Invent. math. (2020) 219:701–778
https://doi.org/10.1007/s00222-019-00915-z

An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups

Lillian B. Pierce[1,2] ·
Caroline L. Turnage-Butterbaugh[3] ·
Melanie Matchett Wood[4]

Received: 4 March 2019 / Accepted: 2 August 2019 / Published online: 10 September 2019

Abstract We prove a new effective Chebotarev density theorem for Galois extensions $L/\mathbb{Q}$ that allows one to count small primes (even as small as an arbitrarily small power of the discriminant of L); this theorem holds for the Galois closures of "almost all" number fields that lie in an appropriate family of field extensions. Previously, applying Chebotarev in such small ranges required assuming the Generalized Riemann Hypothesis. The error term in this new Chebotarev density theorem also avoids the effect of an exceptional zero of the Dedekind zeta function of L, without assuming GRH. We give many different "appropriate families," including families of arbitrarily large degree. To do this, we first prove a new effective Chebotarev density theorem that requires a zero-free region of the Dedekind zeta function. Then we prove that almost

✉ Melanie Matchett Wood
mmwood@berkeley.edu

Lillian B. Pierce
pierce@math.duke.edu

Caroline L. Turnage-Butterbaugh
cturnageb@carleton.edu

1 Department of Mathematics, Duke University, 120 Science Drive, Durham, NC 27708, USA

2 Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA

3 Department of Mathematics and Statistics, Carleton College, 1 North College Street, Northfield, MN 55057, USA

4 Department of Mathematics, University of California, Berkeley, 970 Evans Hall # 3840, Berkeley, CA 94720-3840, USA

all number fields in our families yield such a zero-free region. The innovation that allows us to achieve this is a delicate new method for controlling zeroes of certain families of *non-cuspidal* L-functions. This builds on, and greatly generalizes the applicability of, work of Kowalski and Michel on the average density of zeroes of a family of *cuspidal* L-functions. A surprising feature of this new method, which we expect will have independent interest, is that we control the number of zeroes in the family of L-functions by bounding the number of certain associated fields with fixed discriminant. As an application of the new Chebotarev density theorem, we prove the first nontrivial upper bounds for ℓ-torsion in class groups, for all integers $\ell \geq 1$, applicable to infinite families of fields of arbitrarily large degree.

Mathematics Subject Classification 11R29 · 11R42 · 11R45 · 11N75

1 Overview

In this paper, we give unconditional effective Chebotarev density theorems for almost all number fields in certain families of fields, of a strength that previously required the assumption of GRH. We achieve this by a new method to control zeroes of non-cuspidal L-functions in families, and we give applications including the first non-trivial bounds on ℓ-torsion for all $\ell \geq 1$ in class groups in infinite families of fields of arbitrarily large degree. Our method requires only crude bounds on the number of fields in our families, allowing us to treat families of arbitrarily high degree and more general families than in [28], which gives ℓ-torsion bounds as a result of very precise counting of the families.

1.1 Historical introduction

For any fixed number field k and Galois extension L/k of number fields, consider the counting function of prime ideals of bounded norm in $\mathcal{O}_k$ and specified splitting type in L, defined by

$$\pi_{\mathscr{C}}(x, L/k) := \#\{\mathfrak{p} \subseteq \mathcal{O}_k : \mathfrak{p} \text{ unramified in } L, \left[\frac{L/k}{\mathfrak{p}}\right] = \mathscr{C}, \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x\}, \tag{1.1}$$

in which $\left[\frac{L/k}{\mathfrak{p}}\right]$ is the Artin symbol and $\mathscr{C}$ is any fixed conjugacy class in $\mathrm{Gal}(L/k)$. A central goal is to prove an asymptotic for $\pi_{\mathscr{C}}(x, L/k)$ that is valid for x as small as possible (relative to the absolute discriminant of the number field L), which is a regime in which many of the most interesting applications arise. The celebrated Chebotarev density theorem [75] provides the main term in the asymptotic,

$$\pi_{\mathscr{C}}(x, L/k) \sim \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x), \tag{1.2}$$

as $x \to \infty$, where $\mathrm{Gal}(L/k) = G$ and $\mathrm{Li}(x) = \int_2^x dt/\log t$. When $L = k = \mathbb{Q}$, this is the familiar Prime Number Theorem for $\pi(x)$; when $L = k$, this is the Prime Ideal Theorem, counting prime ideals $\mathfrak{p} \subset \mathcal{O}_k$ with $\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \le x$; when $k = \mathbb{Q}$ and $L = \mathbb{Q}(e^{2\pi i/q})$, this provides Dirichlet's theorem, counting rational primes $p \equiv a \pmod q$ with $p \le x$, for any $(a, q) = 1$.

An effective Chebotarev theorem, conditional on GRH, was proved by Lagarias and Odlyzko (with an improvement by Serre). Given any field extension $F/\mathbb{Q}$ we let $n_F = [F : \mathbb{Q}]$ and set $D_F = |\mathrm{Disc}\, F/\mathbb{Q}|$.

Theorem A (Conditional on GRH, [50, Theorem 1.1], [68, Théorème 4]) *There exists an effectively computable absolute constant $C_0 > 0$ such that for any Galois extension L/k of number fields, if GRH holds for the Dedekind zeta function ζ_L and $G := \mathrm{Gal}(L/k)$, then for any fixed conjugacy class $\mathscr{C} \subseteq G$ and every $x \ge 2$,*

$$\left|\pi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x)\right| \le C_0\frac{|\mathscr{C}|}{|G|}x^{1/2}\log(D_L x^{n_L}).$$

Lagarias and Odlyzko also proved an unconditional result:

Theorem B ([50, Corollary 1.3]) *There exist effectively computable absolute constants $C_1, C_2 > 0$ such that the following holds. Let L/k be a Galois extension of number fields with $G := \mathrm{Gal}(L/k)$. If $n_L > 1$ then $\zeta_L(s)$ has at most one zero $s = \sigma + it$ in the region*

$$\sigma \ge 1 - (4\log D_L)^{-1}, \qquad |t| \le (4\log D_L)^{-1}. \tag{1.3}$$

This exceptional zero, denoted β_0 if it exists, is real and simple. For all $x \ge \exp(10n_L(\log D_L)^2)$,

$$\left|\pi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x)\right| \le \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + C_1 x\exp(-C_2 n_L^{-1/2}(\log x)^{1/2}), \tag{1.4}$$

with the understanding that the β_0 term is present only if β_0 exists.

Theorem A holds for all $x \ge 2$. Theorem B requires at least that $x \ge D_L^{10n_L}$, a power of the discriminant that is too large for many applications. Consequently, citations of the Lagarias-Odlyzko work often use Theorem A and are hence conditional on GRH. Recent unconditional work that considers lower or upper bounds for $\pi_{\mathscr{C}}(x, L/k)$ instead of asymptotics also leads to thresholds for x that are too large for certain applications. For example, [77, Eqn. 1.6],

[78] prove lower bounds for $\pi_{\mathscr{C}}(x, L/k)$ that require x to be as large as a relatively large power of D_L; upper bounds for $\pi_{\mathscr{C}}(x, L/k)$ in the classic work [49, Thm. 1.4] require $x \geq C \exp\{(\log D_L)(\log\log D_L)(\log\log\log D_L)\}$, for some constant C, with improvements e.g. in [21,77].

1.2 New results I: effective Chebotarev theorems

We prove a new effective Chebotarev theorem that includes two breakthroughs: we remove the term corresponding to the exceptional zero in (1.4), and simultaneously we obtain an asymptotic with an effective error term, which in particular holds for x as small as D_L^{δ} for any small fixed $\delta > 0$ (for D_L sufficiently large). Both aspects are critical to applications such as our new bound for ℓ-torsion in class groups. It is unlikely that we could accomplish these goals for *all* fields without proving something significant toward GRH; instead, we prove that within appropriate families of fields, "almost all" of the fields satisfy such an effective Chebotarev theorem.

We first state an inexplicit, general version of our result for a "family" $\mathscr{F}(G)$ of fields (precise quantitative statements appear in Theorems 3.3, 3.9, 3.11, 3.13, 3.14, and Corollary 3.16 of Sect. 3). By a family $\mathscr{F}(G)$ we mean a set of degree n extensions $K/\mathbb{Q}$ with corresponding Galois closures $\tilde{K}/\mathbb{Q}$ having $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq G$ for a fixed transitive subgroup $G \subseteq S_n$. We use $\mathscr{F}(G; X)$ to denote those fields $K \in \mathscr{F}(G)$ with $D_K \leq X$. We also use Vinogradov's notation: $A \ll B$ denotes that there exists a constant C such that $|A| \leq CB$, and $A \ll_{\kappa} B$ denotes that C may depend on κ.

Theorem 1.1 *Fix an appropriate family $\mathscr{F}(G)$ (described explicitly in Sect. 1.2.1), and constants $A \geq 2$ and $\varepsilon > 0$. Then there exist constants $0 < \tau < \beta$ and $\kappa_1, \kappa_2, \kappa_3 > 0$, such that for all $X \geq 1$ we have $|\mathscr{F}(G; X)| \gg X^{\beta}$, and aside from at most $\ll_{\mathscr{F},A,\varepsilon} X^{\tau+\varepsilon}$ possible exceptions, each field $K \in \mathscr{F}(G; X)$ has the property that for every conjugacy class $\mathscr{C} \subseteq G$,*

$$\left| \pi_{\mathscr{C}}(x, \tilde{K}/\mathbb{Q}) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x) \right| \leq \frac{|\mathscr{C}|}{|G|} \frac{x}{(\log x)^A}, \tag{1.5}$$

for all

$$x \geq \kappa_1 \exp\{\kappa_2 (\log\log(D_{\tilde{K}}^{\kappa_3}))^{5/3} (\log\log\log(D_{\tilde{K}}^2))^{1/3}\}. \tag{1.6}$$

In comparison to Theorem B, for each field to which this result applies, this theorem removes the effect of the possible exceptional zero on the error term, and holds for x as small as an arbitrarily small power of $D_{\tilde{K}}$ (and hence of D_K), capabilities critical for many applications.

