theorem 5, which follows from Theorem 3 in conjunction with the p -adic volumes determined in Proposition 6.7.

9.1. Acceptable local specifications, densities, and automorphism groups

Recall that for a collection Σ of local specifications, $\mathcal{L}(\Sigma)$ is the set of D_4 -quartics L such that the pair consisting of the splitting type of L and the splitting type of K (its quadratic subfield at a prime p (respectively, at ∞) is contained in Σ_p for all p , respectively, in Σ_∞). A set Σ of local specifications (and the corresponding family $\mathcal{L}(\Sigma)$) is said to be *acceptable* if for all but finitely many primes p , the set Σ_p contains all unramified splitting types and tamely ramified splitting types without central inertia. (In the notation of (5), Σ_p contains exactly the pairs $(\varsigma_p(L_1), \varsigma_p(K_1))$ contained in the first two groups in Table 1.)

Recall that for a prime p and a splitting type (ζ_p, ζ'_p) , we computed the density $\mu(M_p(\zeta_p, \zeta'_p))$ in Proposition 6.7. We define the density $\mu(\Sigma_p)$ to be the sum of the values of $\mu(M_p(\zeta_p, \zeta'_p))$ over $(\zeta_p, \zeta'_p) \in \Sigma_p$, and define the density of $\mu(\Sigma_\infty)$ to be the sum of $1/\tau_\zeta$ over all $\zeta \in \Sigma_\infty$. The stabilizer quantities τ_ζ are defined in Theorem 7.1, and we list them below for convenience:

$$\tau_\zeta = \begin{cases} 8 & \text{if } \zeta = ((1111), (11)), ((22), (11)), \\ 4 & \text{if } \zeta = ((112), (11)), ((22), (2)). \end{cases} \tag{44}$$

Furthermore, if $\zeta(L) = ((1111), (11))$, then L is a totally real field, and $\text{Aut}(L_\infty, K_\infty) = \text{Aut}(\mathbb{R}^4, \mathbb{R}^2) = D_4$. If $\zeta(L) = ((22), (11))$, then L is a CM field and $\text{Aut}(L_\infty, K_\infty) = \text{Aut}(\mathbb{C}^2, \mathbb{R}^2) = D_4$. If $\zeta(L) = ((112), (11))$, then L has exactly one complex embedding, and $\text{Aut}(L_\infty, K_\infty) = \text{Aut}(\mathbb{R}^2 \oplus \mathbb{C}, \mathbb{R}^2) = V_4$. Finally, if $\zeta(L) = ((22), (2))$, then L is a totally complex field with imaginary quadratic subfield K , and $\text{Aut}(L_\infty, K_\infty) = \text{Aut}(\mathbb{C}^2, \mathbb{C}) = V_4$. Overall, we have shown:

Lemma 9.1. *For any quadratic extension L of a quadratic field K ,*

$$\# \text{Aut}(L_\infty, K_\infty) = \tau_\zeta(L, K).$$

Next, we determine the automorphism groups of étale quartic algebras over \mathbb{Q}_p sending a quadratic subalgebra to itself for odd primes p .

Lemma 9.2. *Let p be an odd prime. The automorphism group of a pair (L, K) , where K is a quadratic étale algebra over \mathbb{Q}_p , and L is a quadratic étale algebra over K , is determined by the splitting type of (L, K) , and is listed in the following table: Above, when we write (a, b) for the number of (isomorphism classes of) étale algebras over \mathbb{Q}_p , the first coordinate indicates the quantity for primes of the form $4k + 1$ and the second coordinate for primes of the form $4k + 3$. Additionally, there are two distinct isomorphism classes of étale algebras with splitting type $(1^2 1^2)$: in the table, we distinguish them by letting $(1^2 1^2)$ refer to the sum of two isomorphic ramified quadratic extensions of \mathbb{Q}_p and letting $(1^2 1^{2'})$ refer to the sum of two non-isomorphic ramified quadratic extensions of \mathbb{Q}_p .*

Proof. The above lemma can be verified case by case using [21] in conjunction with the fact that determining the possible étale algebras for a given splitting type depends only on the congruence class of p mod 4. □

9.2. A refinement of Theorem 5.3 and the proof of Theorem 6

For positive real numbers X and Y , let $\mathcal{N}_q^{(\delta)}(\Sigma; X, Y)$ be as in Section 7. We have the following theorem, giving another proof that the heuristics of (9) holds for certain ranges of X and Y .

