

On the asymptotics of cubic fields ordered by general invariants

Arul Shankar and Frank Thorne

July 18, 2023

Abstract

In this article, we introduce a class of invariants of cubic fields termed “generalized discriminants”. We then obtain asymptotics for the families of cubic fields ordered by these invariants. In addition, we determine which of these families satisfy the Malle–Bhargava heuristic.

1 Introduction

A foundational result due to Davenport–Heilbronn [17] provides asymptotics for the number of real and cubic fields, when these fields are ordered by their discriminants. Specifically, the theorem states:

Theorem 1 (Davenport–Heilbronn) *Let $N_{\text{Disc}}^{\pm}(X)$ denote the number of cubic fields K , up to isomorphism, that satisfy $|\text{Disc}(K)| < X$ and $\pm \text{Disc}(K) > 0$. Then*

$$\begin{aligned} N_{\text{Disc}}^+(X) &= \frac{1}{12\zeta(3)}X + o(X); \\ N_{\text{Disc}}^-(X) &= \frac{1}{4\zeta(3)}X + o(X). \end{aligned}$$

The above theorem, its extensions, and the methods of their proofs, have had a host of applications. Among many other applications, they are used by Yang [38] to verify the Katz–Sarnak heuristics [18] for low-lying zeroes of Dedekind zeta functions of cubic fields; by Bhargava–Wood [11], Belabas–Fouvry [3] and Wang [36] to prove Malle’s conjecture for various different Galois groups; by Martin–Pollack [24] and Cho–Kim [12] to obtain the average value of the smallest prime satisfying certain prescribed splitting conditions; by AS–Södergren–Templier [30] to prove that the Dedekind zeta functions of infinitely many S_3 -cubic fields have negative central values.

Theorem 1 has also been generalized in numerous ways: Belabas–Bhargava–Pomerance [2] prove power saving error terms; Bhargava [4, 6] determines the asymptotics of quartic and quintic fields, when ordered by discriminant; Datskovsky–Wright [16], Taniguchi [31], and Bhargava–AS–Wang [9] count cubic extensions of number fields and function fields; Belabas–Fouvry [3] count subfamilies of cubic fields satisfying congruence conditions on their discriminants; Terr [34] proves that the “shapes” of cubic rings and fields are equidistributed (see also work of Bhargava–Harron [7], who give a uniform proof that shapes of cubic, quartic, and quintic rings and fields are equidistributed); Taniguchi–FT [32] and Bhargava–AS–Tsimerman [8] compute secondary terms (of size $\asymp X^{5/6}$) for the asymptotics of $N_{\text{Disc}}^{\pm}(X)$.

In this paper, we consider generalizations along a different direction: namely, we determine asymptotics for families of cubic fields ordered by invariants more general than the discriminant. Let $C(K)$ be the radical of $|\text{Disc}(K)|$. That is, we have $C(K) := \prod_{p|\text{Disc}(K)} p$. We then prove the following result.

Theorem 2 Let $N_C^\pm(X)$ denote the number of cubic fields K , up to isomorphism, that satisfy $C(K) < X$ and $\pm \text{Disc}(K) > 0$. Then

$$\begin{aligned} N_C^+(X) &= \frac{33}{120} \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 X \log X + o(X \log X); \\ N_C^-(X) &= \left(\frac{3}{10} + \frac{33}{40}\right) \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 X \log X + o(X \log X). \end{aligned}$$

Note that we break up the main term in the asymptotics for $N_C^-(X)$ into two summands; they correspond to what can be considered two disjoint subfamilies of cubic fields, namely, the family of pure cubic fields and the family of non-pure cubic fields.

Theorem 2 will be deduced as a special case of a more general result that counts cubic fields ordered by various different types of invariants.

Generalized discriminants of cubic fields

Let M be a Galois sextic field with Galois group S_3 over \mathbb{Q} . Then K has three cubic S_3 -subfields, which are conjugate to each other. One would therefore expect to be able to understand the family of sextic S_3 -fields via the family of cubic S_3 -fields. Bhargava–Wood [11] and Belabas–Fouvry [3] independently use this philosophy to prove the following result.

Theorem 3 (Belabas–Fouvry, Bhargava–Wood) Let $N_{\Delta_6}^\pm(X)$ denote the number of Galois sextic number fields M with Galois group S_3 , such that $|\text{Disc}(M)| < X$ and $\pm \text{Disc}(M) > 0$.

Then, we have

$$N_{\Delta_6}^\pm(X) = \frac{C^\pm}{12} \prod_p c_p \cdot X^{1/3} + o(X^{1/3}),$$

where $C^+ = 1, C^- = 3$, the product is over all primes, and

$$c_p = \begin{cases} (1 - p^{-1})(1 + p^{-1} + p^{-4/3}) & p \neq 3, \\ (1 - \frac{1}{3})(\frac{4}{3} + \frac{1}{3^{5/3}} + \frac{2}{3^{7/3}}) & p = 3. \end{cases}$$

A power saving error term for the above quantity was obtained by work of Taniguchi–FT [33]. In this work, they also speculate about a possible secondary term, and discuss tensions between theoretical predictions and the data.

Similarly to $C(K)$, we will regard $|\text{Disc}(M)|$ as a “generalized discriminant” of its cubic subfield. More specifically, let K be a non-Galois cubic field, and denote the Galois closure of K by M . Then M has a unique quadratic subfield, denoted L . We say that L is the *quadratic resolvent field* of K . Denote the discriminant of the quadratic resolvent L of K by $D(K)$. Then $D(K) \mid \text{Disc}(K)$, and moreover, $\text{Disc}(K)/D(K)$ is always a perfect integer square. Denote its positive integer squareroot by $F(K)$. We note that apart from a factor of a bounded power of 3, the quantity $F(K)$ is simply the product of primes that totally ramify in K , where p is said to totally ramify in K if p splits as $p = \mathfrak{p}^3$. Similarly, up to a bounded power of 2, the quantity $D(K)$ is the product of primes that ramify, but not totally, in K . For a cubic S_3 -field K , let $\Delta_6(K)$ denote the discriminant of the Galois closure M of K . Then we have the decompositions

$$(1) \quad \text{Disc}(K) = D(K)F(K)^2, \quad \Delta_6(K) = D(K)^3F(K)^4, \quad C(K) = |D(K)|F(K),$$

where the final equality is true up to bounded factors of 2 and 3. For positive real numbers α and β , we say that the invariant $|D|^\alpha F^\beta$ is a *generalized discriminant*. This notion of generalized discriminant encompasses all three invariants we have seen so far, namely, $\text{Disc}(K)$, $\Delta_6(K)$, and $C(K)$.

When K is a cyclic cubic field, the invariant $\Delta_6(K)$ has no special meaning but an otherwise similar analysis holds with $D(K) := 1$. We also define the above quantities analogously when K is a cubic étale extension of \mathbb{Q}_p .

Let $\Sigma = (\Sigma_v)_v$ be a *collection of cubic splitting types*, where for each place v of \mathbb{Q} , the set Σ_v is the set of cubic étale extensions of \mathbb{Q}_v with specified inertial and ramification indices.¹ The collection Σ is said to be a *finite collection* if for all large enough primes p , Σ_p is the set of all cubic étale extensions of \mathbb{Q}_p (i.e., all inertial and ramification indices are allowed). Throughout, we write P_Σ for the product of those primes where Σ_p is a proper subset of these extensions.

Given a finite collection of cubic splitting types Σ , let $\mathcal{F}(\Sigma)$ denote the set of cubic fields K such that $K \otimes \mathbb{Q}_v \in \Sigma_v$ for all v . For a generalized discriminant I , we define

$$N_I(\Sigma; X) := \#\{K \in \mathcal{F}(\Sigma) : I(K) < X, D(K) \neq -3\}.$$

As the pure cubic fields (those with $D(K) = -3$) behave differently from those with other quadratic resolvents, we will treat them separately.

The next result determines asymptotics for the family $\mathcal{F}(\Sigma)$, excluding the pure cubic fields, ordered by generalized discriminants.

Theorem 4 *Fix positive real numbers α and β , and let $I = |D|^\alpha F^\beta$ be a generalized discriminant. Let Σ be a finite collection of cubic splitting types. Then*

(a) *When $\alpha < \beta$, we have*

$$N_I(\Sigma; X) = \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|D(K)|_p |F(K)|_p^{\beta/\alpha}}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p} \right) \cdot X^{\frac{1}{\alpha}} + O_{\epsilon, I}((X^{\frac{2}{\alpha+\beta} + \epsilon} + X^{\frac{5}{6\alpha}}) P_\Sigma^{2/3}).$$

(b) *When $\alpha > \beta$, we have*

$$N_I(\Sigma; X) = \left(\sum_{d \text{ fund. disc} \neq -3} \frac{\text{Res}_{s=1} \Phi_{\Sigma, d}(s)}{|d|^{\alpha/\beta}} \right) \cdot X^{\frac{1}{\beta}} + O_{\epsilon, I}((X^{\frac{3}{2\alpha+\beta} + \epsilon} + X^{\frac{2}{3\beta} + \epsilon}) P_\Sigma^{1/3}),$$

where $\Phi_{\Sigma, d}(s)$ are Dirichlet series introduced in §2.

(c) *When $\alpha = \beta$, we have*

$$N_I(\Sigma; X) = \frac{1}{2\alpha} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|D(K)|_p |F(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p} \right)^2 \cdot X^{\frac{1}{\alpha}} \log X + o_{\Sigma, I}(X^{\frac{1}{\alpha}} \log X).$$

For the pure cubic fields, Cohen and Morra proved [14, Corollary 7.4] that, when $\Sigma_v = \Sigma_v^{\text{all}}$ for all v ,

$$(2) \quad \#\{K \in \mathcal{F}(\Sigma) : D(K) = 3, F(K) < Z\} = C_1 Z (\log(Z) + C_2 - 1) + O(Z^{2/3+\epsilon}),$$

where

$$C_1 := \frac{7}{30} \prod_p \left(1 + \frac{2}{p} \right) \left(1 - \frac{1}{p} \right)^2,$$

$$C_2 := 2\gamma - \frac{16}{35} \log(3) + 6 \sum_p \frac{\log(p)}{p^2 + p - 2},$$

where the sum and product are over all primes p . This result also generalizes to arbitrary Σ ; see (13). Taking $Z = X^{1/\beta} 3^{-\alpha/\beta}$, we see that adding the pure cubic fields adds a term of order $X^{1/\beta} \log(X)$, along with a secondary term of order $X^{1/\beta}$, to each of the results in Theorem 4. For (a) this is subsumed by

¹This is a less general notion than the one which allows Σ_v to be an arbitrary subset of étale cubic extensions of \mathbb{Q}_v . We restrict ourselves to this less general notion for two reasons. First, this is the more natural notion from the point of view of families of L -functions; see the discussion on Sato–Tate equidistribution at the end of the introduction. Second, we did not obtain a version of Theorem 11 valid in this generality. Although this seems likely to be possible, it appears liable to be inelegant while presenting additional complications in the proof.

the error term, and the result is unchanged; for (b), this new contribution dominates the asymptotics by a factor of $\asymp \log X$, so that asymptotically 100% of cubic fields ordered by I will be pure cubic fields; for (c) this contribution is of equal magnitude, and the pure and non-pure cubic fields each constitute a positive proportion of cubic fields ordered by I .