1.2.1 The appropriate families of fields

In general, we construct a set (or "family") of fields as follows. For a number field k, we let

$$Z_n(k, G; X) = \{K/k : K \subset \bar{\mathbb{Q}}, \deg K/k = n, \mathrm{Gal}(\tilde{K}/k) \simeq G, \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathrm{Disc}\, K/k \leq X\},$$

where $\tilde{K}$ is the Galois closure of K over k, the Galois group is considered as a permutation group on the n embeddings of K in $\overline{\mathbb{Q}}$, and the isomorphism with G is one of permutation groups. We let $Z_n(k, G) = Z_n(k, G; \infty)$. For our main results we will work over $\mathbb{Q}$, and study families of the form $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, defined to be the subset of those fields $K \in Z_n(\mathbb{Q}, G; X)$ such that for each rational prime p that is tamely ramified in K (i.e. those p not dividing any of the exponents of their factorization into prime ideals in the ring of integers of K), the inertia group in $\mathrm{Gal}(\tilde{K}/k)$ of every prime ideal $\wp$ of $\tilde{K}$ dividing p is generated by an element of $\mathscr{I}$, where $\mathscr{I}$ specifies one or more conjugacy classes in G. The use of ramification restrictions will play a large role in our method of proof.

The most general families we treat are degree n extensions with square-free discriminant, which are a positive proportion of all degree n fields for $n \leq 5$, and conjecturally so for $n \geq 6$. (These families are recorded in entries (3), (4), (6) in the lists below; square-free discriminant corresponds to $\mathscr{I}$ being transpositions, as explained in Sect. 2.3.) We give further examples to show the range of the method. We prove, unconditionally, that Theorem 1.1 applies to the following families $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ of fields:

(1) G a cyclic group of order $n \geq 2$, with $\mathscr{I}$ comprised of all generators of G (equivalently every rational prime that is tamely ramified in K is totally ramified).
(2) $n = p$ an odd prime, $G = D_p$ the order $2p$ dihedral group of symmetries of a regular p-gon, $\mathscr{I}$ being the conjugacy class of order 2 elements.
(3) $n = 3$, $G \simeq S_3$, $\mathscr{I}$ is transpositions.
(4) $n = 4$, $G \simeq S_4$, $\mathscr{I}$ is transpositions.
(5) $n = 4$, $G \simeq A_4$, $\mathscr{I}$ the two conjugacy classes in A_4 of order 3 elements.

This is the content of Theorem 3.3. Note for family (2) that asymptotic counting of the fields is essentially equivalent to knowing the exact average size of p-torsion of class groups of quadratic fields (and thus is open and very difficult). Our method does not require this counting.

We furthermore prove, conditional on the strong Artin conjecture and (in some cases certain hypotheses for counting number fields), that Theorem 1.1 applies to the following families of fields:

(6) $n \geq 5$, $G \simeq S_n$, $\mathscr{I}$ is transpositions (Theorems 3.9 and 3.11).
(7) $n \geq 5$, $G \simeq A_n$, no ramification restriction (Theorem 3.13).
(8) $G \subseteq S_n$ a transitive simple group, no ramification restriction (Theorem 3.14).

In addition, in Corollary 3.16 we record quantitative results for counting certain types of primes.

1.2.2 The proof strategy

To describe our strategy to prove Theorem 1.1 we define the notion of a δ-exceptional field:

Property 1.2 (δ-exceptional field) *For a fixed $0 < \delta < 1/2$, a number field K is* δ-exceptional *precisely when the Dedekind zeta function of the Galois closure $\tilde{K}$ of K over $\mathbb{Q}$ has the property that $\zeta_{\tilde{K}}(s)/\zeta(s)$ has a zero in the region $[1-\delta, 1] \times [-(\log D_{\tilde{K}})^{2/\delta}, (\log D_{\tilde{K}})^{2/\delta}]$.*

(Under GRH, no field is δ-exceptional for any $0 \leq \delta < 1/2$.) Our first step toward Theorem 1.1 is to prove the following (for a quantitative version over any fixed number field k, see Theorem 3.1):

Theorem 1.3 (Effective Chebotarev for non-δ-exceptional fields) *For every integer $n \geq 1$, and every transitive group $G \subseteq S_n$, for every $A \geq 2$ and every $0 < \delta \leq 1/(2A)$, there exist real numbers $D_0, \kappa_1, \kappa_2, \kappa_3$ (depending on δ, n, A) such that the following holds: for any extension $K/\mathbb{Q}$ with $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq G$ such that $D_{\tilde{K}} \geq D_0$ and $K/\mathbb{Q}$ is not δ-exceptional, we have that for any conjugacy class $\mathscr{C} \subseteq G$, (1.5) holds for all x satisfying (1.6).*

Theorem 1.1 relies on the following crucial step: we prove that within appropriate families, for sufficiently small δ, almost all fields are not δ-exceptional.[1] We achieve this by developing a new method for controlling zeroes of certain families of non-cuspidal L-functions. Previously, work of Kowalski and Michel [45] provided density results for zeroes within appropriate families of cuspidal L-functions. But we require zero-free regions for Dedekind zeta functions of Galois fields, and these correspond (in some cases conjecturally) to automorphic L-functions that are *not cuspidal*. This restriction of [45] to the cuspidal case has been a significant barrier in many previous applications (such as an effective prime ideal theorem in [17], or [16]; see Remark 5.9). We

[1] See also Sect. 4.10 on an unconditional approach to rule out exceptional zeroes in the standard zero-free region for $\zeta_L(s)$, and thus remove the β_0 term in (1.4), for extensions with no quadratic subfields. However, that approach does not rule out the extensions being δ-exceptional, and in particular, does not lead to an effective Chebotarev theorem that can count primes small enough for our purposes.

expect that our new approach to proving density results for zeroes in a family of non-cuspidal L-functions will have many further applications.

Precisely, let G be a fixed transitive subgroup of S_n and let $\rho_0, \rho_1, \ldots, \rho_s$ denote the irreducible representations of G, with ρ_0 being the trivial representation. Then for each $K \in Z_n(\mathbb{Q}, G; X)$, we may write $\zeta_{\tilde{K}}(s)$ as a product of Artin L-functions

$$\zeta_{\tilde{K}}(s) = \zeta(s) \prod_{i=1}^{s} L(s, \rho_i, \tilde{K}/\mathbb{Q})^{\dim \rho_i}. \tag{1.7}$$

In particular, consider a set $\mathscr{F}(X)$ of fields $K \in Z_n(\mathbb{Q}, G; X)$ with distinct Galois closures $\tilde{K}$ over $\mathbb{Q}$, and denote the set of Galois closures by $\tilde{\mathscr{F}}(X)$. For each field $\tilde{K} \in \tilde{\mathscr{F}}(X)$ and each representation ρ_j, there is an associated cuspidal automorphic representation $\pi_{\tilde{K},j}$ of $\mathrm{GL}(m_j)/\mathbb{Q}$ (in some cases conditional on the Strong Artin Conjecture), and then $L(s, \pi_{\tilde{K},j}) = L(s, \rho_j, \tilde{K}/\mathbb{Q})$. For each $1 \leq j \leq s$, we let $\mathscr{L}_j(X)$ denote the set of cuspidal automorphic representations $\pi_{\tilde{K},j}$ of $\mathrm{GL}(m_j)/\mathbb{Q}$ associated to the fields $\tilde{K} \in \tilde{\mathscr{F}}(X)$ and the representation ρ_j. We show using [45] that for each j, $\mathscr{L}_j(X)$ has the property that aside from at most a possible small "bad" exceptional subset, each representation $\pi \in \mathscr{L}_j(X)$ is such that its associated L-function $L(s, \pi)$ is zero-free in an appropriate region. (Of course, if GRH is true, there are no such exceptional L-functions, but we are working without GRH.) In order to deduce that amongst the Dedekind zeta functions $\zeta_{\tilde{K}}(s)$ for $\tilde{K} \in \tilde{\mathscr{F}}(X)$, almost all of them also possess this zero-free region, we need to build up the products as in (1.7), and we need to understand the following question: given a representation $\pi \in \mathscr{L}_j(X)$ (i.e. possibly a "bad" exceptional representation), how many fields $\tilde{K} \in \tilde{\mathscr{F}}(X)$ can have the property that $L(s, \rho_j, \tilde{K}/\mathbb{Q}) = L(s, \pi)$?

This is subtle, and relies on delicate properties of the families considered. At its heart the question is: for a fixed irreducible representation ρ_i of G, for how many fields $K_1, K_2 \in \mathscr{F}(X) \subseteq Z_n(\mathbb{Q}, G; X)$ can we have $L(s, \rho_i, \tilde{K}_1/\mathbb{Q}) = L(s, \rho_i, \tilde{K}_2/\mathbb{Q})$? We transform this into a question of counting how many fields $K_1, K_2 \in \mathscr{F}(X)$ have fixed fields $\tilde{K}_1^H = \tilde{K}_2^H$, where $H = \mathrm{Ker}(\rho_i)$ (see Proposition 6.3). A challenge then appears: for certain groups G, is it possible that such collisions can occur amongst a positive proportion of $K \in Z_n(\mathbb{Q}, G; X)$? (If so, a positive proportion of these fields could have $\zeta_{\tilde{K}}(s)$ containing a factor that is not zero-free in the desired region.)