Theorem 9.3. *Let Σ be an acceptable set of local specifications. For positive real numbers X and Y such that $Y(\log Y)^2 = o(X)$, we have*

$$\mathcal{N}_q^{(\delta)}(\Sigma; X, Y) = \frac{\zeta(2)}{2} \cdot \delta^2 \cdot \mu(\Sigma_\infty) \cdot \prod_p \mu(\Sigma_p) \cdot XY + o_\delta(XY).$$

Table 3. Automorphism groups for étale algebras over \mathbb{Q}_p .

| $\zeta_p(L, K)$ | # of algebras | $\text{Aut}(L, K)$ | $C(L, K)$ |
|----------------------|---------------|--------------------|-----------|
| $((11), (1111))$ | 1 | D_4 | 1 |
| $((11), (112))$ | 1 | V_4 | 1 |
| $((11), (22))$ | 1 | D_4 | 1 |
| $((2), (22))$ | 1 | V_4 | 1 |
| $((2), (4))$ | 1 | C_4 | 1 |
| $((11), (1^2 11))$ | 2 | V_4 | p |
| $((11), (1^2 2))$ | 2 | V_4 | p |
| $((1^2), (1^2 1^2))$ | 2 | V_4 | p |
| $((1^2), (2^2))$ | 2 | V_4 | p |
| $((11), (1^2 1^2))$ | 2 | D_4 | p^2 |
| $((11), (1^2 1^2'))$ | 1 | V_4 | p^2 |
| $((2), (2^2))$ | 1 | V_4 | p^2 |
| $((2), (2^2))$ | 1 | C_4 | p^2 |
| $((1^2), (1^4))$ | $(0, 2)$ | C_2 | p^2 |
| $((1^2), (1^4))$ | $(4, 0)$ | C_4 | p^2 |

Proof. By Proposition 6.3, it suffices to obtain asymptotics for the number of generic $G(\mathbb{Z})$ -orbits (A, B) on $V(\mathbb{Z})$ such that (A, B) is maximal and the splitting type of (A, B) at each place belongs to Σ . The number of generic $G(\mathbb{Z})$ -orbits on $V(\mathbb{Z})$ satisfying any finite set of congruence conditions has been estimated in Theorem 7.10. Theorem 9.3 then follows from Theorem 7.10 and the uniformity estimates in Propositions 8.2 and 8.4 by means of a simple sieve. We omit the details since they are very similar to those in the proof of Theorem 9.4. □

As a consequence of the main terms obtained in Theorems 4.3 and 9.3, we may now prove Theorem 6. It is interesting to note that the proof of Theorem 6 is much more involved than that of Theorem 2. In particular, it is not obvious that the arguments in Section 5 can be refined to directly allow for imposing acceptable sets of local specifications.

Proof of Theorem 6. Let \mathcal{K} denote the set of quadratic fields with prescribed splitting types ζ'_p given at a finite set S of odd primes p . Let $(\Sigma_p)_p$ denote sets, where for each $p \notin S$, $\Sigma_p = \Sigma_p^{\text{full}}$ contains all possible splitting types, and for $p \in S$, $\Sigma_p = \{(*, \zeta'_p)\}$ consists of all possible splitting types compatible with ζ'_p . If we let

$$\Sigma_\infty^{(a)} = \{((1111), (11)), ((112), (11)), ((22), (11))\} \quad \text{and} \quad \Sigma_\infty^{(b)} = \{((22), (2))\},$$

we can define $\Sigma^{(*)}$ to be the collection $(\Sigma_p)_p$ and $\Sigma_\infty^{(*)}$ for $* = a$ or b , which are both acceptable collections.