We recover Theorem 3, with a power saving error term of $O(X^{\frac{2}{7}+\epsilon})$, by taking $\alpha = 3$ and $\beta = 4$ in Theorem 4 and carrying out an appropriate calculation at the 2- and 3-adic places. (This was also noted in [10].) When $\frac{\beta}{\alpha} > \frac{7}{5}$, the error term of $O(X^{\frac{5}{6\alpha}})$ in case (a) dominates the other error term and can be refined into a secondary term extrapolating that proved in [8, 32] for $\alpha = 1$ and $\beta = 2$. More precisely, we have the following result.

Theorem 5 *Let α and β be positive real numbers with $\frac{\beta}{\alpha} > \frac{7}{5}$, and let $I = |\mathcal{D}|^\alpha \mathcal{F}^\beta$. Then we have*

$$N_I(\Sigma; X) = C_1(I; \Sigma) \cdot X^{\frac{1}{\alpha}} + C_2(I; \Sigma) \cdot X^{\frac{5}{6\alpha}} + O_\epsilon((X^{\frac{2}{\alpha+\beta}+\epsilon} + X^{\frac{2}{3\alpha}+\epsilon}) P_\Sigma^{2/3}),$$

where $C_1(I; \Sigma)$ is the leading constant appearing in the right hand side of the displayed equation in Part (a) of the above theorem, and

$$C_2(I; \Sigma) = C(\infty) \frac{4\zeta(1/3)}{5\Gamma(2/3)^3 \zeta(5/3)} \prod_p \left[\frac{\sum_{K_p \in \Sigma_p(f)} \frac{|\mathcal{D}(K_p)|_p |\mathcal{F}(K_p)|_p^{\frac{5\beta+2\alpha}{6\alpha}}}{|\text{Aut}(K_p)|} \int_{\mathcal{O}_{K_p} \setminus p\mathcal{O}_{K_p}} [\mathcal{O}_{K_p} : \mathbb{Z}_p[x]]^{2/3} dx}{\sum_{K_p \in \Sigma_p^{\text{all}}} \frac{|\mathcal{D}(K_p)|_p |\mathcal{F}(K_p)|_p^2}{|\text{Aut}(K_p)|} \int_{\mathcal{O}_{K_p} \setminus p\mathcal{O}_{K_p}} [\mathcal{O}_{K_p} : \mathbb{Z}_p[x]]^{2/3} dx} \right]$$

where $C(\infty)$ is 1, $\sqrt{3}$ or $1 + \sqrt{3}$ depending on whether Σ_∞ consists of \mathbb{R}^3 , $\mathbb{R} \oplus \mathbb{C}$ or both, respectively. Also, \mathcal{O}_K denotes the ring of integral elements in K_p .

The Malle–Bhargava heuristics

In [22, 23], Malle develops heuristics for asymptotics of the number of degree- n number fields with Galois group G and bounded discriminant, where $n > 1$ is any integer and G is a finite group with an action on a set with n elements. These heuristics are believed to be true in most cases. However, see [20] where Klüners demonstrates a counter example in the case $n = 3$ and $G = C_3 \wr C_2$, and [35], where Türkelli modifies Malle’s conjecture so that it holds in the above and similar cases. While Malle’s conjecture has been formulated only for families of fields ordered by discriminant, the same method applies to other orderings, in particular to the generalized discriminants that we work with.

Interestingly, the leading constants appearing in front of Malle’s heuristics are still shrouded with mystery. In the case of degree- n S_n number fields ordered by discriminant, Bhargava [5] formulates a conjecture for the leading coefficients, using a general recipe which constructs these constants from mass formulae counting étale extensions of local fields. Once again, this recipe is quite general, applying to any family of number fields constructed as follows: fix a degree $n > 1$ and a group G with a transitive action on the set $\{1, \dots, n\}$. Then this recipe applies to the family of all degree- n number fields with Galois group G , satisfying any finite set of splitting conditions, ordered by any generalized discriminant. (See also work of Kedlaya [19] describing how these leading constants can be computed in the more general case of families of Galois representations.) However, there are many instances where this prediction gives the incorrect leading constant. The prototypical example is the family of quartic D_4 -fields ordered by discriminant, where the asymptotic constant determined by Cohen–Díaz y Díaz–Olivier [13] is not expected to equal the constant that this recipe would predict. On the other hand, when quartic D_4 -fields are ordered by conductor, Altug–AS–Varma–Wilson [1] establish that the leading asymptotic constant does arise from the Malle–Bhargava recipe. This leads to the natural question, as discussed by Bhargava in [5], of which families of number fields ordered by which invariants satisfy this property.

We say that a family F of number fields, ordered by some generalized discriminant, satisfies the *Malle–Bhargava heuristic* if the asymptotics of every subfamily defined by prescribed splitting at finitely many

primes are as predicted by the Malle–Bhargava recipe. (Despite our terminology, we emphasize again that Bhargava conjectured this only for S_n , and did not predict that it should always hold.)

A necessary condition is that the splitting behaviour of primes is independent. We now precisely define this notion. Let \mathcal{G} be a family of number fields having the same degree n .² Let $\Sigma = (\Sigma_v)_v$ be a *collection of degree- n splitting types*, where for each place v of \mathbb{Q} , Σ_v is the set of degree- n étale extensions of \mathbb{Q}_v satisfying specified inertial and ramification behaviour. For each place v , let Σ_v^{all} denote the set of all degree- n étale extensions of \mathbb{Q}_v . Then Σ is said to be *finite* if $\Sigma_p = \Sigma_p^{\text{all}}$ for all sufficiently large primes p . Let $h : \mathcal{G} \rightarrow \mathbb{R}_{>0}$ be a height function (i.e., there are only finitely many elements of \mathcal{G} having bounded height). Let $N_h(\mathcal{G}_\Sigma; X)$ denote the number of elements in \mathcal{G} satisfying Σ and having height less than X . Then we say that the family \mathcal{G} ordered by h satisfies *independence of primes* if the following is true. For all places v of \mathbb{Q} , there exist functions $\sigma_v : \Sigma_v^{\text{all}} \rightarrow \mathbb{R}_{\geq 0}$ with

$$\sum_{K_v \in \Sigma_v^{\text{all}}} \sigma_v(K_v) = 1,$$

such that the following condition is satisfied. For each finite collection of splitting types Σ , we have

$$N_h(\mathcal{G}_\Sigma; X) \sim \left(\prod_v \sum_{K_v \in \Sigma_v} \sigma_v(K_v) \right) \cdot N_h(\mathcal{G}; X).$$

There are many known examples of families of number fields which do not satisfy independence of primes. See for example [37], in which Wood studies families of number fields with any fixed abelian Galois group, and proves in many cases that, when ordered by discriminant, these families do not satisfy independence of primes. We note that the notion of satisfying independence of primes is a weaker notion than that of satisfying the Malle–Bhargava heuristic, when both these notions make sense. Moreover, independence of primes can be defined for a wider class of families, for example, this notion makes sense for the family of pure cubic fields, the family of monogenic degree- n fields, and many other families for which the Malle–Bhargava heuristics do not apply.

Next, we consider the family of all cubic fields. It is natural to partition this family into two subfamilies: the family of pure cubics and the family of non-pure cubics. The ordering on the family of pure cubic fields coming from any generalized discriminant is the same (since we have $D(K) = -3$ for every pure cubic field K). It follows from the method of Cohen–Morra [14] described in §2.2 that the family of pure cubic fields satisfies independence of primes. For the family of non-pure cubic fields ordered by generalized discriminants, we have the following result.

Theorem 6 *Let $I = |D|^\alpha F^\beta$ be a generalized discriminant. Then the family of all non-pure cubic fields ordered by I satisfies independence of primes and the Malle–Bhargava heuristic if and only if $\alpha \leq \beta$.*

For the $\alpha \leq \beta$ case, the above result is an immediate consequence of Theorem 4. This $\alpha > \beta$ case requires a bit more work, since the residues of the Dirichlet series appearing in Part (b) of Theorem 4 are not explicit. We give a general proof which also applies to many different situations, such as the family of quartic D_4 -fields ordered by discriminant.

Finally, our counting results also have implications towards families of Artin L -functions associated to cubic S_3 -fields. Indeed, let $\rho : S_3 \rightarrow \text{GL}_n(\mathbb{C})$ be any representation of S_3 . Given a cubic S_3 -field K , with normal closure M , we obtain a Galois representation

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(M/\mathbb{Q}) \cong S_3 \rightarrow \text{GL}_n(\mathbb{C}),$$

where the final map is ρ . We associate to this Galois representation its Artin L -function, denoted $L(s; \rho, K)$. Throughout, we assume that ρ contains at least one copy of the standard representation of S_3 , which is necessary to ensure that different cubic fields give rise to different L -functions. Then, given a family $\mathcal{F}(\Sigma)$

²It is not entirely clear exactly what constitutes a *family* of number fields. Being the set of all number fields having the same degree and the same Galois group is assumed to be a sufficient though not a necessary condition. See [28], where a similar question is discussed in detail.

of cubic S_3 -fields K , we obtain a family of Artin L -functions $L(s; \rho, K)$ that we denote by $\mathcal{L}(\rho, \Sigma)$. We order the L -functions in $\mathcal{L}(\rho, \Sigma)$ by their conductors.