For certain G, the answer is yes (see Sect. 6.3.2). In contrast, we show that for the groups G and the corresponding families of fields we construct in our main theorems, the answer is no. Precisely, we define each family $\mathscr{F}(X) \subseteq Z_n(\mathbb{Q}, G; X)$ according to carefully chosen ramification restrictions on tamely ramified primes, and within these carefully constructed families we can transform the problem of counting fields that share a certain fixed field into

a problem of counting number fields of degree n with *fixed* discriminant. This method of constructing families of fields so that we can control the zeroes of associated L-functions by counting number fields is a key innovation of this paper.

Within our chosen families, by counting fields of fixed discriminant, we ultimately show that such collisions of the fixed fields must be relatively rare. We can then prove that aside from at most a possible "small" exceptional subset of $\mathscr{F}(X)$, each field has the property that its Dedekind zeta function is zero-free in an appropriate region.

In general, our approach can be seen as a new strategy that vastly generalizes the applicability of the result of Kowalski and Michel to families of automorphic L-functions corresponding not just to cuspidal automorphic representations but also to isobaric automorphic representations. We expect this new method will be relevant to other problems of interest.

1.3 New results II: counting number fields

Our new effective Chebotarev theorem for families of fields relies on quantitative counts for number fields in two ways. First, we must bound from above the number of fields in the family that have a fixed discriminant; second we must bound from below the number of fields in the family with bounded discriminant. In general, such questions lie in the arena of Malle's conjecture [52] and the Malle-Bhargava principle [88, Section 10], and many questions remain open.

Definition 1.4 Within a certain family $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$, we say a subset E has *density zero* if for some $\gamma > 0$ and some $c_1 > 0$, for all $X \geq 1$,

$$|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)|/|E \cap Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| \geq c_1 X^{\gamma}.$$

Each of our main results takes the form of an effective Chebotarev density theorem that holds for each field within a family of fields, except for fields belonging to a possible subfamily of density zero. In all cases, proving an upper bound for $|E \cap Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)|$ is a significant part of our new work; in many cases, proving a lower bound for $|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)|$ is also a significant part of our new work.

For certain of the families of fields we consider, we prove the first recorded lower bounds. For example, we prove the following general result, from which we deduce the first lower bound in the literature for $|Z_n(\mathbb{Q}, A_n; X)|$ that grows like a power of X (Theorem 2.6).

Theorem 1.5 *Fix an integer $n \geq 2$ and a transitive subgroup $G \subset S_n$. Suppose $f(X, T_1, \ldots, T_j) \in \mathbb{Q}[X, T_1, \ldots, T_j]$ is a regular polynomial of total degree*

d in the T_i and of degree n in X with transitive Galois group $G \subset S_n$ over $\mathbb{Q}(T_1, \ldots, T_j)$. Then, for every $X \geq 1$ and every $\varepsilon > 0$,

$$|Z_n(\mathbb{Q}, G; X)| \gg_{f,\varepsilon} X^{\frac{1-|G|^{-1}}{d(2n-2)}-\varepsilon}.$$

Note that a recent paper of Dèbes [22] proves an analogous result for counting the degree $|G|$ Galois extensions in $\mathbb{Z}_{|G|}(\mathbb{Q}, G; X)$ rather than the degree n extensions we consider in Theorem 1.5 (or equivalently, only in the case that G is simply transitive).

In a different direction, as mentioned above, at a key step of extending the Kowalski-Michel zero density theorem to our setting (related to bounding $|E \cap Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)|$ from above), we require an upper bound for how many fields have any given *fixed* discriminant. To make things precise, we define the following property (always defining extensions within $\overline{\mathbb{Q}}$):

Property 1.6 ($\mathbf{D}_n(G, \varpi)$) *Let $n \geq 2$ be fixed and let G be a fixed transitive subgroup of S_n. We say that property $\mathbf{D}_n(G, \varpi)$ holds if for every fixed integer $D > 1$ and for every $\varepsilon > 0$ there exist at most $\ll_{n,G,\varepsilon} D^{\varpi+\varepsilon}$ fields $K/\mathbb{Q}$ of degree n and $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq G$ such that $D_K = D$. Moreover, we say that property $\mathbf{D}_n(\varpi)$ holds if for every fixed integer $D > 1$ and for every $\varepsilon > 0$ there exist at most $\ll_{n,\varepsilon} D^{\varpi+\varepsilon}$ fields $K/\mathbb{Q}$ of degree n such that $D_K = D$.*

For appropriate families, we can control $|E \cap Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)|$ if we can prove Property $\mathbf{D}_n(G, \varpi)$ for a sufficiently small ϖ. In particular we prove new results for $\mathbf{D}_4(A_4, \varpi)$, $\mathbf{D}_5(\varpi)$, and $\mathbf{D}_p^{\mathscr{J}}(D_p, \varpi)$, in the latter case assuming a certain ramification restriction.

The way Property $\mathbf{D}_n(\varpi)$ arises in our work on families of automorphic L-functions appears to be completely new. But it is actually the subject of a well-known conjecture which occupies a rather central role in number theory. Specifically, Duke [26, § 3] and Ellenberg and Venkatesh [29, Conjecture 1.3] conjecture:

Conjecture 1.7 (Discriminant Multiplicity Conjecture) *For each $n \geq 2$, $\mathbf{D}_n(0)$ holds.*

Of course, $\mathbf{D}_2(0)$ holds; for $n \geq 3$, much less is known, and results toward Conjecture 1.7 would have strong implications. First, the "pointwise" counts encapsulated in Property $\mathbf{D}_n(\varpi)$ relate to "average" counts for the number of extensions of degree n with bounded discriminant. In one direction, this is trivial: Property $\mathbf{D}_n(\varpi)$ immediately implies there are at most $\ll_{n,\varepsilon} X^{1+\varpi+\varepsilon}$ degree n extensions of $\mathbb{Q}$ with discriminant at most X. It may be surprising that there is also an implication in the other direction; this has been proved by Ellenberg and Venkatesh [29, Prop. 4.8].

Second, questions about $\mathbf{D}_n(\varpi)$ are directly connected to questions about ℓ-torsion in class groups, for primes ℓ. As just one example (see Duke [25]), quartic fields of fixed discriminant $-q$ (q prime) can be explicitly classified by odd octahedral Galois representations of conductor q, and the number of such fields can be expressed as in [38] as an appropriate average of the number of 2-torsion elements in the class groups of cubic number fields of discriminant $-q$. More generally, as noted in [29, p. 164], if Conjecture 1.7 holds (for all n), then it implies the main pointwise conjecture, Conjecture 7.1, for upper bounds for ℓ-torsion in class groups (for all n, ℓ). The way we employ property $\mathbf{D}_n(\varpi)$ in the present work is in some sense more efficient, since to study ℓ-torsion (for all $\ell \geq 1$) in class groups of degree n_0 fields we only require information about $\mathbf{D}_n(\varpi)$ for $n = n_0$, not for all n.

1.4 New results III: applications

We expect that the new effective Chebotarev theorems for families of fields will have many applications, and we exhibit two. First, we prove nontrivial bounds for ℓ-torsion, for all integers $\ell \geq 1$, in class groups of "almost all" fields in each of the families to which our Chebotarev theorems apply (Theorem 7.2). In many cases, these are the first ever nontrivial bounds for ℓ-torsion, and in particular the first that apply to families of fields of arbitrarily large degree. As a second (related) application, we prove a result on the density of number fields with small generators, spurred by a question of Ruppert (Theorem 8.2). Further applications will be described in later work.

1.5 Organization of the paper

In Part I, we state and prove the results we require for counting number fields, both with bounded discriminant and with fixed discriminant. In Part II, we turn to the Chebotarev theorems: in Sect. 3 we state quantitative versions of all the effective Chebotarev theorems; in Sect. 4 we prove the quantitative version of Theorem 1.3, and in Sects. 5 and 6 we prove the quantitative versions of Theorem 1.1. In Part III, we treat the two applications mentioned above.

Contents

Part I: Counting number fields

2 Counting families of fields

As described in Sect. 1.3, we require results counting number fields, and we prove those in this section. Our principal concern is families of the form

$Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, defined to be the subset of those fields $K \in Z_n(\mathbb{Q}, G; X)$ such that for each rational prime p that is tamely ramified in K, an inertia group for p is generated by an element of $\mathscr{I}$. We require an upper bound for $|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)|$, which can be an overestimate, a lower bound for $|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)|$, which we aim to make as sharp as currently feasible, and upper bounds on the number of fields in $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ of discriminant D.

2.1 Cyclic fields

The strategy for counting cyclic extensions goes back to Cohn [19]; see [32, 51,87,89] for results counting abelian extensions of arbitrary degree. Let G be cyclic of order $n \geq 2$ and let g denote the smallest prime divisor of n. Then we have (see, e.g. [89]) that

$$|Z_n(\mathbb{Q}, G; X)| \sim cX^{\frac{1}{n-n/g}} \tag{2.1}$$

for a certain constant $c = c(n) > 0$. We require the following refinement:

Proposition 2.1 (Cyclic groups) *Let $n \geq 2$ be fixed and let G be a cyclic group of order n. Let $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ count those fields $K \in Z_n(\mathbb{Q}, G; X)$ such that every rational prime that ramifies tamely in K is totally ramified in K, that is, the inertia group is generated by an element that is of full order in G. Then there exists a constant $c_n > 0$ such that*

$$|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| \sim c_n X^{\frac{1}{n-1}}. \tag{2.2}$$

Furthermore, Property $\mathbf{D}_n(G, 0)$ holds.