Recall that $N_C(\Sigma^{(*)}; X, X^\beta)$ counts the number of isomorphism classes of D_4 -quartics $L \in \mathcal{L}(\Sigma^{(*)})$ such that $|C(L)| < X$ and $|d(L)| < X^\beta$. As before, let $r_2(K)$ denote

the number of pairs of complex embeddings of K . From Theorem 4.3 we have, for $* = a$ or b and $\beta < 2/3$,

$$N_C(\Sigma^{(*)}; X, X^\beta) = \frac{X}{2\zeta(2)} \cdot \sum_{\substack{K \in \mathcal{K}(\Sigma^{(*)}) \\ |\text{Disc}(K)| < X^\beta}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{2^{-r_2(K)}}{|\text{Disc}(K)|} + o_\beta(X). \tag{45}$$

On the other hand, we can also estimate $N_C(\Sigma^{(*)}; X, X^\beta)$ using Theorem 9.3 as follows. Consider the region

$$R_{X,\beta} := \{(d, q) \in \mathbb{R}^2 : |d \cdot q| < X, |d| < X^\beta\}.$$

There exist regions $R_{X,\beta}^{(\pm)}$, that are disjoint unions of δ -adic rectangles, such that

$$R_{X,\beta}^{(-)} \subset R_{X,\beta} \subset R_{X,\beta}^{(+)}$$

and such that

$$|\text{Vol}(R_{X,\beta}) - \text{Vol}(R_{X,\beta}^{(\pm)})| \ll \delta \cdot X \log(X^\beta).$$

The volume of $R_{X,\beta}$ is $X \log(X^\beta)$. Therefore, from Theorem 9.3, we see that for $\beta < 1/2$,

$$N_C(\Sigma^{(*)}; X, X^\beta) = \frac{\zeta(2)}{2} \cdot X \log(X^\beta) \cdot \mu(\Sigma_\infty^{(*)}) \cdot \prod_p \mu(\Sigma_p) + o_\delta(X \log(X^\beta)) + O(\delta X \log(X^\beta)). \tag{46}$$

Equating the right hand sides of (45) and (46), dividing both sides by $X \log(X^\beta)$, first letting X^β tend to infinity, and then finally letting δ tend to 0, we obtain

$$\frac{1}{2\zeta(2)} \cdot \sum_{\substack{K \in \mathcal{K}(\Sigma^{(*)}) \\ |\text{Disc}(K)| < X}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \cdot \frac{2^{-r_2(K)}}{|\text{Disc}(K)|} \sim \frac{\zeta(2)}{2} \cdot \mu(\Sigma_\infty^{(*)}) \cdot \prod_p \mu(\Sigma_p) \cdot \log X. \tag{47}$$

It is a direct computation to verify from (44) and the definitions of $\Sigma_\infty^{(*)}$ that $2^{r_2(K)} \cdot \mu(\Sigma_\infty^{(*)})$ is always equal to $1/2$, independently of the choice of $K \in \mathcal{K}(\Sigma^{(*)})$. Furthermore, the values of $\mu(\Sigma_p) = \sum_{(\zeta_p, \zeta'_p) \in \Sigma_p} \mu(M_p(\zeta_p, \zeta'_p))$ can be computed from Proposition 6.7, and it then follows that the right hand sides of Theorem 6(a, b) are asymptotically equal to

$$\frac{\zeta(2)^2}{2} \cdot \prod_p \mu(\Sigma_p) \cdot \log X.$$

This concludes the proof of Theorem 6. □

9.3. The proofs of Theorems 1 and 3

We next obtain asymptotics for $\mathcal{N}_q^{(\delta)}(\Sigma; X, Y)$ when $Y \gg X$. Recall that the outer automorphism ϕ of D_4 provides a non-isomorphic D_4 -quartic $\phi(L)$ for each D_4 -quartic L , and the fields L and $\phi(L)$ have the same conductor but (possibly) different invariants. Proposition 2.6 can be used to compute the invariants of $\phi(L)$ in terms of the invariants of L . Note that if $d(L) > q(L)$, then $d(\phi(L)) < q(\phi(L))$. Hence, for a collection Σ of local specifications, we may relate counts of D_4 -quartics with $d > q$ to counts of D_4 -quartics with $d < q$.