Ordering $\mathcal{L}(\rho, \Sigma)$ by conductor corresponds to ordering $\mathcal{F}(\Sigma)$ by a certain generalized discriminant $I = |D|^\alpha F^\beta$ depending on ρ . Indeed, we have $(\alpha, \beta) = c_1(1, 2) + c_2(1, 0)$ where $c_1 \geq 1$ and $c_2 \geq 0$ are the multiplicities of the standard and sign representations respectively, so that $\alpha > 0$ and $\beta > 0$. A consequence of Theorem 4 is that the family $\mathcal{L}(\rho, \Sigma)$ satisfies Sato–Tate equidistribution in the sense of [28, Conjecture 1]. Loosely speaking, a family of L -functions arising from number fields satisfies Sato–Tate equidistribution when the asymptotics of these number fields, ordered by the conductors of their L -functions, satisfy the Malle–Bhargava heuristics on average over primes p . Identically to the arguments in [29, §3.1], when $\alpha \leq \beta$, this follows immediately from the shape of the leading constant in Parts (a) and (c) of Theorem 4. When $\alpha > \beta$ the situation is similar to the case of the family of Dedekind zeta functions of D_4 -fields considered in [29, §6.2]. As there, we consider the family of cubic fields ordered by I to be a countable union of subfamilies, one for each fixed quadratic resolvent field. Since each of these subfamilies contributes a positive proportion to the full family, Sato–Tate equidistribution for the full family follows from Sato–Tate equidistribution for each subfamily. Thus, we have the following consequence to Theorem 4:

Corollary 7 *With notation as above, the families $\mathcal{L}(\rho, \Sigma)$ satisfy Sato–Tate equidistribution.*

It is interesting to note that despite independence of primes not always holding, Sato–Tate equidistribution is always satisfied for our families.

Organization of the paper

We begin in §2 by considering families of cubic fields with one fixed invariant. Invoking work of Bhargava–Taniguchi–FT [10] on the Davenport–Heilbronn theorem, we obtain asymptotics for families of cubic fields with fixed F ; using work of Cohen–Morra [14] and Cohen–FT [15] on a Kummer-theoretic approach, we deduce asymptotics for families of cubic fields with fixed D . The leading constants appearing in the asymptotics for the latter family are somewhat inexplicit, but in §3 we prove that the average values of these constants have an explicit description given in terms of products of mass formulae.

The results of the previous two subsections allow us to determine asymptotics for $\mathcal{F}(\Sigma)$ ordered by generalized discriminants. This is accomplished in §4, and we extract secondary terms and power saving error terms when possible. We then establish exactly when independence of primes holds, thereby proving Theorem 6. Finally, we conclude in §5 by presenting some numerical data.

Throughout, implied constants may depend on ϵ , α , and β , but not Σ unless otherwise noted.

2 Families of cubic fields with a fixed invariant

Recall that for each cubic field or étale algebra K/\mathbb{Q} or K/\mathbb{Q}_p , we have a decomposition

$$(3) \quad \text{Disc}(K) = D(K)F(K)^2,$$

where $D(K)$ is the discriminant of the *quadratic resolvent* algebra of K . When K is a S_3 -cubic field $D(K)$ is the discriminant of the unique quadratic field contained in the Galois closure of K , and when K is a cyclic cubic field $D(K) = 1$. We decompose these quantities into local factors

$$(4) \quad \text{Disc}(K) = \pm \prod_p \text{Disc}_p(K), \quad D(K) = \pm \prod_p D_p(K), \quad F(K) = \prod_p F_p(K),$$

with $D_p(K) = p^{v_p(D(K))}$ and $F_p(K) = p^{v_p(F(K))}$. Then these quantities enjoy the following properties:

(a) When $p > 3$, then

$$(D_p(K), F_p(K)) \in \{(1, 1), (p, 1), (1, p)\},$$

with the three cases corresponding to the ramification type of p in K : unramified, partially ramified, or totally ramified, respectively.

(b) When $p = 3$, we have

$$(D_3(K), F_3(K)) \in \{(1, 1), (p, 1), (p, p), (1, p^2), (p, p^2)\}.$$

Here p is unramified in the first case, partially ramified in the second case, and totally ramified in the remaining cases.

(c) When $p = 2$, we have

$$(D_2(K), F_2(K)) \in \{(1, 1), (p^2, 1), (p^3, 1), (1, p)\}.$$

Here p is unramified in the first case, partially ramified in the next two cases, and totally ramified in the last case.

Given a positive number f , squarefree away from 3, and indivisible by 27, we let $\mathcal{F}(\Sigma)^{(f)}$ denote the set of cubic S_3 -fields $K \in \mathcal{F}(\Sigma)$ with $F(K) = f$. Given a fundamental discriminant d , we let $\mathcal{F}(\Sigma)_d$ denote the set of cubic S_3 -fields $K \in \mathcal{F}(\Sigma)$ with $D(K) = d$. (By convention, we consider 1 to be a fundamental discriminant.) In this section, we obtain asymptotics for the number of $K \in \mathcal{F}(\Sigma)^{(f)}$ with $|D(K)| < Y$ in §2.1, and the number of $K \in \mathcal{F}(\Sigma)_d$ with $F(K) < Z$ in §2.2. In particular, we obtain error terms that control the dependence on Σ .

2.1 Counting cubic fields K with fixed $F(K)$

Let f be a fixed positive integer, squarefree away from 3. To count cubic fields K where $F(K) = f$, we appeal to a strengthening of the Davenport-Heilbronn theorem. Define the quantity

$$N(\mathcal{F}(\Sigma)^{(f)}; Y) := \#\{K \in \mathcal{F}(\Sigma)^{(f)} : |D(K)| < Y\}.$$

Then we have the following:

Theorem 8 ([10], Theorem 1.4) *We have*

$$(5) \quad N(\mathcal{F}(\Sigma)^{(f)}; Y) = C_1(\Sigma, f) \cdot Y + C_2(\Sigma, f) \cdot Y^{5/6} + O(E(Y; f, \Sigma)),$$

for constants $C_1(\Sigma, f)$ and $C_2(\Sigma, f)$ described below, and with the following ‘averaged’ bound on $E(Y; f, \Sigma)$: for each $f \leq F$, choose independent and arbitrary values $Y_f \leq Y$. Then, we have

$$\sum_{f \leq F} E(Y_f; f, \Sigma) \ll_{\epsilon} Y^{2/3+\epsilon} F^{4/3+\epsilon} P_{\Sigma}^{2/3},$$

uniformly in F .

The leading constant $C_1(\Sigma, f)$ is described as follows. First, for a prime p and a positive integer f , define the set $\Sigma_p(f)$ of f -compatible algebras in Σ_p to be those étale cubic extensions K_p of \mathbb{Q}_p such that the powers of p dividing $F(K_p)$ and f are the same. Then we have

$$C_1(\Sigma, f) := \frac{1}{2} \left(\sum_{K_{\infty} \in \Sigma_{\infty}} \frac{1}{|\text{Aut}(K_{\infty})|} \right) \prod_p \left[\left(\sum_{K_p \in \Sigma_p(f)} \frac{|\text{D}(K_p)|_p}{|\text{Aut}(K_p)|} \right) \left(1 - \frac{1}{p}\right) \right].$$

For each prime $p > 3$, when $\Sigma_p = \Sigma_p^{\text{all}}$, we have

$$(6) \quad \left(\sum_{K_p \in \Sigma_p(f)} \frac{|\text{D}(K_p)|_p}{|\text{Aut}(K_p)|} \right) \left(1 - \frac{1}{p}\right) = \begin{cases} \left(1 - \frac{1}{p}\right) & \text{when } p \mid f; \\ \left(1 - \frac{1}{p^2}\right) & \text{when } p \nmid f. \end{cases}$$

Meanwhile, the secondary constant $C_2(\Sigma, f)$ is given by

$$C_2(\Sigma, f) := C(\infty) \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)} \prod_p \nu_p(\Sigma_p, f),$$

where $C(\infty)$ is 1, $\sqrt{3}$, or $1 + \sqrt{3}$ depending on whether Σ_∞ consists of \mathbb{R}^3 , $\mathbb{R} \oplus \mathbb{C}$, or both, respectively, and

$$(7) \quad \nu_p(\Sigma_p, f) := \frac{\sum_{K_p \in \Sigma_p(f)} \frac{|\mathbf{D}(K_p)|_p |\mathbf{F}(K_p)|_p^{1/3}}{|\text{Aut}(K_p)|} \int_{\mathcal{O}_{K_p} \setminus p\mathcal{O}_{K_p}} [\mathcal{O}_{K_p} : \mathbb{Z}_p[x]]^{2/3} dx}{\sum_{K_p \in \Sigma_p^{\text{all}}} \frac{|\mathbf{D}(K_p)|_p |\mathbf{F}(K_p)|_p^2}{|\text{Aut}(K_p)|} \int_{\mathcal{O}_{K_p} \setminus p\mathcal{O}_{K_p}} [\mathcal{O}_{K_p} : \mathbb{Z}_p[x]]^{2/3} dx}.$$

Moreover we have $C_1(\Sigma, f) < 1$ and $|C_2(\Sigma, f)| \ll f^{-1/3}$ for all Σ and f .

To compute average values of these constants, we introduce the Dirichlet series $L_1(\Sigma, s)$ and $L_2(\Sigma, s)$ given by

$$(8) \quad L_1(\Sigma, s) := \sum_f C_1(\Sigma, f) f^{-s}; \quad L_2(\Sigma, s) := \sum_f C_2(\Sigma, f) f^{-s};$$

These series satisfy the following Euler product decomposition in their domains of absolute convergence.

Proposition 9 *For $\Re(s) > 1$, we have*

$$\begin{aligned} L_1(\Sigma, s) &= \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\mathbf{D}(K)|_p |\mathbf{F}(K)|_p^s}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p} \right); \\ L_2(\Sigma, s - 1/3) &= C(\infty) \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)} \prod_p \left[\frac{\sum_{K_p \in \Sigma_p} \frac{|\mathbf{D}(K_p)|_p |\mathbf{F}(K_p)|_p^{s/3}}{|\text{Aut}(K_p)|} \int_{\mathcal{O}_{K_p} \setminus p\mathcal{O}_{K_p}} [\mathcal{O}_{K_p} : \mathbb{Z}_p[x]]^{2/3} dx}{\sum_{K_p \in \Sigma_p^{\text{all}}} \frac{|\mathbf{D}(K_p)|_p |\mathbf{F}(K_p)|_p^2}{|\text{Aut}(K_p)|} \int_{\mathcal{O}_{K_p} \setminus p\mathcal{O}_{K_p}} [\mathcal{O}_{K_p} : \mathbb{Z}_p[x]]^{2/3} dx} \right]. \end{aligned}$$

Proof: To prove the first equality in the above displayed notation, note that we have

$$(9) \quad \begin{aligned} L_1(\Sigma, s) &= \sum_{f \geq 1} \frac{C_1(\Sigma, f)}{f^s} \\ &= \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \sum_{f \geq 1} \frac{1}{f^s} \prod_p \left(\sum_{K \in \Sigma_p(f)} \frac{|\mathbf{D}(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p} \right) \\ &= \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\mathbf{D}(K)|_p |\mathbf{F}(K)|_p^s}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p} \right), \end{aligned}$$

as necessary. The second equality follows in identical fashion. \square

2.2 Counting cubic fields K with fixed $\mathbf{D}(K)$

For each nonzero fundamental discriminant d , define a Dirichlet series

$$\Phi_{\Sigma, d}(s) := c_{\text{red}} + \sum_{K \in \mathcal{F}(\Sigma)_d} \frac{1}{\mathbf{F}(K)^s},$$

where c_{red} is either 1/2 or 0 depending on whether or not the étale cubic algebra $\mathbb{Q} \oplus \mathbb{Q}(\sqrt{d})$ satisfies the splitting conditions specified by Σ . Using Kummer theory and class field theory, Cohen, Morra, and the second author [14, 15] proved the following explicit formula for $\Phi_{\Sigma, d}(s)$ when $P_\Sigma = 1$, i.e. for counting all cubic fields whose quadratic resolvent is $\mathbb{Q}(\sqrt{d})$.