Remark 2.2 If $|G| = n$ is prime then $1/(n - n/g) = 1/(n - 1)$. However, when $|G| = n$ is not prime then $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ is itself of density zero in $Z_n(\mathbb{Q}, G; X)$, by comparison of (2.1) and (2.2).

Proof Let $a_1 = 1$ and for $m \geq 2$, let a_m be $|\operatorname{Aut}(G)|$ times the number of fields counted by $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ with absolute discriminant m. We define a Dirichlet series $A(s) := \sum_{m \geq 1} a_m m^{-s}$, and by class field theory and now standard arguments we have

$$A(s) = P(s) \prod_{p \equiv 1 \pmod{n}} (1 + \phi(n) p^{-(n-1)s}), \tag{2.3}$$

where $P(s)$ is a product over $p|n$ of polynomials in p^{-s}. Briefly, by class field theory we are counting certain homomorphisms from the idèle class group to G, by [87, Lemma 4.2] we can replace the idèle class group with a product

of p-adic units, and then we can easily count the local homomorphisms (see, e.g. [87, Section 4], for a similar analysis in a more difficult case).

When a_m is non-zero, we have $a_m \leq C_n \phi(n)^{\omega(m)}$ where $\omega(m)$ is the number of distinct prime divisors of m and C_n is a constant depending only on n. (In particular, C_n can be bounded above by the sum of the absolute values of all coefficients of the polynomial factors in the finite product $P(s)$.) Thus $a_m \ll_{n,\varepsilon} m^{\varepsilon}$ for any $\varepsilon > 0$, proving Property $\mathbf{D}_n(G; 0)$.

For comparison to $A(s)$ we consider the product $B(s)$ over all Dirichlet characters defined modulo n, given for $\Re(s) > 1$ by

$$B(s) = \prod_{\chi} L(s, \chi) = \prod_{\chi} \prod_{p} (1 - \chi(p) p^{-s})^{-1}$$

which has a pole of order 1 at $s = 1$ and otherwise may be analytically continued as a holomorphic function. Writing the Euler product as $\prod_p \mu_p(s)^{-1}$, note that $\mu_p(s) = 1 - \sum_{\chi} \chi(p) p^{-s} + O(p^{-2s})$; by orthogonality of characters, the coefficient $\sum_{\chi} \chi(p) = \phi(n)$ if $p \equiv 1 \pmod{n}$ and zero otherwise. We can then check that $A(s)/B((n-1)s)$ is holomorphic in $\Re(s) > (2(n-1))^{-1}$. Thus $A(s)$ has a meromorphic continuation in $\Re(s) > (2(n-1))^{-1}$ with only a simple pole at $s = (n-1)^{-1}$; moreover $A(s)$ inherits a standard convexity estimate from $B(s)$ (see e.g. [42, Lemma 5.2, Thm. 5.23]). So, by the main term in a standard Tauberian theorem (see for example [18, Thm. A.1] and [60, Section 6.4]), we have

$$|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| = c_n X^{1/(n-1)} + o(X^{1/(n-1)}),$$

for a certain constant c_n. □

2.2 Dihedral groups D_p

For p an odd prime, let D_p be the order $2p$ group of symmetries of the vertices of a regular p-gon. Klüners [43, Theorem 3.5] obtained the lower bound $|Z_p(\mathbb{Q}, D_p; X)| \gg X^{2/(p-1)}$ predicted by Malle's conjecture [52]. Klüners also showed that Malle's conjectured upper bound $X^{2/(p-1)+\varepsilon}$ follows from a special case of the Cohen-Lenstra heuristics [43, Thm. 2.5], as well as proving [43, Theorem 2.7] an unconditional upper bound $|Z_p(\mathbb{Q}, D_p; X)| \ll_{\varepsilon} X^{3/(p-1)+\varepsilon}$. This has recently been improved by Cohen and Thorne [20, Thm 1.1], based on nontrivial bounds of [28] for averages of ℓ-torsion over quadratic fields, to

$$|Z_p(\mathbb{Q}, D_p; X)| \ll_{\varepsilon} X^{\frac{3}{p-1} - \frac{1}{p(p-1)} + \varepsilon}. \tag{2.4}$$

We require a lower bound that includes a ramification restriction. We let Property $\mathbf{D}_p^{\mathscr{I}}(D_p, \varpi)$ be the analog of Property $\mathbf{D}_p(D_p, \varpi)$ in which we only count D_p-fields and with the ramification restriction $\mathscr{I}$ for all tamely ramified primes.

Proposition 2.3 (Dihedral group D_p of order $2p$) *For p an odd prime, let D_p act on the p vertices of the regular p-gon in the usual way, and let $Z_p^{\mathscr{I}}(\mathbb{Q}, D_p; X)$ count those fields $K \in Z_p(\mathbb{Q}, D_p; X)$ with the following ramification restriction $\mathscr{I}$: every rational prime that ramifies tamely in K has inertia group generated by an element in the conjugacy class $[(2\ \ p)(3\ \ p-1)\cdots(\frac{p+1}{2}\ \ \frac{p+3}{2})]$ of reflections. Then $|Z_p^{\mathscr{I}}(\mathbb{Q}, D_p; X)| \gg_p X^{\frac{2}{p-1}}$.*

Further, $\mathbf{D}_p^{\mathscr{I}}(D_p, 1/(p-1))$ holds. More generally, if we know that for all quadratic fields L we have $|\mathrm{Cl}_L[p]| = O_p(D_L^b)$ for a certain exponent $b > 0$, then $\mathbf{D}_p^{\mathscr{I}}(D_p, 2b/(p-1))$ holds.

Note: here we use the notation $\mathrm{Cl}_L[p]$ to denote the p-torsion subgroup of the class group Cl_L of the field $L/\mathbb{Q}$; see e.g. (7.1) for the definition.

2.2.1 Proof of the upper bound

Next we count degree p D_p-fields with a fixed discriminant. We may trivially state that $\mathbf{D}_p(D_p, \varpi)$ holds with $\varpi = 3/(p-1) - 1/p(p-1)$, by applying (2.4). We improve on this by only counting fields with a fixed discriminant and using our additional ramification restriction.

Let $K \in Z_p^{\mathscr{I}}(\mathbb{Q}, D_p)$ be a degree p D_p-field with absolute discriminant D. Let $\tilde{K}$ be the Galois closure of K and L be the quadratic field inside $\tilde{K}$, so $\tilde{K}/L$ is a cyclic p extension. Our ramification restriction implies that $\tilde{K}/L$ is unramified except perhaps at primes dividing $2p$. We have, by our ramification restriction, that $|\mathrm{Disc}\, K| = 2^a p^b Q^{(p-1)/2}$, where Q is square-free and relatively prime to $2p$. Then $|\mathrm{Disc}\, L| = 2^{a'} p^{b'} Q$ for some a', b' that are bounded in terms of p. Thus, given D, there are a constant (in terms of p) possible quadratic fields L, and for each of them we will count the possible cyclic p extensions $\tilde{K}/L$ that could arise.

Let J_L be the idèle class group of L. For a finite place v of L, let $\mathcal{O}_v$ be the elements of non-negative valuation in the completion L_v, and for an infinite place v let $\mathcal{O}_v = L_v$. From the exact sequence $\prod_v \mathcal{O}_v^* \to J_L \to \mathrm{Cl}_L \to 1$ [61, Ch. VI Prop. 1.3] (where the product is over all places of L), and the left-exactness of $\mathrm{Hom}_{cts}(-, C_p)$, we have an exact sequence

$$1 \to \mathrm{Hom}(\mathrm{Cl}_L, C_p) \to \mathrm{Hom}_{cts}(J_L, C_p) \to \mathrm{Hom}_{cts}(\prod_v \mathcal{O}_v^*, C_p),$$

where we can take the product just above over finite places v of L, since there are no continuous homormorphisms from $\mathbb{R}^*$ or $\mathbb{C}^*$ into C_p for p odd. Our desired C_p-extensions of L correspond via class field theory to elements of $\mathrm{Hom}_{cts}(J_L, C_p)$ that for each $v \nmid 2p$ map $\mathcal{O}_v^*$ to the identity, since they are unramified at such v. Thus the number of possible images in $\mathrm{Hom}_{cts}(\prod_v \mathcal{O}_v^*, C_p)$ for our desired elements of $\mathrm{Hom}_{cts}(J_L, C_p)$ is $|\mathrm{Hom}(\prod_{v|2p} \mathcal{O}_v^*, C_p)|$. The number of $v \mid 2p$ is at most 4 since L is quadratic. Since L_v is either $\mathbb{Q}_p$ or $\mathbb{Q}_2$ or quadratic over $\mathbb{Q}_p$ or $\mathbb{Q}_2$ (and there are only finitely many possibilities for the latter), the number of homomorphisms from $\mathcal{O}_v^*$ to C_p for $v \mid 2p$ is bounded in terms of p. Also, $|\mathrm{Hom}(\mathrm{Cl}_L, C_p)| = |\mathrm{Cl}_L[p]|$. Note $\mathrm{Disc}\, L = O_p(|\mathrm{Disc}\, K|^{2/(p-1)})$. So if we assume $|\mathrm{Cl}_L[p]| = O_p(|\mathrm{Disc}\, L|^b)$, then the number of possible $\tilde{K}$, and thus the number of possible K, is $O_p(D^{2b/(p-1)})$.