Given an acceptable collection Σ , let $\phi(\mathcal{L}(\Sigma))$ denote the family defined by

$$\phi(\mathcal{L}(\Sigma)) := \{\phi(L) : L \in \mathcal{L}(\Sigma)\}$$

There exists another acceptable collection $\phi(\Sigma)$ of local specifications such that $\phi(\mathcal{L}(\Sigma)) = \mathcal{L}(\phi(\Sigma))$. Furthermore, for every odd prime p , by Table 1 in conjunction with Proposition 6.7 and Lemma 6.8 for an acceptable collection Σ , we have $\mu(\Sigma_p) = \mu(\phi(\Sigma_p))$. An acceptable family Σ is said to be *very stable at 2* if the set Σ_2 either contains all splitting types with central inertia (pairs $(\varsigma_2(L_1), \varsigma_2(K_1))$ in the latter two groups of Table 1), or contains none of them. Our next result computes the number of D_4 -quartics in $\mathcal{L}(\Sigma)$ satisfying $X \leq |q(L)| \leq (1 + \delta)X$ and $Y \leq |d(L)| < (1 + \delta)Y$ when Y is much larger than X .

Theorem 9.4. *Let Σ be an acceptable collection of local specifications that is very stable at 2. Let X and Y be positive real numbers such that $X(\log X)^2 = o(Y)$. Then*

$$\mathcal{N}_q^{(\delta)}(\Sigma; X, Y) = \frac{\zeta(2)}{2} \cdot \delta^2 \cdot \mu(\Sigma_\infty) \cdot \prod_p \mu(\Sigma_p) \cdot XY + o(XY).$$

Proof. For a prime p and an integer $a \geq 1$, let $\mathcal{V}(p, a)$ denote the set of D_4 -quartics L such that $J_p(L) = p^a$. Recall that $J(L)$ is defined in (7), and an odd prime p divides $J(L)$ if and only if $p^2 \parallel L$ if and only if L has splitting type $((2^2), (2))$, or $((1^2 1^2), (11))$. Let \mathcal{V}_p denote the union of $\mathcal{V}(p, a)$ over all $a \geq 1$, and for any integer $n \geq 1$, let $\mathcal{L}(\Sigma)^{(n)}$ denote the set of fields L in $\mathcal{L}(\Sigma)$ such that $J(L) = n$. One can check that $\mathcal{L}(\Sigma)^{(n)}$ is defined by an acceptable collection $\Sigma^{(n)}$ of local specifications that is very stable at 2, i.e., $\mathcal{L}(\Sigma^{(n)}) = \mathcal{L}(\Sigma)^{(n)}$. Using (7) and the fact that $J(L) = J(\phi(L))$, we have

$$\mathcal{N}_q^{(\delta)}(\Sigma; X, Y) = \sum_{n \geq 1} \mathcal{N}_q^{(\delta)}(\Sigma^{(n)}; X, Y) = \sum_{n \geq 1} \mathcal{N}_q^{(\delta)}(\phi(\Sigma^{(n)}); Yn, X/n).$$

For a fixed integer M , we use Theorem 9.3 to evaluate $\mathcal{N}_q^{(\delta)}(\phi(\Sigma)^{(n)}; Yn, X/n)$ for $n \leq M$ and Proposition 8.2 to bound $\mathcal{N}_q^{(\delta)}(\phi(\Sigma)^{(n)}; Yn, X/n)$ for $n > M$. Altogether, we obtain

$$\begin{aligned} &\mathcal{N}_q^{(\delta)}(\Sigma; X, Y) \\ &\sim \frac{\zeta(2)}{2} \cdot \delta^2 \cdot \mu(\phi(\Sigma)_\infty) \cdot \left(\sum_{n=1}^M \prod_{p^a \parallel n} \mu(\phi(\Sigma)_p \cap \mathcal{V}(p, a)) \cdot \prod_{p \nmid n} \mu(\phi(\Sigma)_p \setminus \mathcal{V}_p) \right) \cdot XY \end{aligned}$$

up to an error of $o_{\delta,M}(XY) + O_{\epsilon,\delta}(XY/M^{1-\epsilon})$, where we assume that $a \geq 1$. Dividing by XY , letting X and Y tend to infinity, and then letting M tend to infinity, we obtain