Theorem 10 ([15], Theorem 2.5) *For any nonzero fundamental discriminant d we have*

$$(10) \quad c_d \Phi_d(s) = \frac{1}{2} M_{1,d}(s) \prod_{p \nmid 3d} \left(1 + \frac{1 + \left(\frac{-3d}{p}\right)}{p^s} \right) + \sum_{E \in \mathcal{L}_3(d)} M_{2,E}(s) \prod_{p \nmid 3d} \left(1 + \frac{\omega_E(p)}{p^s} \right),$$

where:

- $c_d = 1$ if $d = 1$ or $d < -3$, and $c_d = 3$ if $d = -3$ or $d > 1$.
- $\mathcal{L}_3(d)$ is the set of cubic fields of discriminant $-d/3$, $-3d$, and $-27d$. (The first case can of course only occur if $3 \mid d$, and the second only if $3 \nmid d$.)
- For any cubic field E and prime $p \nmid \text{Disc}(E)$, we define

$$\omega_E(p) := \begin{cases} 2 & \text{if } p \text{ is totally split in } E, \\ 0 & \text{if } p \text{ is partially split in } E, \\ -1 & \text{if } p \text{ is inert in } E, \end{cases}$$

- The 3-Euler factors $M_{1,d}(s)$ and $M_{2,E}(s)$ are given in the following table.

Condition on d	$M_{1,d}(s)$	$M_{2,E}(s)$, $\text{Disc}(E) \in \{-d/3, -3d\}$	$M_{2,E}(s)$, $\text{Disc}(E) = -27d$
$3 \nmid d$	$1 + 2/3^{2s}$	$1 + 2/3^{2s}$	$1 - 1/3^{2s}$
$d \equiv 3 \pmod{9}$	$1 + 2/3^s$	$1 + 2/3^s$	$1 - 1/3^s$
$d \equiv 6 \pmod{9}$	$1 + 2/3^s + 6/3^{2s}$	$1 + 2/3^s + 3\omega_E(3)/3^{2s}$	$1 - 1/3^s$

We will use this result, together with standard analytic techniques, to count cubic fields K with fixed $D(K)$ and varying $F(K)$. Such a result was given as [14, Proposition 6.3] and we give a version where the dependence of the error term on $D(K)$ is specified.

We also extend these results to $P_\Sigma > 1$, counting cubic fields with specified splitting types. The key result is where $\Sigma_p = \mathbb{Q}_p^3$ for each $p \mid P_\Sigma$, corresponding to a demand that each such p split completely in each cubic field being counted. Write $\mathcal{L}_3(P_\Sigma, d)$ for the set of cubic fields whose discriminant is $-k^2d/3$, $-3k^2d$, or $-27k^2d$, where k is any positive divisor of P_Σ . Thus the quadratic resolvent of every field in $\mathcal{L}_3(P_\Sigma, d)$ is $\mathbb{Q}(\sqrt{-3d})$.

Theorem 11 *With $\Sigma_p = \mathbb{Q}_p^3$ for each $p \mid P_\Sigma$ and $\mathcal{L}_3(P_\Sigma, d)$ defined as above, we have*

$$(11) \quad c_d 3^{\omega(P_\Sigma)} \Phi_{\Sigma,d}(s) = \frac{1}{2} M_{1,d}(s) \prod_{p \nmid 3dP_\Sigma} \left(1 + \frac{1 + \left(\frac{-3d}{p}\right)}{p^s} \right) + \sum_{E \in \mathcal{L}_3(P_\Sigma, d)} M_{2,E}(s) \prod_{p \nmid 3dP_\Sigma} \left(1 + \frac{\omega_E(p)}{p^s} \right)$$

provided that $\left(\frac{d}{p}\right) = 1$ for every prime $p \mid P_\Sigma$, and $\Phi_{\Sigma,d}(s) = 0$ otherwise. Here $\omega(P_\Sigma)$ denotes the number of prime divisors of P_Σ , and if $3 \mid P_\Sigma$ then the factors $M_{1,d}(s)$ and $M_{2,E}(s)$ are to be omitted.

The special cases $3 \mid P_\Sigma$ and/or $d \in \{1, -3\}$ are all allowed; if $d = 1$ then $\Phi_{\Sigma,d}(s)$ counts cyclic cubic fields, and if $d = -3$ then the fields in $\mathcal{L}_3(P_\Sigma, d)$ are cyclic.

Remark 12 *The explicit form of $\Phi_{\Sigma,d}$ stated in Theorem 11 will not be used in the proofs of our main results. The “average residue computation” that is required for our proofs will be obtained indirectly from results proved using geometry-of-numbers methods.*

All that is necessary for us is an asymptotic formula for the partial sums of $\Phi_{\Sigma,d}$ with bounds on the error; this is done in Theorem 13 by interpreting $\Phi_{\Sigma,d}$ as the weighted sum of incomplete Dedekind zeta functions and incomplete Artin L-functions, both having conductor $\ll_\Sigma d$.

We then immediately show that $\Phi_{d,\Sigma}(s)$ can be written as such a weighted sum in the case when Σ is an arbitrary finite collection of splitting types in the following steps:

- The splitting type at infinity: the sign of the discriminant of a cubic field is the same as the sign of the discriminant of its quadratic resolvent field. Hence, $\Phi_{\Sigma,d}$ will be 0 if the prescribed splitting type at infinity is incompatible with the sign of d , and unchanged if it is compatible.
- (21) – A prime p is partially split in K if and only if it is unramified in K and inert in $\mathbb{Q}(\sqrt{d})$. Therefore, if $(\frac{d}{p}) = 1$ for any such prime p then $\Phi_{\Sigma,d}(s) = 0$, and otherwise we eliminate all of the p -Euler factors from $\Phi_{\Sigma,d}(s)$.
- (1²1) – A prime p is partially ramified in K if and only if it is ramified in $\mathbb{Q}(\sqrt{d})$; therefore, $\Phi_{\Sigma,d} = 0$ if $p \nmid d$ for any such p , and otherwise $\Phi_{\Sigma,d}(s)$ is unchanged.
- (1³) – A prime p is totally ramified in K if and only if $p \mid f(K)$. Accordingly we remove the constant terms from the p -Euler factors.
- The remaining primes p are required to have splitting types (111) or (3). We handle the (111) case by applying equation (11) directly, and the (3) case by inclusion-exclusion.

In summary, the proof of Theorem 11 follows from a careful reading of [14] and [15]. The proof in [14] proceeds by setting $L = \mathbb{Q}(\sqrt{d}, \sqrt{-3})$, and enumerating those cyclic cubic extensions N_z/L which contain an appropriate K . By Kummer theory, any such extension is of the form $N_z = L(\sqrt[3]{\alpha})$. Writing $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ for squarefree integral coprime ideals \mathfrak{a}_0 and \mathfrak{a}_1 , the conductor $\mathfrak{f}(N/\mathbb{Q}(\sqrt{d}))$ is given (see [14, Theorem 3.7]) by $\mathfrak{a}_0\mathfrak{a}_1$ times a 3-adic factor, and this 3-adic factor depends on the solubility of $x^3 - \alpha$ modulo powers of 3.

The splitting conditions in K/\mathbb{Q} are equivalent to solubility in L of $x^3 - \alpha$ modulo P_Σ , or modulo $3P_\Sigma$ if $3 \mid P_\Sigma$, and hence the existing machinery of [14] is well suited to select for them. This is the reason that Theorem 11 has a very similar shape to Theorem 10.

We now proceed to explain the proof of Theorem 11 in more detail. As discussed above we may assume that $(\frac{d}{p}) = 1$ for every $p \mid P_\Sigma$, as otherwise $\Phi_{\Sigma,d}(s) = 0$. Write $\mathcal{P} = P_\Sigma$ if $3 \nmid P_\Sigma$, and $\mathcal{P} = 3P_\Sigma$ if $3 \mid P_\Sigma$.

Step 1 – Parametrization. Let $L = \mathbb{Q}(\sqrt{d}, \sqrt{-3})$ as before. In [14, Proposition 2.7], Cohen and Morra enumerate the set of cubic fields K with resolvent $\mathbb{Q}(\sqrt{d})$; each occurs as the cubic subextension (unique up to isomorphism) of a field $N_z = L(\sqrt[3]{\alpha})$ with $\alpha = \alpha_0u$, where α_0 is determined by the class in I/I^3 of the ideal (α) , and u represents an element \bar{u} of a 3-Selmer group $S_3(L)[T]$. The notation $[T]$ indicates that \bar{u} is annihilated by two particular elements of $\mathbb{F}_3[\text{Gal}(L/\mathbb{Q})]$ (one if $d = 1$ or $d = -3$).

A prime p splits in such a K if and only if: (1) it splits in $\mathbb{Q}(\sqrt{d})$, and (2) every prime \mathfrak{p}_z of L above p splits completely in N_z . Since L contains the third roots of unity, each such \mathfrak{p}_z of L splits completely in N_z if and only if $x^3 = \alpha$ is soluble in the completion of L at \mathfrak{p}_z . By Hensel's lemma, if $3 \nmid \mathfrak{p}_z$ this happens if and only if $x^3/\alpha \equiv 1 \pmod{*\mathfrak{p}_z}$ is soluble in L . Further, if α is coprime to 3, the primes above 3 split in N_z/L if and only if $x^3/\alpha \equiv 1$ is soluble modulo 9; to see this, note that if $v_3(\beta^3 - \alpha) > \frac{3}{2}$ with α, β integral, then $v_3((\beta')^3 - \alpha) > v_3(\beta^3 - \alpha)$ with $\beta' := \beta - \frac{\beta^3 - \alpha}{3\beta^2}$, yielding a sequence of β_i converging to a solution of $x^3 = \alpha$ in each 3-adic completion of L .