2.2.2 *Proof of the lower bound*

Given a quadratic field L, if $\mathrm{Cl}_L[p]$ is non-trivial, class field theory gives an unramified cyclic degree p extension L'/L. The group $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$ acts on Cl_L by inversion (since for an ideal $\mathfrak{a}$ of L, we have that $\mathfrak{a}\sigma(\mathfrak{a})$ is principal). It follows that $L'/\mathbb{Q}$ is a degree $2p$ D_p-extension, with all inertia trivial or in a subgroup generated by a reflection.

Now given an imaginary quadratic field L with units ± 1 such that $\mathrm{Cl}_L[p]$ is trivial and p splits completely in L, we we will show by other means that we still can obtain a degree $2p$ D_p-extension $L'/\mathbb{Q}$ containing L, and with our required ramification condition. We will construct a surjection ϕ from J_L to the cyclic group C_p of order p. Let v_1, v_2 be the two places of L above p. We let $\phi_{v_1} : \mathcal{O}_{v_1}^* \to C_p$ be any surjection. We let $\phi_{v_2} : \mathcal{O}_{v_2}^* \to C_p$ be defined by $\phi_{v_2}(u) = \phi_{v_1}(\sigma(u))^{-1}$. At every other place $v \neq v_1, v_2$, we let $\phi_v : \mathcal{O}_v^* \to C_p$ be trivial. Then at each place v, we pick an element $\alpha_v \in L$ that has valuation 1 at v and valuation divisible by p at all other places (which we can do since $\mathrm{Cl}_L[p]$ is trivial). We extend ϕ_v to $\phi_v : L_v^* \to C_p$ by letting $\phi_v(\alpha_v) = \prod_{w \neq v} \phi_w(\alpha_v)^{-1}$. The ϕ_v combine to give a map $\phi : \prod_v L_v^* \to C_p$, that is trivial on the diagonal embeddings of pth powers, the α_v, and units. These elements generate L^* (since $\mathrm{Cl}_L[p]$ is trivial), and so ϕ descends to a map $\phi : J_L \to C_p$. We can check that it follows from our definitions that $\phi(\sigma(x)) = \phi(x)^{-1}$. We recall from class field theory that the Artin map for L is equivariant for the usual action of $\mathrm{Gal}(L/\mathbb{Q})$ on J_L and the action of $\mathrm{Gal}(L/\mathbb{Q})$ on $\mathrm{Gal}(L^{ab}/L)$ given by conjugation by a lift in $\mathrm{Gal}(L^{ab}/\mathbb{Q})$ [74, Thm 11.5 (i)]. So since $\ker \phi$ is $\mathrm{Gal}(L/\mathbb{Q})$ invariant, it follows from Galois theory that the degree p cyclic extension L' of L corresponding to ϕ (from class field theory) is actually Galois over $\mathbb{Q}$. Since p is odd, we have that $\mathrm{Gal}(L'/\mathbb{Q})$ is a semi-direct product $\mathrm{Gal}(L'/L) \rtimes \mathrm{Gal}(K/\mathbb{Q})$, and the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the

index p subgroup $\mathrm{Gal}(L'/L)$ given above shows that $\mathrm{Gal}(L'/\mathbb{Q}) \simeq D_p$. Since L'/L has no tame ramification by choice of the $\phi_v|_{\mathcal{O}_v^*}$, all tame ramification of $L'/\mathbb{Q}$ has inertia in the subgroup of a reflection.

So for all but finitely many imaginary quadratic fields L in which p splits completely, we have constructed a degree $2p$ D_p-extension $L'/\mathbb{Q}$ containing L with our required ramification condition, which in particular contains a degree p D_p-extension K. At primes $\ell \nmid 2p$ of $\mathbb{Q}$, the exponent of ℓ in $\mathrm{Disc}\, K$ is $(p-1)/2$ if ℓ is ramified in L and 0 otherwise. So we have that $\mathrm{Disc}\, K$ is within a constant (depending on p) factor of $(\mathrm{Disc}\, L)^{(p-1)/2}$. Since we have $\gg_p X$ of these quadratic fields L, we conclude we have $\gg_p X^{2/(p-1)}$ fields counted by $Z_p^{\mathscr{J}}(\mathbb{Q}, D_p; X)$.

2.3 Symmetric groups S_n

Our work on S_n-fields requires understanding the size of $Z_n^{\mathscr{J}}(\mathbb{Q}, S_n; X)$ with $\mathscr{J} = [(1\ 2)]$; this is equivalent to requiring that the tamely-ramified part of D_K is square-free. This is a consequence of a standard fact (see Lemma 6.9) that p is tamely ramified in K with inertia group generated by a transposition if and only if $p \| D_K$. We record for $n = 3, 4, 5$, that by work of Bhargava [7, Theorem 1.3],

$$|Z_n^{\mathscr{J}}(\mathbb{Q}, S_n; X)| \sim c_n X. \tag{2.5}$$

By the asymptotic counts of S_3-fields due to Davenport and Heilbronn [23] and S_4-fields and S_5-fields due to Bhargava [4,6], the fields in $Z_n^{\mathscr{J}}(\mathbb{Q}, S_n)$ are a positive proportion of all S_n fields for $n = 3, 4, 5$. Moreover, it is conjectured by Malle [52] and Bhargava [5,7] that asymptotics of order X hold for $Z_n^{\mathscr{J}}(\mathbb{Q}, S_n; X)$ and $Z_n(\mathbb{Q}, S_n; X)$ when $n \geq 6$.

For symmetric groups S_n with $n \geq 6$, the best proven results are much weaker. For $n > 2$, we have an upper bound of Ellenberg and Venkatesh [30] on all degree n number fields $Z_n(\mathbb{Q})$,

$$|Z_n(\mathbb{Q}; X)| \ll (\alpha_n X)^{\exp(C\sqrt{\log n})}, \tag{2.6}$$

where α_n is a constant depending only on n and C is an absolute constant. The best known lower bound for S_n-fields is $|Z_n(\mathbb{Q}, S_n; X)| \gg_n X^{1/2+1/n}$ by Bhargava, Shankar and Wang [11, Thm. 1.3], and importantly for us, all of the fields they construct to deduce this new lower bound have square-free discriminant. As a consequence, for all $n \geq 6$ and $\mathscr{J} = [(1\ 2)]$,

$$|Z_n^{\mathscr{J}}(\mathbb{Q}, S_n; X)| \gg_n X^{1/2+1/n}. \tag{2.7}$$

We also require upper bounds on S_n-fields of a fixed discriminant, and we state the best known results here. Ellenberg and Venkatesh [31, p. 1] prove

Property $\mathbf{D}_3(S_3, 1/3)$. Klüners [44] proves Property $\mathbf{D}_4(S_4, 1/2)$. From Bhargava's count for quintic fields, we may trivially deduce that $\mathbf{D}_5(S_5, 1)$ holds. For our work, knowing $\mathbf{D}_5(S_5, \varpi)$ for any $\varpi < 1$ would suffice, so we make the following simple observation:

Proposition 2.4 *Property* $\mathbf{D}_5(\varpi)$ *holds for* $\varpi = 199/200$.

This follows immediately from the power-saving count for quintic S_5-fields proved by Shankar and Tsimerman [72] (see also the power-saving count for all quintic fields in [28, Thm. 2.4]). Indeed, letting $Z_5(\mathbb{Q}; X)$ denote all quintic fields with $D_K \leq X$, we have a constant $c_{5a} > 0$ such that

$$|Z_5(\mathbb{Q}; X)| = c_{5a}X + O_\varepsilon(X^{199/200+\varepsilon})$$

for every $\varepsilon > 0$, so that upon differencing this for $X = D$ and $X = D - 1$, Proposition 2.4 follows.

2.4 The alternating group A_4

For A_4, it is known by Baily [3] that the lower bound conjectured by Malle [52] holds, $|Z_4(\mathbb{Q}, A_4; X)| \gg X^{1/2}$, and by Wong [86] that a weaker upper bound holds,

$$|Z_4(\mathbb{Q}, A_4; X)| \ll X^{5/6+\varepsilon}. \tag{2.8}$$

We require a lower bound that includes a ramification restriction and an upper bound for fields of fixed discriminant.

Proposition 2.5 *(Alternating group* A_4*) Let* $Z_4^{\mathscr{J}}(\mathbb{Q}, A_4; X)$ *count those fields* $K \in Z_4(\mathbb{Q}, A_4; X)$ *such that every rational prime that ramifies tamely in* K *has inertia group generated by an element in either of the conjugacy classes* $\{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\}$ *or* $\{(1\ 3\ 2), (1\ 4\ 3), (1\ 2\ 4), (2\ 3\ 4)\}$. *Then* $|Z_4^{\mathscr{J}}(\mathbb{Q}, A_4; X)| \gg X^{1/2}$. *Moreover,* $\mathbf{D}_4(A_4, \varpi)$ *holds for* $\varpi = 0.2784\ldots$.

Property $\mathbf{D}_4(A_4, \varpi)$ was previously known for $\varpi = 3/4$ due to Wong [84, Thm. 6], but this is not small enough for our purposes.