$$\begin{aligned} & \lim_{M \rightarrow \infty} \lim_{X, Y \rightarrow \infty} \frac{\mathcal{N}_q^{(\delta)}(\Sigma; X, Y)}{\delta^2 XY} \\ &= \frac{\zeta(2)}{2} \cdot \mu(\phi(\Sigma)_\infty) \cdot \sum_{n \geq 1} \left(\prod_{p^a \parallel n} \mu(\phi(\Sigma)_p \cap \mathcal{V}(p, a)) \cdot \prod_{p \nmid n} \mu(\phi(\Sigma)_p \setminus \mathcal{V}_p) \right) \\ &= \frac{\zeta(2)}{2} \cdot \mu(\phi(\Sigma)_\infty) \cdot \sum_{n \geq 1} \left(\prod_p \mu(\phi(\Sigma)_p \setminus \mathcal{V}_p) \cdot \prod_{p^a \parallel n} \frac{\mu(\phi(\Sigma)_p \cap \mathcal{V}(p, a))}{\mu(\phi(\Sigma)_p \setminus \mathcal{V}_p)} \right) \\ &= \frac{\zeta(2)}{2} \cdot \mu(\phi(\Sigma)_\infty) \cdot \prod_p \mu(\phi(\Sigma)_p \setminus \mathcal{V}_p) \cdot \prod_p \left(1 + \sum_{a \geq 1} \frac{\mu(\phi(\Sigma)_p \cap \mathcal{V}(p, a))}{\mu(\phi(\Sigma)_p \setminus \mathcal{V}_p)} \right) \\ &= \frac{\zeta(2)}{2} \cdot \mu(\phi(\Sigma)_\infty) \cdot \prod_p \mu(\phi(\Sigma)_p). \end{aligned}$$

Since $\mu(\Sigma_p) = \mu(\phi(\Sigma)_p)$ for all primes p and $\mu(\Sigma_\infty) = \mu(\phi(\Sigma_\infty))$, we obtain the result. □

We now have theorems computing $\mathcal{N}_q^{(\delta)}(\Sigma; X, Y)$ when $X(\log X)^2 = o(Y)$ (Theorem 9.3) and when $Y(\log Y)^2 = o(X)$ (Theorem 9.4) with identical right hand sides. Our last task in proving Theorem 3 is to show that the region that neither Theorem 9.3 nor 9.4 covers contributes negligibly to $\mathcal{N}_q^{(\delta)}(\Sigma; X, Y)$. For that we need the following lemma.

Lemma 9.5. *The number of D_4 -quartics L such that $|C(L)| \leq X$ and $X(\log X)^{-3} \leq |d(L)| \leq X(\log X)^3$ is bounded by $O(X \log \log X)$.*

Proof. The number of D_4 -quartics satisfying the conditions of the lemma can be estimated as a sum of ratios of L -values from Theorem 4.3. This sum can be bounded, using Proposition 5.2, by

$$X \cdot \sum_{D=X(\log X)^{-3}}^{X(\log X)^3} \frac{1}{D},$$

yielding the lemma. □

Proof of Theorem 3. The invariants d and q of a D_4 field with absolute conductor bounded by X satisfy $|d \cdot q| < X$. Consider the region $R_X := \{(d, q) \in \mathbb{R}^2 : |d \cdot q| < X\}$. We bound the number of D_4 -quartics L with $\sqrt{X}(\log \sqrt{X})^{-3} \leq d(L) \leq \sqrt{X}(\log \sqrt{X})^3$ using Lemma 9.5, and estimate the rest of the D_4 -quartics using Theorems 9.3 and 9.4 with an argument identical to the proof of Theorem 6, obtaining

$$N_{D_4}(\Sigma, X) \sim \frac{\zeta(2)}{2} \cdot \mu(\Sigma_\infty) \cdot \prod_p \mu(\Sigma_p) \cdot X \log X.$$

Let $\zeta_p(L_p, K_p)$ denote the splitting type of a pair (L_p, K_p) of local extensions of \mathbb{Q}_p .

From Proposition 6.7 and Lemma 9.2 we obtain, for each odd prime p ,

$$\frac{1}{\#\text{Aut}(L_p, K_p)} \cdot \frac{1}{C_p(L_p)} \cdot \left(1 - \frac{1}{p}\right)^2 = \frac{\mu(M_p(\zeta_p(L_p, K_p)))}{1 - p^{-2}},$$

and at ∞ , Lemma 9.1 implies $\#\text{Aut}(L_\infty, K_\infty) = \tau_\zeta(L_\infty, K_\infty)$. For $p = 2$, we can utilize Proposition 3.1(3) to conclude the proof of Theorem 3. □

Theorem 1 follows directly from Theorem 3 in conjunction with the p -adic density computations in Theorem 6.9 and the following density computations at ∞ using (44):

- (0) D_4 -quartic fields with exactly four real embeddings all have infinite splitting type ((1111), (11)), and therefore $\mu(\Sigma_\infty) = 1/8$;
- (1) D_4 -quartic fields with exactly two real embeddings all have infinite splitting type ((112), (11)), and therefore $\mu(\Sigma_\infty) = 1/4$;
- (2) D_4 -quartic fields with no real embeddings have infinite splitting type ((22), (11)) or ((22), (2)), and therefore $\mu(\Sigma_\infty) = 1/8 + 1/4 = 3/8$.