Step 2 – Conductors and Selmer group counting. In [14, Theorem 3.7], a formula is given for the conductor $\mathfrak{f}(N/\mathbb{Q}(\sqrt{d}))$. One writes $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ where \mathfrak{a}_0 and \mathfrak{a}_1 are integral coprime squarefree ideals, has $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$ for an ideal \mathfrak{a}_α of $\mathbb{Q}(\sqrt{d})$, and has that $\mathfrak{f}(N/\mathbb{Q}(\sqrt{d}))$ is the product of \mathfrak{a}_α times a complicated 3-adic factor, depending on the solubility of $x^3/\alpha \equiv 1 \pmod{*\mathfrak{p}_z^n}$ for ideals \mathfrak{p}_z over 3. They enumerate these 3-adic factors by inclusion-exclusion, involving a quantity

$$f_{\alpha_0}(\mathfrak{b}) = \#\{ \bar{u} \in S_3(L)[T], x^3/(\alpha_0u) \equiv 1 \pmod{*\mathfrak{b}} \text{ soluble in } L \},$$

where \mathfrak{b} ranges over (possibly fractional) powers of 3. This leads ([14, Proposition 4.6]) to a formula for $\Phi_d(s)$, where \mathfrak{b} ranges over a set of 3-adic ideals \mathcal{B} , and $f_{\alpha_0}(\mathfrak{b})$ appears as a counting function for the number of ideals with fixed conductor.

As discussed above, the splitting conditions in places in S are equivalent to requiring that $x^3/(\alpha_0 u) \equiv 1$ be soluble modulo other ideals. If $3 \nmid P_\Sigma$, multiply each \mathfrak{b} by \mathcal{P} . If $3 \mid P_\Sigma$, then 3 cannot ramify in any cubic field being counted: the sum over $\mathfrak{b} \in \mathcal{B}$ and all 3-adic factors disappear from $\Phi_d(s)$. In place of this sum, one takes \mathfrak{b} equal to \mathcal{P} .

The computation of $f_{\alpha_0}(\mathfrak{b})$ is carried out in Section 5 of [14], and also in Morra's thesis [25] where more detailed proofs are presented. One checks that, when varying \mathfrak{b} as above, the proofs are identical through Lemma 5.4.

We diverge somewhat in Lemma 5.6, which computes the size of $(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]$, where $Z_\mathfrak{b} := (\mathbb{Z}_L/\mathfrak{b}\mathbb{Z}_L)^*$. By the Chinese remainder theorem, the size of this group is multiplicative in \mathfrak{b} , so it suffices to carry out the computation for $\mathfrak{b} = (9)$ or $\mathfrak{b} = (p)$ for p a rational prime other than 3.

For F equal to L , $\mathbb{Q}(\sqrt{-3D})$, or \mathbb{Q} write $\Gamma_{F,\mathfrak{b}}$ for the multiplicative group of $\mathbb{Z}_F/(\mathbb{Z}_F \cap \mathfrak{b})$ modulo cubes, so that $\Gamma_{L,\mathfrak{b}} = Z_\mathfrak{b}/Z_\mathfrak{b}^3$ by definition. Then for $d \neq 1, -3$ a 'descent' argument similar to that presented in the proof of [15, Proposition 3.4] yields an isomorphism $\Gamma_{L,\mathfrak{b}}[T] \simeq \Gamma_{\mathbb{Q}(\sqrt{-3d}),\mathfrak{b}}[1 + \tau]$, and when $d = 1$ this holds (tautologically) as an equality. Similarly to [15, Lemma 5.6], we obtain

$$(12) \quad |(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]| = \begin{cases} |\Gamma_{\mathbb{Q}(\sqrt{-3d}),\mathfrak{b}}|/|\Gamma_{\mathbb{Q},\mathfrak{b}}| & \text{if } d \neq -3 \\ |\Gamma_{\mathbb{Q},\mathfrak{b}}| & \text{if } d = -3. \end{cases}$$

By direct computation, we readily check that the right side of (12) is 3 in all cases. (Recall that $(\frac{d}{p}) = 1$.) This yields a version of [14, Theorem 6.1], which gives an expression for $\Phi_d(s)$ in terms of characters of $G_\mathfrak{b} := (\text{Cl}_\mathfrak{b}(L)/\text{Cl}_\mathfrak{b}(L)^3)[T]$, with the following modifications:

- If $3 \nmid P_\Sigma$, then each ideal $\mathfrak{b} \in \mathcal{B}$ is multiplied by \mathcal{P} , and $|(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]|$ is multiplied by $3^{\omega(P_\Sigma)}$.
- If $3 \mid P_\Sigma$, then the sum over $\mathfrak{b} \in \mathcal{B}$ is replaced with the single choice $\mathfrak{b} = \mathcal{P}$; $(Z_\mathfrak{b}/Z_\mathfrak{b}^3)[T]$ has size $3^{\omega(P_\Sigma)}$.

Step 3 – Interpretation in terms of field counting. For $d \neq 1, -3$ the analogue of [15, Proposition 3.4] continues to hold, yielding a 'descent' isomorphism $G_\mathfrak{b} \simeq H_{\mathfrak{a}'}$, where $\mathfrak{a}' := \mathfrak{b} \cap \mathbb{Z}_{\mathbb{Q}(\sqrt{-3d})}$, and $H_{\mathfrak{a}'} := (\text{Cl}_{\mathfrak{a}'}(\mathbb{Q}(\sqrt{-3d}))/\text{Cl}_{\mathfrak{a}'}^3(\mathbb{Q}(\sqrt{-3d}))[1 + \tau]$. Then, Proposition 4.1 of [15] uses class field theory to establish a bijection between pairs of nontrivial characters of $G_\mathfrak{b}$ and cubic fields E . The same argument continues to hold, with the set of cubic fields E is expanded to those whose discriminant is equal to $-3d$ times the square of any rational integer divisor of \mathfrak{b} . The second half of the proof of Proposition 4.1 in [15] is unnecessary, as the conclusion follows more simply from Lemma 1.3 and equation (1.3) of earlier work of Nakagawa [26].

If $d = 1$ then as before the 'descent' isomorphism is replaced by an equality and we proceed identically. If $d = -3$ then we obtain $G_\mathfrak{b} \simeq \text{Cl}_{\mathfrak{a}'}(\mathbb{Q})/\text{Cl}_{\mathfrak{a}'}^3(\mathbb{Q})$ with $\mathfrak{a}' = \mathfrak{b} \cap \mathbb{Z}$ and a more direct application of class field theory establishes the required bijection.

This completes the proof.

We turn now to the analytic consequences. Let $d \neq -3$ be a fundamental discriminant and let Σ be a finite collection of splitting types such that $\mathcal{F}(\Sigma)_d$ is non-empty. In this case $\Phi_{\Sigma,d}(s)$ is a Dirichlet series with nonnegative coefficients, and we will see that it has a simple pole at $s = 1$ with positive residue. Define the quantity

$$N(\mathcal{F}(\Sigma)_d; Z) := \#\{K \in \mathcal{F}(\Sigma)_d : F(K) < Z\}.$$

Then we have the following consequence of Theorem 11 and its extension to arbitrary splitting conditions described after Remark 12.

Theorem 13 *Let d and Σ be as above. Then we have*

$$N(\mathcal{F}(\Sigma)_d; Z) = \text{Res}_{s=1}(\Phi_{\Sigma,d}(s)) \cdot Z + O_\epsilon(|\mathcal{L}_3(P_\Sigma, d)| |d|^{1/6} P_\Sigma^{1/3} Z^{2/3+\epsilon}).$$

Proof: As this is standard, we give a brief account. Write the left side as

$$\#\{K \in \mathcal{F}(\Sigma)_d : F(K) < Z\} = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \Phi_{\Sigma,d}(s) \frac{Z^s}{s} ds.$$

We then write each Euler product in $\Phi_{\Sigma,d}(s)$ as the product of a Dedekind zeta function $\zeta_{\mathbb{Q}(\sqrt{-3d})}(s)$ or an irreducible degree 2 Artin L -function, times a function holomorphic and bounded in any half plane $\Re(s) \geq \sigma_0 > \frac{1}{2}$.

As all of the L -functions have conductor $\ll |d|P_{\Sigma}^2$, the convexity bound yields

$$\left| \Phi_{\Sigma,d}(s) - \frac{\text{Res}_{s=1}(\Phi_{\Sigma,d}(s))}{s-1} \right| \ll |\mathcal{L}_3(P_{\Sigma}, d)| \cdot |d|^{1/4} ((1+t)P_{\Sigma})^{1/2},$$

uniformly in $\Re(s) = \sigma + it$ with $1 > \sigma \geq \sigma_0$.

Pick $T > 1$ to be optimized later. We shift the contour to the left, picking up one residue at 1, ending up with a sum of the following integrals: from $1 + \epsilon \pm iT$ to $1 + \epsilon \pm i\infty$; from $1 + \epsilon \pm iT$ to $\sigma_0 \pm iT$; and from $\sigma_0 - iT$ to $\sigma_0 + iT$. The residue gives the required main term, while the sum of these integrals is

$$\ll |\mathcal{L}_3(P_{\Sigma}, d)| \cdot \left(\frac{Z^{1+\epsilon}}{T} + Z^{\sigma_0} T^{1/2} |d|^{1/4} P_{\Sigma}^{1/2} \right).$$

The result now follows by optimizing the value of T to be $Z^{1/3}/(d^{1/6}P_{\Sigma}^{1/3})$. \square

Remark 14 *The error terms in the above theorem can clearly be improved by using subconvex estimates in place of the convexity bound. However, we do not state this improvement since we have no need for it.*

In the case $d = -3$, the same result and proof hold, except that $(\frac{-3d}{p}) = 1$ for all $p \nmid 3d$, so that $\Phi_{\Sigma, -3}(s)$ has a double pole at $s = 1$, as opposed to a simple pole. Therefore, as explained in [14, Corollary 7.4], we obtain the asymptotic (2) for $P_{\Sigma} = 1$, and for $P_{\Sigma} > 1$ this generalizes to

$$(13) \quad \#\{K \in \mathcal{F}(\Sigma) : D(K) = -3, F(K) < Z\} = C_1(\Sigma)Z(\log(Z) + C_2(\Sigma) - 1) + O(P_{\Sigma}^{1/3+\epsilon}Z^{2/3+\epsilon}),$$

where

$$\begin{aligned} C_1(\Sigma) &:= C_1 \prod_{\substack{p|P_{\Sigma} \\ p \neq 3}} \frac{p}{3p+6} \cdot \prod_{\substack{p|P_{\Sigma} \\ p=3}} \frac{1}{7} \\ C_2(\Sigma) &:= C_2 + \sum_{\substack{p|P_{\Sigma} \\ p \neq 3}} \frac{2 \log p}{p+2} + \sum_{\substack{p|P_{\Sigma} \\ p=3}} \frac{6}{7} \log 3. \end{aligned}$$

3 The asymptotics of cubic fields with bounded invariants

For a finite collection Σ of splitting types and positive real numbers Y and Z , define

$$N(\Sigma; Y, Z) := \{K \in \mathcal{F}(\Sigma) : 3 \neq |D(K)| < Y, F(K) < Z\}.$$

In this section, we compute asymptotics for $N(\Sigma; Y, Z)$. We will handle the ‘large Y case’ (i.e., large $\frac{\log Y}{\log Z}$) using Theorem 8 and the ‘small Y case’ using Theorem 13. Our error terms are strong enough that these ranges of Y overlap, yielding an asymptotic estimate for all Y and Z . Indeed, we obtain asymptotic formulas with different expressions for the main terms, which we may then conclude are equal.