2.4.1 The upper bound

To show that $\mathbf{D}_4(A_4, \varpi)$ holds with $\varpi = 0.2784...$, we will apply Baily's connection [3] of A_4 fields to certain quadratic ray class characters of cyclic cubic fields, in combination with the bound on the 2-torsion in class groups of cubic fields due to Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao [10]. We thank Manjul Bhargava for suggesting this approach.

Let K_4 be a quartic A_4-field of discriminant D. Let K_3 be the fixed field of the subgroup of A_4 generated by $\{(1\ 2)(3\ 4), (2\ 3)(1\ 4)\}$, and note that

K_3 is cyclic cubic. We can check using Lemma 6.9 that tame rational primes with inertia type in the conjugacy class of (1 2)(3 4) appear squared in the discriminant of K_4 and do not appear in the discriminant of K_3. Similarly, tame rational primes with inertia type in the conjugacy class of (1 2 3) appear squared in the discriminants of both K_4 and K_3. So $\text{Disc}\, K_3 \mid 2^a 3^b \text{Disc}\, K_4$, for some absolute positive integers a, b.

Let K_6 be one of the (conjugate) sextic subfields of the Galois closure of K_4. Note that K_4 and K_6 have the same Galois closure, and so to count K_4 we may equivalently (up to a fixed constant) count the associated K_6. By [3, Lemmas 13 and 15] we have that $K_6 = K_3(b^{1/2})$, where $b \in \mathcal{O}_{K_3} \setminus \{\mathbb{Z} \cup \mathcal{O}_{K_3}^2\}$ and $N_{K_3/\mathbb{Q}}(b)$ is a square rational integer. We have that $N_{K_3/\mathbb{Q}}(\text{Disc}\,(K_6/K_3)) = \text{Disc}\, K_4/\text{Disc}\, K_3$ (see [3, Lemma 11]).

Now, we sum over each divisor d of $2^a 3^b D$ the number of quartic A_4-fields K_4 of discriminant D with $\text{Disc}\, K_3 = d$. There are $O(2^{\omega(d)})$ cyclic cubic fields of discriminant d [19]. Given a fixed cyclic cubic field K_3 of discriminant d, for an upper bound, it suffices to bound the number of sextic fields of the form $K_3(b^{1/2})$, where $b \in \mathcal{O}_{K_3} \setminus \{\mathbb{Z} \cup \mathcal{O}_{K_3}^2\}$ and $N_{K_3/\mathbb{Q}}(b)$ is a square rational integer. We do this following the argument in [3, Lemma 10]. Such a sextic field corresponds to a quadratic ray class character of conductor $\mathfrak{d}$ with finite part $\mathfrak{d}^* = \text{Disc}\,(K_6/K_3)$, and such a character is a product of a character on $(\mathcal{O}_{K_3}/\mathfrak{d}^*)^\times$, a character on the class group of K_3, and a character on signature (see [3, (4)]). Baily [3, Lemma 8] describes the possible forms of $\mathfrak{d}$, and in the proof of [3, Lemma 9] gives a generating function for all the primitive quadratic characters on $(\mathcal{O}_{K_3}/\mathfrak{d}^*)^\times$. From this it follows there are $O(3^{\omega(D/d)})$ choices of $\mathfrak{d}^*$ with characters on $(\mathcal{O}_{K_3}/\mathfrak{d}^*)^\times$ such that we will have $\text{Disc}\,(K_6/K_3) = D/d$. Let $h_2(K_3)$ denote the size of the 2-torsion subgroup of the class group of K_3. There are at most $h_2(K_3)$ class group characters, and $h_2(K_3) = O_\varepsilon(d^{0.2784\cdots+\varepsilon})$ by [10, Equation (4)]. There are at most 8 characters of signature, and so in conclusion, there are at most

$$O_\varepsilon\left(\sum_{d \mid D} 2^{\omega(d)} 3^{\omega(D/d)} d^{0.2784\ldots+\varepsilon}\right) = O_\varepsilon(D^{0.2784\ldots+\varepsilon})$$

quartic A_4-fields of discriminant D.

2.4.2 *The lower bound*

The lower bound on the number of quartic A_4-fields with our required ramification condition follows from the proof of [3, Theorem 3]. As stated in line 2 of the proof of [3, Lemma 16], the degree 6 fields K_6 constructed by Baily are unramified over the relevant degree 3 cyclic field K_3, except perhaps at

primes of K_3 dividing 2. These fields K_6 have Galois closure K_{12} of degree 12 with Galois group A_4. The fact that K_6/K_3 is unramified except at primes of K_3 dividing 2 means that for each odd rational prime p the inertia groups of p in $\mathrm{Gal}(K_{12}/\mathbb{Q})$ must be trivial or generated by a three-cycle. The same holds for $p = 2$ if the primes of K_3 that divide 2 are unramified in K_6/K_3. If a prime dividing 2 is ramified in K_6/K_3, it is wildly ramified, and thus 2 in wildly ramified in K_{12}.

2.5 The alternating groups A_n and proof of Theorem 1.5

The fact that for $n \geq 5$, A_n is a simple group will make a later part of our argument much simpler, but on the other hand we require a lower bound for the number of degree n A_n-extensions of $\mathbb{Q}$ with bounded discriminant, which was not previously in the literature. We prove:

Theorem 2.6 (Alternating groups A_n, $n \geq 3$) *For each integer $n \geq 3$, there exists a real number $\beta_n > 0$ such that for all $X \geq 1$, for every $\varepsilon > 0$, $|Z_n(\mathbb{Q}, A_n; X)| \gg_{n,\varepsilon} X^{\beta_n - \varepsilon}$. In fact we may take $\beta_n = (1 - \frac{2}{n!})/(4n - 4)$.*

We first observe that Theorem 1.5 implies Theorem 2.6 when we specialize G to A_n. For each $n \geq 3$, Hilbert [40] gave polynomials $f(x, t) \in \mathbb{Q}[x, t]$ that have Galois group A_n over $\mathbb{Q}(t)$ and are degree n in x and degree 2 in t. (Hilbert in turn credits Hurwitz with the examples: see [40, p. 125] for n even and [40, p. 126] for n odd; see also [69, Section 10.3].) Moreover, these same polynomials (by the same argument) have Galois group A_n over $E(t)$, for any number field E, and thus their splitting fields do not contain a non-trivial finite extension of $\mathbb{Q}$ (i.e. they are regular). Thus Theorem 1.5 with $|G| = |A_n| = n!/2$, $j = 1$, $m = n$ and $d = 2$ verifies Theorem 2.6.

We now prove Theorem 1.5; we thank Akshay Venkatesh and Manjul Bhargava for suggesting the approach we use, and for a number of helpful discussions. The method of proof, in imprecise terms, is as follows. Suppose that $f(x, \mathbf{t})$ has Galois group G over $\mathbb{Q}(\mathbf{t})$, resulting in, say, y different fields with Galois group G as $\mathbf{t}$ varies over all integral tuples with coordinates at most T in absolute value. Then by showing that $f(x, \mathbf{t}) f(x, \mathbf{t}')$ typically has Galois group $G \times G$ and very rarely has Galois group G (which occurs when the fields provided by $f(x, \mathbf{t})$ and $f(x, \mathbf{t}')$ collide), we will deduce that $f(x, \mathbf{t})$ must have produced many different fields to begin with, that is, y must grow at least like a small power of T. See also [69, p. 137] for a hint at a similar philosophy applied to generating infinitely many G-extensions if one such extension is known.

In order to put this into action in precise terms, we require a quantitative version of the Hilbert irreducibility theorem, for which we cite [13]:

Theorem C *Suppose* $f(X, T_1, \ldots, T_j) \in \mathbb{Q}[X, T_1, \ldots, T_j]$ *is an irreducible polynomial with splitting field* K *over* $\mathbb{Q}(T_1, \ldots, T_j)$ *such that* $\mathrm{Gal}(K/\mathbb{Q}(T_1, \ldots, T_j)) \simeq G$. *For any subgroup* $H \subset G$ *set*

$$N_f(T; H) = \#\{\mathbf{t} \in \mathbb{Z}^j : |\mathbf{t}|_\infty \leq T \text{ and the splitting field of } f(X, \mathbf{t}) \text{ over } \mathbb{Q} \text{ has Galois group } \simeq H\}.$$

Then for every $T \geq 1$ *and every* $\varepsilon > 0$, $N_f(T; H) \ll_{f,\varepsilon} T^{j-1+|G/H|^{-1}+\varepsilon}$.

We also require the following key lemma:

Lemma 2.7 *Let* $f(x, t_1, \ldots, t_j) \in \mathbb{Q}(t_1, \ldots, t_j)[x]$ *be a polynomial with splitting field* K *over* $\mathbb{Q}(t_1, \ldots, t_j)$ *such that* $\mathrm{Gal}(K/\mathbb{Q}(t_1, \ldots, t_j)) \simeq G$. *Suppose that* $f(x, t_1, \ldots, t_j)$ *is regular, i.e.* K *does not contain a non-trivial finite extension of* $\mathbb{Q}$. *Then* $f(x, t_1, \ldots, t_j) f(x, s_1, \ldots, s_j)$ *has splitting field with Galois group* $G \times G$ *over* $\mathbb{Q}(t_1, \ldots, t_j, s_1, \ldots, s_j)$.