9.4. The proof of Theorem 5

We end this article with the proof and a discussion of Theorem 5.

Let $K \in \mathcal{K}$ be a quadratic field, and for each $p \in S$, let ζ denote the prescribed splitting type at p for \mathcal{K} . Since finite abelian groups are isomorphic to their duals, we see that $\#\text{Cl}(K)[4] - \#\text{Cl}(K)[2]$, the number of elements in $\text{Cl}(K)$ having exact order 4, is equal to twice the number of index-4 subgroups of $\text{Cl}(K)$ whose quotients are cyclic. By class field theory, such index-4 subgroups of $\text{Cl}(K)$ are in bijection with isomorphism classes of unramified extensions M of K with $\text{Gal}(M/K) = C_4$. Such an extension M is Galois over \mathbb{Q} with Galois group D_4 . Conversely, if M is an octic D_4 -quartic whose splitting type at every prime p lies in the first two quadrants of Table 1, then M is unramified over K , its quadratic subfield fixed by $C_4 \subset D_4$. Furthermore, it is straightforward to check from Table 1 that under these conditions, M is unramified over K .

Now we define three collections $\Sigma^{(i)}$ of local specifications corresponding to the three cases in Theorem 5. First, let $\mathcal{K}^{(*)}$ be the subset of $K \in \mathcal{K}$ with $\zeta_\infty(K) = (11)$ when $* = a$ or c , and $\zeta_\infty(K) = (2)$ when $* = b$, and define

$$\Sigma_\infty^{(*)} := \begin{cases} \{((1111), (11))\} & \text{if } * = a, \\ \{((112), (11)), ((22), (2))\} & \text{if } * = b, \\ \{((1111), (11)), ((22), (11))\} & \text{if } * = c. \end{cases}$$

Next we define Σ_p for all finite primes p . If $p \notin S$, define

$$\Sigma_p = \{(\zeta_p, \zeta'_p) : (\zeta_p, \zeta'_p) \text{ lacks central inertia}\}.$$

For $p \in S$, define

$$\Sigma_p = \begin{cases} \{((1111), (11)), ((22), (11)), ((4), (2))\} & \text{if } \zeta = (11), \\ \{((112), (11)), ((22), (2))\} & \text{if } \zeta = (2), \\ \{((1^211), (11)), ((1^22), (11)), ((1^21^2), (1^2)), ((2^2), (1^2))\} & \text{if } \zeta = (1^2). \end{cases}$$

Let $\Sigma^{(*)}$ then denote the collection of local specifications consisting of $(\Sigma_p)_p$ along with $\Sigma_\infty^{(*)}$ for $* = a, b, \text{ or } c$, which is acceptable and very stable at 2. It is easily checked from Table 1 that the Galois closures of fields in $\mathcal{L}(\Sigma^{(*)})$ correspond to cyclic quartic unramified extensions of fields in $\mathcal{K}^{(*)}$. When $* = a$ or b , $\mathcal{L}(\Sigma^{(*)})$ corresponds to order-4 elements in the class groups of $\mathcal{K}^{(*)}$. On the other hand, $\mathcal{L}(\Sigma^{(c)})$ corresponds to cyclic quartic extensions of $\mathcal{K}^{(c)}$ that are unramified at every finite place, but possibly ramified at infinity; thus, they correspond to order-4 elements in the narrow class groups of real quadratic fields in \mathcal{K} . Furthermore, from (5), it follows that exactly two distinct isomorphism classes of D_4 -quartics yield the same Galois closure, but additionally every index-4 subgroup of the class group corresponds to two order-4 ideal classes. Thus, we conclude that the left hand sides of Theorem 5(*) are equal to $N_{D_4}(\Sigma^{(*)}, X)$, for $* = a, b$, and c . The theorem follows from Theorem 3 along with density computations following from Proposition 6.7. \square