These results will be used in the proofs of Theorems 2 and 4(c), where D and F are given equal weight. For parts (a) and (b) of Theorem 4 we will instead use a more direct approach so as to optimize the error terms. All of these proofs will be given in Section 4.

We begin with the following important uniformity estimate due to Davenport–Heilbronn (see, e.g., [2, Lemma 3.3]).

Lemma 15 *The number of cubic fields K such that $|\text{Disc}(K)| < X$ and $F(K) = f$ is bounded by $O_{\epsilon}(X^{1+\epsilon}/f^2)$.*

The key result of this section is the following proposition:

Proposition 16 *Let Σ be an finite collection of splitting types, and let Y and Z be positive real numbers. Then*

$$\begin{aligned} N(\Sigma; Y, Z) &= \left(\sum_{f < Z} C_1(\Sigma, f) \right) \cdot Y + O_\epsilon(Y^{5/6} Z^{2/3} + Y^{2/3+\epsilon} Z^{4/3} P_\Sigma^{2/3}); \\ N(\Sigma; Y, Z) &= \left(\sum_{\substack{|d| < Y \\ \text{fund.disc} \neq -3}} \text{Res}_{s=1} \Phi_{\Sigma, d}(s) \right) \cdot Z + O_{\epsilon, \Sigma} \left(Y^{7/6+\epsilon} Z^{2/3+\epsilon} P_\Sigma^{1/3+\epsilon} \right). \end{aligned}$$

Proof: To prove the first equality, we fiber by $F(K)$ and apply Theorem 8 (Davenport-Heilbronn), obtaining

$$\begin{aligned} N(\Sigma; Y, Z) &= \sum_{f < Z} N(\mathcal{F}(\Sigma)^{(f)}; Y) \\ &= \left(\sum_{f < Z} C_1(\Sigma, f) \right) \cdot Y + O \left(\sum_{f < Z} (f^{-1/3} Y^{5/6} + E(Y; f, \Sigma)) \right) \\ &= \left(\sum_{f < Z} C_1(\Sigma, f) \right) \cdot Y + O \left(Y^{5/6} Z^{2/3} + Y^{2/3+\epsilon} Z^{4/3} P_\Sigma^{2/3} \right), \end{aligned}$$

as necessary. To prove the second equality, we fiber by $D(K)$ and apply Theorem 13 (Cohen-Morra):

$$\begin{aligned} N(\Sigma; Y, Z) &= \sum_{\substack{|d| < Y \\ \text{fund.disc} \neq -3}} N(\mathcal{F}(\Sigma)_d; Z) \\ &= \left(\sum_{\substack{|d| < Y \\ \text{fund.disc} \neq -3}} \text{Res}_{s=1} \Phi_{\Sigma, d}(s) \right) \cdot Z + O_{\Sigma, \epsilon} \left(\sum_{\substack{|d| < Y \\ \text{fund.disc} \neq -3}} |\mathcal{L}_3(P_\Sigma, d)| |d|^{1/6} Z^{2/3+\epsilon} P_\Sigma^{1/3} \right) \\ &= \left(\sum_{\substack{|d| < Y \\ \text{fund.disc} \neq -3}} \text{Res}_{s=1} \Phi_{\Sigma, d}(s) \right) \cdot Z + O_{\Sigma, \epsilon} \left(Y^{7/6+\epsilon} Z^{2/3+\epsilon} P_\Sigma^{1/3+\epsilon} \right), \end{aligned}$$

where the bound on the sum over d of the sizes of $\mathcal{L}_3(P_\Sigma, d)$ follows from Lemma 15. This concludes the proof of the proposition. \square

Next, we estimate the leading constant in the right hand side of the first equation of Proposition 16.

Proposition 17 *We have*

$$\sum_{f < Z} C_1(\Sigma, f) = \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\text{D}(K)|_p |\text{F}(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p} \right)^2 \cdot Z + O_\epsilon(Z^{3/5+\epsilon});$$

Proof: Recall the Dirichlet series $L_1(\Sigma, s) := \sum_f C_1(\Sigma, f) f^{-s}$ from §2.1. It is easy to see that $L_1(\Sigma, s)$ is holomorphic to the right of $\Re(s) > 1/2$ with a simple pole at $s = 1$. Indeed, the shape of $C_1(\Sigma, f)$ described in (6) implies that $L_1(\Sigma, s)/\zeta(s)$ converges absolutely and is bounded uniformly in Σ and s to the right of $\Re(s) = \sigma$ for any $\sigma > 1/2$. Pick a real number T to be optimized later. Following the proof of Theorem 13, we have

$$\begin{aligned} (14) \quad \sum_{f < Z} C_1(\Sigma, f) &= \int_{\Re(s)=2} L_1(\Sigma, s)(s) \frac{Z^s}{s} ds \\ &= \text{Res}_{s=1} L_1(\Sigma, s) \cdot Z + O_\epsilon \left(\frac{Z^{1+\epsilon}}{T} + Z^{1/2+\epsilon} T^{1/4} \right), \end{aligned}$$

where we use the convex bound to estimate the growth of $\zeta(s)$ (and therefore $L_1(\Sigma, s)$) on the line $\Re(s) = 1/2 + \epsilon$. From the Euler product expansion of $L_1(\Sigma, s)$ derived in Proposition 9, it follows that the residue of $L_1(\Sigma, s)$ at $s = 1$ is given by

$$(15) \quad \text{Res}_{s=1} L_1(\Sigma, s) = \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\mathcal{D}(K)|_p |\mathcal{F}(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p}\right)^2.$$

The proposition follows by choosing $T = Z^{2/5}$. \square

The above two propositions have the following consequence:

Corollary 18 *We have*

$$\frac{1}{Y} \sum_{\substack{|d| < Y \\ \text{fund.disc} \neq -3}} \text{Res}_{s=1} \Phi_{\Sigma, d}(s) = \frac{1}{2} \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\mathcal{D}(K)|_p |\mathcal{F}(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p}\right)^2 + O_{\epsilon, \Sigma}(Y^{-1/12+\epsilon}).$$

Proof: The result follows from Propositions 16 and 17 by setting $Z = Y^{3/4}$. \square

In particular, the two estimates of Proposition 16 are asymptotic formulas for $Y > Z^{1+\epsilon}$ and $Y < Z^{2-\epsilon}$, respectively. Since these ranges overlap, we obtain the following result.

Theorem 19 *We have*

$$N(\Sigma; Y, Z) = \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\mathcal{D}(K)|_p |\mathcal{F}(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p}\right)^2 \cdot YZ + o_\Sigma(Y)Z + Yo_\Sigma(Z).$$

Proof: Combining the above results yields the claimed result with an error term

$$\ll_{\epsilon, \Sigma} (YZ)^\epsilon (YZ^{3/5} + Y^{11/12}Z + \min(Y^{2/3}Z^{4/3}, Y^{7/6}Z^{2/3})),$$

which is sufficiently small. \square

4 Ordering cubic fields by generalized discriminants

In this section we determine asymptotics for the number of cubic fields with bounded generalized discriminant, thereby proving Theorem 4. We also then determine which generalized discriminants I are such that the family of cubic fields ordered by I satisfy independence of primes, thus also proving Theorem 6.

For a generalized discriminant $I = |\mathcal{D}|^\alpha \mathcal{F}^\beta$, after normalizing we may assume that one of α or β equals 1 and the other is ≥ 1 . We handle each of the three possible cases in turn.

Proposition 20 *For a finite collection Σ of cubic splitting types and a real number $\beta > 1$, we have*

$$N_{|\mathcal{D}|F^\beta}(\Sigma; X) = L_1(\Sigma, \beta) \cdot X + L_2(\Sigma, 5\beta/6)X^{5/6} + O_{\epsilon, \beta}((X^{\frac{2}{\beta+1}+\epsilon} + X^{\frac{2}{3}+\epsilon})P_\Sigma^{2/3}),$$

with $L_1(\Sigma, \beta)$ and $L_2(\Sigma, 5\beta/6)$ as given in Proposition 9.