2.5.1 Proof of Lemma 2.7

We will prove the lemma in the case $j = 1$; a straightforward extension of this argument applies to the general case. Let $F(x, t) \in \mathbb{Q}[t, x]$ be a monic irreducible polynomial of x with a root θ that generates K over $\mathbb{Q}(t)$. We let all our splitting fields be in a fixed algebraic closure of $\mathbb{Q}(s, t)$. Then $K\mathbb{Q}(s)$ is the splitting field of $f(x, t)$ over $\mathbb{Q}(s, t)$. We will show below that if $G(s, x) \in \mathbb{Q}[s, x]$ is a monic polynomial irreducible over $\mathbb{Q}(s)$ that generates a Galois extension of $\mathbb{Q}(s)$ and does not contain a non-trivial finite extension of $\mathbb{Q}$, then $G(s, x)$ is irreducible over $K\mathbb{Q}(s)$. We will see now that this will suffice to prove the lemma. Applying this in the case where F is trivial, we will see that $G(s, x)$ is irreducible over $\mathbb{Q}(s, t)$, and in particular, analogously we will see that $F(x, t)$ is irreducible over $\mathbb{Q}(s, t)$ and so $[K\mathbb{Q}(s) : \mathbb{Q}(s, t)] = |G|$. So if L is the splitting field of $f(s, x)$ over $\mathbb{Q}(s)$, then L is generated by $F(s, x)$, and applying the above with $G(s, x) = F(s, x)$, we see that $[KL : K\mathbb{Q}(s)] = |G|$. Thus $\mathrm{Gal}(KL/\mathbb{Q}(s, t))$ has order $|G|^2$ and injects into $\mathrm{Gal}(K/\mathbb{Q}(t)) \times \mathrm{Gal}(L/\mathbb{Q}(s))$, and so $\mathrm{Gal}(KL/\mathbb{Q}(s, t)) \simeq G \times G$. Since KL is the splitting field of $f(x, t) f(x, s)$ over $\mathbb{Q}(s, t)$, this proves the lemma.

Now we show that $G(s, x)$ with the assumptions above is irreducible over $K\mathbb{Q}(s)$. Suppose that $G(s, x)$ factored into $a(x)b(x)$ over $K\mathbb{Q}(s)$. We can write

$$a(x) = \sum_{i=0}^{k} \frac{n_i(s, t, \theta)}{d_i(s, t)} x^i$$

where $n_i(y, z, w) \in \mathbb{Q}[y, z, w]$ and $n_i(y, z) \in \mathbb{Q}[y, z]$. (Since θ is algebraic over $\mathbb{Q}(s, t)$, we can write elements of $K\mathbb{Q}(s)$ as polynomials in θ with coefficients in $\mathbb{Q}(s, t)$, and so we can arrange to have no θ's in the denominators.) Let $n_{i,j}(z, w)$ be the coefficient of y^j in $n_i(y, z, w)$. Let I_a be the ideal in $\mathbb{Q}[z, w]$ generated by all the $n_{i,j}(z, w)$ for all j and for $i \geq 1$, and define I_b analogously. We claim that, as ideals of $\mathbb{Q}[z, w]$, we have $(F(w, z)) \supset I_a I_b$. Suppose not. Then there are infinitely many maximal ideals m of $\mathbb{Q}[z, w]$ that contain $(F(w, z))$ but not $I_a I_b$. Each such maximal ideal gives values $t_0, \theta_0 \in \overline{\mathbb{Q}}$ such that $F(\theta_0, t_0) = 0$, but upon substitution of $z \mapsto t_0$ and $w \mapsto \theta_0$, some element of I_a and some element of I_b remain non-zero, which gives a non-trivial factorization of $G(s, x)$ over $\overline{\mathbb{Q}}(s)$ unless some denominator $d_i(s, t_0)$ is identically zero (or similarly for the denominators in $b(x)$). Since only finitely many t_0 can make a denominator zero, and each have a finitely many associated θ_0, we conclude that $G(s, x)$ factors non-trivially over $\overline{\mathbb{Q}}(s)$, and thus over $E(s, x)$ for some Galois number field E. Since $\mathrm{Gal}(E(s)/\mathbb{Q}(s)) \to \mathrm{Gal}(E/\mathbb{Q})$ is an isomorphism, the subfields of $E(s)$ that contain $\mathbb{Q}(s)$ are $E'(s)$ for the subfields E' of E. If M is the field generated by $G(s, x)$ over $\mathbb{Q}(s)$, then $[ME(s) : E(s)] = [M : M \cap E(s)]$. Since $G(s, x)$ factors non-trivially over $E(s)$, we have $[ME(s) : E(s)] < [M : \mathbb{Q}(s)]$, and thus $M \cap E(s)$ is a non-trivial extension of $\mathbb{Q}(s)$ inside $E(s)$, and thus contains some number field E'. In particular M contains a non-trivial number field, which contradicts our assumption on $G(s, x)$. Thus, we conclude that $(F(w, z)) \supset I_a I_b$, and thus $(F(w, z))|I_a I_b$, and thus either$(F(w, z))|I_a$ or $(F(w, z))|I_b$, since $(F(w, z))$ is prime. But this implies that either a or b has all coefficients 0 except the constant one, and thus we conclude $G(s, x)$ is irreducible over $K\mathbb{Q}(s)$. This concludes the proof of Lemma 2.7.

2.5.2 *Proof of Theorem 1.5*

With Lemma 2.7 and Theorem C in hand, we may now prove Theorem 1.5. Suppose $f(X, T_1, \dots, T_j)$ is a polynomial of total degree d in the T_i with Galois group G over $\mathbb{Q}(T_1, \dots, T_j)$ (with degree n in X). For $\mathbf{t} = (t_1, \dots, t_j)$, we define $|\mathbf{t}|_\infty = \max_{1 \leq \ell \leq j} |t_\ell|$, so that there are $\gg T^j$ possible values of $\mathbf{t} \in \mathbb{Z}^j$ with $|\mathbf{t}|_\infty \leq T$. For each $\mathbf{t} \in \mathbb{Z}^j$, let $L_{\mathbf{t}}$ be the splitting field of $f(X, t_1, \dots, t_j)$ in $\bar{\mathbb{Q}}$. Let y be the size of the set $\{L_{\mathbf{t}} : \mathbf{t} \in \mathbb{Z}^j, |\mathbf{t}|_\infty \leq T, \mathrm{Gal}(L_{\mathbf{t}}/\mathbb{Q}) \simeq G\}$ (note it is possible that different $\mathbf{t}$ give the same $L_{\mathbf{t}}$), and we also write $L_1, \dots, L_y$ for the fields in this set.

For each $1 \leq i \leq y$, suppose A_i of the values $\mathbf{t}$ have $L_{\mathbf{t}} = L_i$. So

$$A_1 + \cdots + A_y = A,$$

where A is the total number of values of $|\mathbf{t}|_\infty \le T$ with $\mathrm{Gal}(L_\mathbf{t}/\mathbb{Q}) \simeq G$. From Theorem C above, we have that $A \gg_f T^j$, since there are finitely many subgroups which each appear with an upper bound with exponent strictly smaller than j.

For each $\mathbf{t} \in \mathbb{Z}^{2j}$, let $M_\mathbf{t}$ be the splitting field of $f(X, t_1, \ldots, t_j) f(X, t_{j+1}, \ldots, t_{2j})$. We ask how many $\mathbf{t} \in \mathbb{Z}^{2j}$ with $|\mathbf{t}|_\infty \le T$ have $\mathrm{Gal}(M_\mathbf{t}/\mathbb{Q}) \simeq G$? By Lemma 2.7 and the assumption that f is regular, we have that $f(X, T_1, \ldots, T_j) f(X, T_{j+1}, \ldots, T_{2j})$ has Galois group $G \times G$ over $\mathbb{Q}(T_1, \ldots, T_{2j})$. Thus, by Theorem C, the number of $\mathbf{t} \in \mathbb{Z}^{2j}$ with $|\mathbf{t}|_\infty \le T$ and $\mathrm{Gal}(M_\mathbf{t}/\mathbb{Q}) \simeq G$ is $\ll_{f,\varepsilon} T^{2j-1+|G|^{-1}+\varepsilon}$. However, note that this occurs whenever $f(X, t_1, \ldots, t_j)$ and $f(X, t_{j+1}, \ldots, t_{2j})$ have the same splitting field with Galois group G, and so

$$A_1^2 + \cdots + A_y^2 \ll_{f,\varepsilon} T^{2j-1+|G|^{-1}+\varepsilon}.$$

By Cauchy-Schwarz, $(A_1 + \cdots + A_y)^2 \le y(A_1^2 + \cdots + A_y^2)$, and we conclude that

$$y \ge \frac{(A_1 + \cdots + A_y)^2}{(A_1^2 + \cdots + A_y^2)} \gg_{f,\varepsilon} \frac{T^{2j}}{T^{2j-1+|G|^{-1}+\varepsilon}} = T^{1-|G|^{-1}-\varepsilon}.$$

Thus there are $\gg_{f,\varepsilon} T^{1-|G|^{-1}-\varepsilon}$ different fields with Galois group G that come from specializations of $f(X, T_1, \ldots, T_j)$ to some $\mathbf{t}$ with $|\mathbf{t}|_\infty \le T$. For $|\mathbf{t}|_\infty \le T$, we have that $f(X, t_1, \ldots, t_j)$ is a degree n polynomial in X with coefficients $\ll_f T^d$ and thus with absolute discriminant $\ll_f T^{d(2n-2)}$. Thus $L_\mathbf{t}$ has absolute discriminant $\ll_f T^{d(2n-2)}$. In conclusion, there are $\gg_{f,\varepsilon} X^{(1-|G|^{-1}-\varepsilon)/(d(2n-2))}$ degree n G-fields with absolute discriminant at most X, completing the proof of Theorem 1.5.