Remark 9.6. Fouvry–Klüners [15] prove that the average size of $2^{\text{rk}_4(\text{Cl}^+(K))}$ over imaginary (respectively, real) quadratic fields K ordered by discriminant is equal to 2 (respectively, $3/2$), where $\text{rk}_4(\text{Cl}^+(K)) = \dim_{\mathbb{F}_2}(\text{Cl}^+(K)^4/\text{Cl}^+(K)^2)$. Furthermore,

$$\# \text{Cl}_4^+(K) - \# \text{Cl}_2^+(K) = (2^{\text{rk}_4(\text{Cl}^+(K))} - 1) \cdot (\# \text{Cl}_2^+(K)).$$

Genus theory implies that for any quadratic field K , $\# \text{Cl}_2^+(K) = 2^{\omega(\text{Disc}(K)) - 1}$, where $\omega(D)$ denotes the number of prime factors of D . Additionally, using similar techniques to those in §5.2, one can check the genus theory formula for the size of $\text{Cl}_2^+(K)$ implies the asymptotics

$$\sum_{\substack{K \text{ quad.} \\ -X \leq \text{Disc}(K) < 0}} \# \text{Cl}_2^+(K) \sim \frac{1}{4} \cdot \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X,$$

$$\sum_{\substack{K \text{ quad.} \\ 0 < \text{Disc}(K) \leq X}} \# \text{Cl}_2^+(K) \sim \frac{1}{4} \cdot \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X.$$

Combining the above result with those of [15] and Theorem 5 illustrates an interesting “independence” phenomenon: the average value of the product $(2^{\text{rk}_4(\text{Cl}^+(K))} - 1) \cdot (\# \text{Cl}_2^+(K))$ is equal to the product of the average value of $2^{\text{rk}_4(\text{Cl}^+(K))} - 1$ and the average size of $\text{Cl}_2^+(K)$.

Acknowledgments. We thank Manjul Bhargava, Henri Cohen, Dorian Goldfeld, Joseph Gunther, John W. Jones, Jürgen Klüners, Aaron Landesman, André Macedo, Samuel Ruth, Xiaoheng Wang, and Melanie Matchett Wood for helpful conversations. We would also like to thank the anonymous referee for providing detailed and thoughtful comments on previous versions of this article.

References

[1] Bhargava, M.: Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)* **159**, 1329–1360 (2004) [Zbl 1169.11045](#) [MR 2113024](#)