Proof: We fiber over $f \geq 1$ and write

$$N_{|\mathcal{D}|F^\beta}(\Sigma, X) = \sum_f N(\mathcal{F}(\Sigma)^{(f)}; f^{2-\beta}X) + O(X^{\frac{1}{\beta}} \log(X)),$$

where $N(\mathcal{F}(\Sigma)^{(f)}; f^{2-\beta}X)$ denotes the number of cubic fields $K \in \mathcal{F}(\Sigma)^{(f)}$ such that $|\text{Disc}(K)| < f^{2-\beta}X$, and the error term accounts for the pure cubic fields. For any $1 < Y \ll X^{1/\beta}$, by Lemma 15 we have

$$\sum_{f \geq Y} N(\mathcal{F}(\Sigma)^{(f)}; f^{2-\beta}X) \ll_{\epsilon} \sum_{f \geq Y} \frac{f^{2-\beta+\epsilon}X^{1+\epsilon}}{f^2} \ll_{\epsilon} \frac{X^{1+\epsilon}}{Y^{\beta-1-\epsilon}}.$$

For $f < Y$, by Theorem 8 we have

$$\sum_{f < Y} N(\mathcal{F}(\Sigma)^{(f)}; f^{2-\beta}X) = \sum_{f < Y} \left(\frac{C_1(\Sigma, f)}{f^{\beta}} X + \frac{C_2(\Sigma, f)}{f^{5\beta/6}} X^{5/6} + O(E(X/f^{\beta}, f, \Sigma)) \right).$$

The error term is bounded by

$$\begin{aligned} \sum_{k < \log_2 Y} \sum_{2^k \leq f < 2^{k+1}} E(X/f^{\beta}; f, \Sigma) &\ll \sum_{k < \log_2 Y} X^{2/3+\epsilon} (2^k)^{4/3-2\beta/3+\epsilon} P_{\Sigma}^{2/3} \\ &\ll X^{2/3+\epsilon} P_{\Sigma}^{2/3} \cdot \max(Y^{4/3-2\beta/3+\epsilon}, 1). \end{aligned}$$

Meanwhile, the two main terms are:

$$\begin{aligned} \sum_{f < Y} \frac{C_1(\Sigma, f)}{f^{\beta}} &= \sum_{f \geq 1} \frac{C_1(\Sigma, f)}{f^{\beta}} + O_{\beta}(Y^{1-\beta}) \\ &= L_1(\Sigma, \beta) + O_{\beta}(Y^{1-\beta}); \\ \sum_{f < Y} \frac{C_2(\Sigma, f)}{f^{5\beta/6}} &= \sum_{f \geq 1} \frac{C_2(\Sigma, f)}{f^{5\beta/6}} + O_{\beta}(Y^{1-5\beta/6}) \\ &= L_2(\Sigma, 5\beta/6) + O_{\beta}(Y^{1-5\beta/6}). \end{aligned}$$

Optimizing (in X aspect), we pick $Y = X^{\frac{1}{\beta+1}}$ and obtain the result. \square

Proposition 21 *For a finite collection Σ of cubic splitting types and a real number $\alpha > 1$, we have*

$$N_{|\text{D}|^{\alpha}\text{F}}(\Sigma; X) = \left(\sum_{d \text{ fund. disc} \neq -3} \frac{\text{Res}_{s=1} \Phi_{\Sigma, d}(s)}{|d|^{\alpha}} \right) \cdot X + O_{\epsilon, \alpha}((X^{3/(2\alpha+1)+\epsilon} + X^{2/3+\epsilon}) P_{\Sigma}^{1/3}).$$

Proof: We fiber over d and write

$$N_{|\text{D}|^{\alpha}\text{F}}(\Sigma, X) = \sum_{d \text{ fund. disc} \neq -3} N(\mathcal{F}(\Sigma)_d; X/|d|^{\alpha}),$$

Pick a real number $1 < Y \ll X^{1/\alpha}$ to be optimized later. For each fundamental discriminant d such that $|d| \geq Y$, the condition $|d|^{\alpha}f < X$ implies that $f < X/Y^{\alpha}$. Hence by Lemma 15 we have

$$\begin{aligned} \sum_{\substack{d \text{ fund. disc} \neq -3 \\ |d| \geq Y}} N(\mathcal{F}(\Sigma)_d; X/|d|^{\alpha}) &\leq \sum_{f < X/Y^{\alpha}} \#\{K \in \mathcal{F}(\Sigma)^{(f)} : |\text{Disc}(K)| < X^{1/\alpha} f^{2-1/\alpha}\} \\ &\ll \sum_{f < X/Y^{\alpha}} X^{\epsilon} \cdot (X/f)^{1/\alpha} \\ &\ll \frac{X^{1+\epsilon}}{Y^{\alpha-1}}. \end{aligned}$$

To estimate the main term, we use Theorem 13 to write

$$\sum_{\substack{d \text{ fund. disc} \neq -3 \\ |d| < Y}} N(\mathcal{F}(\Sigma)_d; X/|d|^{\alpha}) = \left(\sum_{\substack{d \text{ fund. disc} \neq -3 \\ |d| < Y}} \frac{\text{Res}_{s=1} \Phi_{\Sigma, d}(s)}{|d|^{\alpha}} \right) \cdot X + O(E),$$

where the error term E is easily bounded by breaking up the sum over d into dyadic ranges and using Lemma 15 to estimate the size of $\mathcal{L}_3(P_\Sigma, d)$:

$$\begin{aligned} E &\ll \sum_{\substack{d \text{ fund. disc} \neq -3 \\ |d| < Y}} |\mathcal{L}_3(P_\Sigma, d)| \cdot |d|^{1/6} P_\Sigma^{1/3} (X/|d|^\alpha)^{2/3+\epsilon} \\ &\ll X^{2/3+\epsilon} \max(Y^{7/6-2\alpha/3}, 1) P_\Sigma^{1/3}. \end{aligned}$$

Optimizing, we pick $Y = X^{2/(2\alpha+1)}$ and obtain the required result. \square

Theorem 22 *We have*

$$(16) \quad N_{|\mathbf{D}|F}(\Sigma; X) = \frac{1}{2} \left(\sum_{K \in \Sigma_\infty} \frac{1}{|\text{Aut}(K)|} \right) \prod_p \left(\sum_{K \in \Sigma_p} \frac{|\mathbf{D}(K)|_p |\mathbf{F}(K)|_p}{|\text{Aut}(K)|} \right) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X + o(X \log X).$$

Proof: Given $\epsilon > 0$, choose $\epsilon' < \epsilon$ so that the interval $[1, \sqrt{X}]$ may be divided exactly into $\frac{1}{2}(\epsilon'^{-1} + O(1)) \log X$ intervals of the form $[(1 + \epsilon')^k, (1 + \epsilon')^{k+1}]$, and write $Y_k := (1 + \epsilon')^k$ and $Z_k := X/(1 + \epsilon')^k$. By Theorem 19, we have that

$$N(\Sigma; Y_{k+1}, Z_k) - N(\Sigma; Y_k, Z_k) = C_1(\mathbf{DF}, \Sigma) \cdot \epsilon' X + o(Y_k) Z_k,$$

where $C_1(\mathbf{DF}, \Sigma)$ is the constant in (16), and the same is true with the roles of Y and Z reversed. Since every field counted by $N_{|\mathbf{D}|F}(\mathcal{F}(\Sigma); X)$ is counted in one of the above rectangles, we obtain

$$N_{|\mathbf{D}|F}(\mathcal{F}(\Sigma); X) \leq C_1(\mathbf{DF}, \Sigma) X \log X \cdot (1 + O(\epsilon) + \epsilon'^{-1} o_X(1)).$$

Choosing $\epsilon \rightarrow 0$ as $X \rightarrow \infty$, we obtain the result as an upper bound. To obtain the lower bound, proceed analogously, choosing $Z_k := X/(1 + \epsilon')^{k+1}$ and subtracting the $O(X)$ fields in $N(\Sigma; \sqrt{X}, \sqrt{X})$ which are counted twice. \square

Theorems 4 and 5 follow immediately from Propositions 20 and 21, and Theorem 22. We conclude by proving Theorems 2 and 6.

Proof of Theorem 2: For a prime $p > 3$ and étale cubic extension K_p of \mathbb{Q}_p , as noted previously we have that $p^2 \nmid \mathbf{D}(K)\mathbf{F}(K)$. Therefore, for a cubic field K , we have $\text{rad}(\text{Disc}(K)) = \mathbf{D}(K)\mathbf{F}(K)$ up to sign and bounded powers of 2 and 3. Let δ_2 and δ_3 be powers of 2 and 3, respectively. For $p = 2, 3$ let $S(\delta_p)$ be the set of cubic étale extensions K_p of \mathbb{Q}_p for which $\mathbf{D}(K_p)\mathbf{F}(K_p)$ has p -adic part δ_p , and let $\Sigma(\delta_2, \delta_3)$ be the finite collection of cubic splitting types defined by $\Sigma_2 = S(\delta_2)$, $\Sigma_3 = S(\delta_3)$, and $\Sigma_v = \Sigma_v^{\text{all}}$ for all other places v . Then we have

$$\begin{aligned} \#\{K \in \mathcal{F}(\Sigma) : C(K) < X, \mathbf{D}(K) \neq -3, \pm \text{Disc}(K) > 0\} &= N_{|\mathbf{D}|F}\left(\Sigma; \frac{\delta_2 \delta_3}{\text{rad}(\delta_2 \delta_3)} \cdot X\right) \\ &= \frac{1}{2\sigma_\pm} \mathcal{C}(\delta_2) \mathcal{C}(\delta_3) \prod_{p \geq 5} \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X \\ &\quad + o(X \log X), \end{aligned}$$

where $\sigma_+ = 6$ and $\sigma_- = 2$ are the sizes of the automorphism groups of \mathbb{R}^3 and $\mathbb{R} \times \mathbb{C}$, respectively, and

$$\mathcal{C}(\delta_2) = \left(1 - \frac{1}{2}\right)^2 \sum_{K_2 \in S(\delta_2)} \frac{\text{rad}(\delta_2)^{-1}}{|\text{Aut}(K_2)|}; \quad \mathcal{C}(\delta_3) = \left(1 - \frac{1}{3}\right)^2 \sum_{K_3 \in S(\delta_3)} \frac{\text{rad}(\delta_3)^{-1}}{|\text{Aut}(K_3)|}.$$

Summing over all δ_2 and δ_3 , we obtain

$$\#\{K \in \mathcal{F} : C(K) < X, \mathbf{D}(K) \neq -3, \pm \text{Disc}(K) > 0\} = \frac{1}{2\sigma_\pm} \prod_p \mathcal{C}(p) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X + o(X \log X),$$

where for any prime p , the quantity $\mathcal{C}(p)$ is defined to be

$$\mathcal{C}(p) := \sum_{K \in \Sigma_p^{\text{all}}} \frac{|\text{rad}(|D(K)|F(K))|_p}{|\text{Aut}(K)|}.$$

To compute these constants, we use the database of local fields available at lmfdb.org [21], which lists each quadratic or cubic ramified extension of \mathbb{Q}_2 and \mathbb{Q}_3 with its Galois group; we obtain that $\mathcal{C}(2) = 3$ and $\mathcal{C}(3) = 11/3$.

Finally, to count the contribution of the pure cubic fields, observe that we have

$$\sum_{D(K)=-3} C(K)^{-s} = -\frac{1}{2} \cdot 3^{-s} + \frac{3}{2} \cdot 3^{-s} \prod_{p \neq 3} \left(1 + \frac{2}{p^s}\right).$$

by [14, Proposition 7.3]. By an argument identical to that of Theorem 13 or [14, Proposition 7.4], we have

$$\#\{K \in \mathcal{F} : C(K) < X, D(K) = -3, \pm \text{Disc}(K) > 0\} = \frac{3}{10} \prod_p \left(1 + \frac{2}{p}\right) \left(1 - \frac{1}{p}\right)^2 \cdot X \log X + o(X \log X),$$

thereby completing the proof. \square

Proof of Theorem 6: For $\alpha \leq \beta$ this follows immediately from the shape of the leading asymptotics in parts (a) and (c) of Theorem 4. It remains to prove the result when $\alpha > \beta$, and as before we may assume that $\beta = 1$. For fixed $\epsilon > 0$ let $N(\epsilon)$ be the smallest positive integer such that the following inequality is satisfied:

$$(17) \quad \epsilon \cdot \frac{\text{Res}_{s=1} \Phi_{\Sigma^{\text{all}}, 5}}{5^\alpha} > \sum_{\substack{|d| > N(\epsilon) \\ \text{fund.disc.}}} \frac{\text{Res}_{d=1} \Phi_{\Sigma^{\text{all}}, d}}{|d|^\alpha}.$$

Such an $N(\epsilon)$ exists for each ϵ since the sum of $\text{Res}_{d=1}(\Phi_{\Sigma^{\text{all}}, d})/|d|^\alpha$ is convergent, as can be seen from Corollary 18 for example.

For each fundamental discriminant d with $3, 5 \neq |d| \leq N(\epsilon)$, now let $p_d \neq 7$ be a prime such that the splitting types of p_d at $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{d})$ differ. (For $d = 1$, we choose p_1 to be inert in $\mathbb{Q}(\sqrt{5})$.) Define $\Sigma_{p_d}^{(\epsilon)}$ to be the set of all étale cubic extensions of \mathbb{Q}_{p_d} whose quadratic resolvents are equal to $\mathbb{Q}(\sqrt{5}) \otimes \mathbb{Q}_{p_d}$. We then define the collection $\Sigma^{(\epsilon)}$ by taking $\Sigma_{p_d}^{(\epsilon)}$ as above, and choosing $\Sigma_p^{(\epsilon)} = \Sigma_p^{\text{all}}$ for p not equal to any of the p_d .

Then (17) holds with Σ^{all} replaced by $\Sigma^{(\epsilon)}$ and $|d| > N(\epsilon)$ replaced by $d \neq -3, 5$, as the newly imposed splitting conditions do not exclude any of the fields counted on the left, nor do they include any of the fields added to the right. Since $K \otimes \mathbb{Q}_7 \not\cong \mathbb{Q}_7^3$ for any K with resolvent $\mathbb{Q}(\sqrt{5})$, this implies that

$$0 < \lim_{X \rightarrow \infty} \frac{\#\{K \in \mathcal{F}(\Sigma^{(\epsilon)}) : D(K) \neq -3, D(K)^\alpha F(K) < X, K \otimes \mathbb{Q}_7 \cong \mathbb{Q}_7^3\}}{\#\{K \in \mathcal{F}(\Sigma^{(\epsilon)}) : D(K) \neq -3, D(K)^\alpha F(K) < X\}} < \frac{\epsilon}{1 + \epsilon} < \epsilon.$$

In particular, since 7 does not split in $\mathbb{Q}(\sqrt{5})$, the probability of the prime 7 splitting completely in $\mathcal{F}(\Sigma^{(\epsilon)})$ goes to 0 as ϵ tends to 0. Moreover, the probability that 7 splits completely in $\mathcal{F}(\Sigma^{\text{all}})$ is positive, since 7 splits completely a positive proportion of the time in cubic fields with resolvent, say, $\mathbb{Q}(\sqrt{-19})$. The result now follows from the fact that $\Sigma_7^{(\epsilon)}$ is constant for all ϵ . \square

5 Numerical data

As a double check on our work we numerically verified Theorem 11 (the explicit Dirichlet series counting cubic fields with local conditions, by quadratic resolvent), and the $\alpha = \beta = 1$ case of Theorem 4 (counting cubic fields with $|D|F < X$). Our code can be readily modified to cover additional cases of Theorem 4.

We used the PARI/GP programming language [27], and our source code and data may be downloaded from `thornef.github.io`: a program `cm-test.gp` to compute instances of Theorem 11, and compare against known data when possible; a program `cubic-count.gp` to generate the data below; and lists of cubic fields (`rcf-1500k.gp` and `icf-1000k.gp`) obtained from `lmfdb.org` [21].

For counting cubic fields with $|D|F < X$, the following table presents a comparison (for relatively small X) of the asymptotics proved in Theorem 4(c) with the data:

X	Theorem 4(c)	Actual Data
100	50	38
1000	748	629
10000	9977	9181
20000	21456	20044
30000	33502	31427

We note the apparent presence of one or more negative lower order terms. There are at least three possible explanations for the discrepancy between the data and the asymptotics:

- the negative secondary term in the Davenport-Heilbronn theorem (5);
- the exclusion of $D = -3$ from our counts, which is not ‘visible’ in the main term of Theorem 4(c);
- the natural tendency for asymptotics with logarithmic terms to have lower order terms without the logarithms, e.g. the divisor sum estimate $\sum_{n < X} d(n) = X \log X + (2\gamma - 1)X + O(\sqrt{X})$.

We leave a more detailed analysis for followup work.

Acknowledgments

It is a pleasure to thank Manjul Bhargava, Robert Lemke Oliver, and Takashi Taniguchi for helpful conversations. We are extremely grateful to the anonymous referee for a very thorough reading and many useful suggestions.

AS is supported by an NSERC Discovery Grant and a Sloan Research Fellowship. FT was partially supported by the National Science Foundation under Grant No. DMS-2101874, by the National Security Agency under Grant H98230-16-1-0051, and by grants from the Simons Foundation (Nos. 563234 and 586594).

Finally, this project was begun at the Palmetto Number Theory Series in Columbia, SC in December 2016, hosted by Matthew Boylan, Michael Filaseta, and FT. We would like to thank Boylan and Filaseta for hosting, and the NSF (Grant No. DMS-1601239) and NSA (Grant No. H98230-14-1-0151) for funding the conference.

References

- [1] S. A. Altug, A. Shankar, I. Varma, and K. H. Wilson. The number of D_4 -fields ordered by conductor. *J. Eur. Math. Soc. (JEMS)*, 23(8):2733–2785, 2021.
- [2] K. Belabas, M. Bhargava, and C. Pomerance. Error estimates for the Davenport-Heilbronn theorems. *Duke Math. J.*, 153(1):173–210, 2010.
- [3] K. Belabas and E. Fouvry. Discriminants cubiques et progressions arithmétiques. *Int. J. Number Theory*, 6(7):1491–1529, 2010.
- [4] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.
- [5] M. Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm052, 20, 2007.

- [6] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.
- [7] M. Bhargava and P. Harron. The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields. *Compos. Math.*, 152(6):1111–1120, 2016.
- [8] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.
- [9] M. Bhargava, A. Shankar, and X. Wang. Geometry-of-numbers methods over global fields I. *arXiv preprint 1512.03035*, 2015.
- [10] M. Bhargava, T. Taniguchi, and F. Thorne. Improved error estimates for the Davenport-Heilbronn theorems. *arXiv preprint 2107.12819*, 2021.
- [11] M. Bhargava and M. M. Wood. The density of discriminants of S_3 -sextic number fields. *Proc. Amer. Math. Soc.*, 136(5):1581–1587, 2008.
- [12] P. J. Cho and H. H. Kim. The smallest prime in a conjugacy class and the first sign change for automorphic L -functions. *Proc. Amer. Math. Soc.*, 149(3):923–933, 2021.
- [13] H. Cohen, F. Diaz y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of \mathbb{Q} . *Compositio Math.*, 133(1):65–93, 2002.
- [14] H. Cohen and A. Morra. Counting cubic extensions with given quadratic resolvent. *J. Algebra*, 325:461–478, 2011.
- [15] H. Cohen and F. Thorne. Dirichlet series associated to cubic fields with given quadratic resolvent. *Michigan Math. J.*, 63(2):253–273, 2014.
- [16] B. Datskovsky and D. J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.*, 386:116–138, 1988.
- [17] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.
- [18] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.
- [19] K. S. Kedlaya. Mass formulas for local Galois representations. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm021, 26, 2007. With an appendix by Daniel Gulotta.
- [20] J. Klüners. A counterexample to Malle’s conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.
- [21] LMFDB Collaboration, The. The L-functions and modular forms database. <http://www.lmfdb.org>, 2022.
- [22] G. Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.
- [23] G. Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.
- [24] G. Martin and P. Pollack. The average least character non-residue and further variations on a theme of Erdős. *J. Lond. Math. Soc. (2)*, 87(1):22–42, 2013.
- [25] A. Morra. *Comptage asymptotique et algorithmique d’extensions cubiques relatives*. PhD thesis, Université Bordeaux I, 2009.

- [26] J. Nakagawa. On the relations among the class numbers of binary cubic forms. *Invent. Math.*, 134(1):101–138, 1998.
- [27] PARI Group, The. *PARI/GP version 2.8.0*. Bordeaux, 2014. Available from <http://pari.math.u-bordeaux.fr/>.
- [28] P. Sarnak, S. W. Shin, and N. Templier. Families of L -functions and their symmetry. In *Families of automorphic forms and the trace formula*, Simons Symp., pages 531–578. Springer, [Cham], 2016.
- [29] A. Shankar, A. Södergren, and N. Templier. Sato-Tate equidistribution of certain families of Artin L -functions. *Forum Math. Sigma*, 7:Paper No. e23, 62, 2019.
- [30] A. Shankar, A. Södergren, and N. Templier. Central values of zeta functions of non-Galois cubic fields. *arXiv preprint arXiv:2107.10900*, 2022.
- [31] T. Taniguchi. Distributions of discriminants of cubic algebras. *arXiv preprint 0606109*, 2006.
- [32] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, 162(13):2451–2508, 2013.
- [33] T. Taniguchi and F. Thorne. An error estimate for counting S_3 -sextic number fields. *Int. J. Number Theory*, 10(4):935–948, 2014.
- [34] D. Terr. *The distribution of shapes of cubic orders*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley.
- [35] S. Türkelli. Connected components of Hurwitz schemes and Malle’s conjecture. *J. Number Theory*, 155:163–201, 2015.
- [36] J. Wang. Malle’s conjecture for $S_n \times A$ for $n = 3, 4, 5$. *Compos. Math.*, 157(1):83–121, 2021.
- [37] M. M. Wood. On the probabilities of local behaviors in abelian field extensions. *Compos. Math.*, 146(1):102–128, 2010.
- [38] A. Yang. *Distribution problems associated to zeta functions and invariant theory*. 2009. Thesis (Ph.D.)–Princeton University.