- [2] Bhargava, M.: The density of discriminants of quartic rings and fields. *Ann. of Math. (2)* **162**, 1031–1063 (2005) [Zbl 1159.11045](#) [MR 2183288](#)
- [3] Bhargava, M.: Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *Int. Math. Res. Notices* **2007**, art. rnm052, 20 pp. [Zbl 1145.11080](#) [MR 2354798](#)
- [4] Bhargava, M.: The density of discriminants of quintic rings and fields. *Ann. of Math. (2)* **172**, 1559–1591 (2010) [Zbl 1220.11139](#) [MR 2745272](#)
- [5] Bhargava, M., Shankar, A.: Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)* **181**, 191–242 (2015) [Zbl 1307.11071](#) [MR 3272925](#)
- [6] Bhargava, M., Wood, M. M.: The density of discriminants of S_3 -sextic number fields. *Proc. Amer. Math. Soc.* **136**, 1581–1587 (2008) [Zbl 1171.11058](#) [MR 2373587](#)
- [7] Cassels, J. W. S., Fröhlich, A.: *Algebraic Number Theory*. Academic Press (1967) [Zbl 0153.07403](#)
- [8] Cohen, H.: Constructing and counting number fields. In: *Proc. Int. Congress of Mathematicians (Beijing, 2002)*, Vol. II, Higher Ed. Press, Beijing, 129–138 (2002) [Zbl 1042.11067](#) [MR 1957027](#)
- [9] Cohen, H., Diaz y Diaz, F., Olivier, M.: Enumerating quartic dihedral extensions of \mathbb{Q} . *Compos. Math.* **133**, 65–93 (2002) [Zbl 1050.11104](#) [MR 1918290](#)
- [10] Cohen, H., Diaz y Diaz, F., Olivier, M.: A survey of discriminant counting. In: *Algorithmic Number Theory (Sydney, 2002)*, Lecture Notes in Computer Sci. 2369, Springer, Berlin, 80–94 (2002) [Zbl 1058.11076](#) [MR 2041075](#)
- [11] Cohen, H., Lenstra, H. W., Jr.: Heuristics on class groups of number fields. In: *Number Theory, Noordwijkerhout 1983*, Lecture Notes in Math. 1068, Springer, Berlin, 33–62 (1984) [Zbl 0558.12002](#) [MR 756082](#)
- [12] Cohen, H., Martinet, J.: Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.* **404**, 39–76 (1990) [Zbl 0699.12016](#) [MR 1037430](#)
- [13] Davenport, H.: On a principle of Lipschitz. *J. London Math. Soc.* **26**, 179–183 (1951) [Zbl 0042.27504](#) [MR 43821](#)
- [14] Davenport, H., Heilbronn, H.: On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A* **322**, 405–420 (1971) [Zbl 0212.08101](#) [MR 491593](#)
- [15] Fouvry, E., Klüners, J.: On the 4-rank of class groups of quadratic number fields. *Invent. Math.* **167**, 455–513 (2007) [Zbl 1126.11062](#) [MR 2276261](#)
- [16] Fouvry, E., Klüners, J.: Weighted distribution of the 4-rank of class groups and applications. *Int. Math. Res. Notices* **2011**, 3618–3656 [Zbl 1251.11076](#) [MR 2824840](#)
- [17] Gerth, F., III: Extension of conjectures of Cohen and Lenstra. *Exposition. Math.* **5**, 181–184 (1987) [Zbl 0613.12003](#) [MR 887792](#)
- [18] Johnson, S.: *Weighted discriminants and Mass formulas for number fields*. ProQuest LLC, Ann Arbor, MI (2015) [MR 3358235](#)
- [19] Jones, J. W., Roberts, D. P.: A database of local fields. *J. Symbolic Comput.* **41**, 80–97 (2006) [Zbl 1140.11350](#) [MR 2194887](#)
- [20] Kedlaya, K. S.: Mass formulas for local Galois representations. *Int. Math. Res. Notices* **2007**, art. rnm021, 26 pp. [Zbl 1175.11071](#) [MR 2354797](#)
- [21] LMFDB Collaboration: *The L-functions and Modular Forms Database*. <http://www.lmfdb.org> (2013)
- [22] Mäki, S.: The conductor density of abelian number fields. *J. London Math. Soc. (2)* **47**, 18–30 (1993) [Zbl 0727.11041](#) [MR 1200974](#)
- [23] Malle, G.: On the distribution of Galois groups. II. *Experiment. Math.* **13**, 129–135 (2004) [Zbl 1099.11065](#) [MR 2068887](#)

-
- [24] Malle, G.: On the distribution of class groups of number fields. *Experiment. Math.* **19**, 465–474 (2010) [Zbl 1297.11139](#) [MR 2778658](#)
 - [25] Martinet, J.: Les discriminants quadratiques et la congruence de Stickelberger. *Sém. Théor. Nombres Bordeaux (2)* **1**, 197–204 (1989) [Zbl 0731.11061](#) [MR 1050275](#)
 - [26] Nakagawa, J.: Orders of a quartic field. *Mem. Amer. Math. Soc.* **122**, no. 583, viii+75 pp. (1996) [Zbl 0865.11069](#) [MR 1342021](#)
 - [27] Rose, H. E.: *A Course on Finite Groups*. Universitext, Springer London, London (2009) [Zbl 1200.20001](#) [MR 2583713](#)
 - [28] Siegel, C. L.: The average measure of quadratic forms with given determinant and signature. *Ann. of Math. (2)* **45**, 667–685 (1944) [Zbl 0063.07007](#) [MR 12642](#)
 - [29] Wood, M. M.: Mass formulas for local Galois representations to wreath products and cross products. *Algebra Number Theory* **2**, 391–405 (2008) [Zbl 1176.11063](#) [MR 2411405](#)
 - [30] Wood, M. M.: *Moduli spaces for rings and ideals*. ProQuest LLC, Ann Arbor, MI (2009) [MR 2713054](#)
 - [31] Wood, M. M.: On the probabilities of local behaviors in abelian field extensions. *Compos. Math.* **146**, 102–128 (2010) [Zbl 1242.11081](#) [MR 2581243](#)