Part II: Effective Chebotarev theorems

3 Quantitative statements of Chebotarev theorems for families

We now state quantitative versions of our main Chebotarev theorems, starting with a quantitative version of Theorem 1.3.

Theorem 3.1 (Chebotarev conditional on zero-free region) *Let k be a fixed number field. Fix $A \ge 2$, $0 < \delta \le 1/(2A)$, and an integer $n \ge 1$. Let G be a fixed transitive subgroup of S_n. Then there exists $D_0 \ge 1$ and $\kappa_1, \kappa_2, \kappa_3 > 0$ such that the following holds: for any Galois extension of number fields L/k with $\mathrm{Gal}(L/k) \simeq G$ such that $D_L \ge D_0$ and such that the Artin L-function $\zeta_L(s)/\zeta_k(s)$ is zero-free in the region*

$$[1-\delta, 1] \times [-(\log D_L)^{2/\delta}, (\log D_L)^{2/\delta}], \tag{3.1}$$

we have that for any conjugacy class $\mathscr{C} \subseteq G$,

$$\left| \pi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x) \right| \leq \frac{|\mathscr{C}|}{|G|} \frac{x}{(\log x)^A} \tag{3.2}$$

for all

$$x \geq \kappa_1 \exp\{\kappa_2 (\log\log(D_L^{\kappa_3}))^2\}. \tag{3.3}$$

If moreover $k = \mathbb{Q}$, (3.2) *holds for all*

$$x \geq \kappa_1 \exp\{\kappa_2 (\log\log(D_L^{\kappa_3}))^{5/3} (\log\log\log(D_L^2))^{1/3}\}. \tag{3.4}$$

Remark 3.2 The parameters D_0 and $\kappa_1, \kappa_2, \kappa_3$ depend on n, $|G|$, A, δ, and the field k; they are precisely specified in Remark 4.11 and (4.47), respectively.

We next state, in quantitative form, the cases of Theorem 1.1 that are completely unconditional.

Theorem 3.3 *For each family* $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ *specified in items (1)–(5) of the list below, there exist constants* β, d *with* $0 < \beta \leq d$ *such that for all* $X \geq 1$,

$$X^{\beta} \ll_{n,G,\mathscr{I}} |Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| \ll_{n,G,\mathscr{I}} X^d. \tag{3.5}$$

Moreover, there exists a constant τ_* *with* $0 \leq \tau_* < \beta$, *such that for every* $\tau > \tau_*$ *and every sufficiently small* $\varepsilon_0 > 0$, *there exists a constant* D_3 *and a constant*

$$\delta = \delta(\varepsilon_0, m, |G|d) \tag{3.6}$$

such that for all $X \geq 1$, *there are at most* $D_3 X^{\tau+\varepsilon_0}$ δ*-exceptional fields in* $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$; *here* m *is the maximum dimension of an irreducible representation of* G.

Moreover, fix any $A \geq 2$. *Then for any* $\varepsilon_0 > 0$ *such that* δ *as defined in* (3.6) *satisfies* $\delta \leq 1/(2A)$, *there exists a constant* $D_5 \geq 1$ *and constants* $\kappa_1, \kappa_2, \kappa_3 > 0$ *such that for all* $X \geq 1$, *aside from a set* $E(X)$ *of at most* $D_5 X^{\tau+\varepsilon_0}$ *possible exceptions, each field* $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ *has the property that for its Galois closure* $\tilde{K}$ *over* $\mathbb{Q}$, *for every conjugacy class* $\mathscr{C} \subseteq G$,

$$\left| \pi_{\mathscr{C}}(x, \tilde{K}/\mathbb{Q}) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x) \right| \leq \frac{|\mathscr{C}|}{|G|} \frac{x}{(\log x)^A}$$

for all $x \geq \kappa_1 \exp\{\kappa_2 (\log\log(D_{\tilde{K}}^{\kappa_3}))^{5/3} (\log\log\log(D_{\tilde{K}}^2))^{1/3}\}$.

The families $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ are defined by:

(1) *G a cyclic group of order $n \geq 2$, with $\mathscr{I}$ comprised of all generators of G (equivalently, every rational prime that is tamely ramified in K is totally ramified). In this case $|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| \sim c_n X^{1/(n-1)}$ and $\tau_* = 0$. (Hence, the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^\varepsilon$ for every $\varepsilon > 0$.)*

(2) *$n = 3$, $G \simeq S_3$ acting on a set of 3 elements, $\mathscr{I}$ being the conjugacy class $[(1\ 2)]$ of transpositions. In this case, $|Z_3^{\mathscr{I}}(\mathbb{Q}, S_3; X)| \sim c_3 X$ and $\tau_* = 1/3$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^{1/3+\varepsilon}$ for every $\varepsilon > 0$.)*

(3) *$n = 4$, $G \simeq S_4$ acting on a set of 4 elements, $\mathscr{I}$ being the conjugacy class $[(1\ 2)]$ of transpositions. In this case, $|Z_4^{\mathscr{I}}(\mathbb{Q}, S_4; X)| \sim c_4 X$ and $\tau_* = 1/2$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^{1/2+\varepsilon}$ for every $\varepsilon > 0$.)*

(4) *$n = p$ an odd prime, $G = D_p$ the order $2p$ dihedral group of symmetries of a regular p-gon, $\mathscr{I}$ being the conjugacy class of order 2 elements. In this case, for all $X \geq 1$,*

$$X^{2/(p-1)} \ll_p |Z_p^{\mathscr{I}}(\mathbb{Q}, D_p; X)| \ll_{p,\varepsilon} X^{3/(p-1)-1/(p(p-1))+\varepsilon}$$

and $\tau_* = 1/(p-1)$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^{1/(p-1)+\varepsilon}$ for every $\varepsilon > 0$.)

(5) *$n = 4$, $G \simeq A_4$ as a subgroup of S_4 acting on a set of 4 elements, $\mathscr{I}$ comprised of the two conjugacy classes of order 3 elements. In this case, for all $X \geq 1$,*

$$X^{1/2} \ll |Z_4^{\mathscr{I}}(\mathbb{Q}, A_4; X)| \ll_\varepsilon X^{5/6+\varepsilon},$$

and $\tau_* = 0.2784\ldots$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^{0.2784\ldots\varepsilon}$ for every $\varepsilon > 0$.)

Note we have that $m \leq |G|^{.5}$ (see [80] for asymptotics when $G = S_n$).

Remark 3.4 Kowalski and Michel's result [45, Theorem 2] leads to the choice $\delta = \frac{\varepsilon_0}{5m|G|/2+2d+4\varepsilon_0}$. Within a fixed family $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$, note that as we choose ε_0 smaller (so that δ correspondingly decreases), the density of potential δ-exceptional fields decreases, in accord with the fact that the requirement that $\zeta_{\tilde{K}}(s)/\zeta(s)$ be zero-free in a box to the right of $\Re(s) = 1 - \delta$ becomes less stringent, and fewer fields would be expected to violate it. Simultaneously, as δ and accordingly the width of the zero-free region decreases, the lower-bound threshold for x increases, since the explicit expressions given for the parameters κ_i grow with $1/\delta$ as specified in (4.47). This is also as expected.

Remark 3.5 (Cyclic fields of prime degree) If G is a cyclic group of prime order $p \geq 2$, then for each Galois extension $K/\mathbb{Q}$ with Galois group $\simeq G$, every ramified prime is totally ramified, so that for $\mathscr{I}$ as in Theorem 3.3, $Z_p^{\mathscr{I}}(\mathbb{Q}, G; X) = Z_p(\mathbb{Q}, G; X)$.

Remark 3.6 (degree n S_n-fields with square-free discriminant) Recall from Sect. 2.3 that for each $n \geq 2$, the family $Z_n^{\mathscr{I}}(\mathbb{Q}, S_n; X)$ with $\mathscr{I} = [(1\ 2)]$ includes all degree n S_n-fields with square-free discriminant, which are known in the case of $n = 3, 4, 5$ (and conjectured for $n \geq 6$) to be a positive proportion of all degree n fields.

Remark 3.7 (degree p D_p-fields) It is conjectured that $|Z_p(\mathbb{Q}, D_p; X)| \sim c_{D_p} X^{2/(p-1)}$ for some $c_{D_p} > 0$ (see [53], [43, p. 608]); assuming this is the true order, our family of degree p D_p-fields exhibited in case (4) is a positive proportion of all degree p D_p-fields.

Remark 3.8 (degree 4 A_4-fields) Based on heuristics as well as numerical evidence, it is conjectured that $|Z_4(\mathbb{Q}, A_4; X)| \sim c_{A_4} X^{1/2} \log X$ for some $c_{A_4} > 0$ (see [14, §2.7], [53, Ex. 3.2]); assuming this is the true order, our family of degree 4 A_4-fields exhibited in case (5) of Theorem 3.3 just fails to be a positive proportion of all degree 4 A_4-fields.

Finally, we state the quantitative forms of Theorem 1.1 that are conditional on the strong Artin conjecture, and in certain cases on hypotheses for counting number fields.

Theorem 3.9 (Quintic S_5-fields) *Consider the family $Z_5^{\mathscr{I}}(\mathbb{Q}, S_5)$ for $\mathscr{I}$ being the conjugacy class $[(1\ 2)]$ of transpositions, in which case $|Z_5^{\mathscr{I}}(\mathbb{Q}, G; X)| \sim c_5 X$. The conclusions of Theorem 3.3 hold for $Z_5^{\mathscr{I}}(\mathbb{Q}, G)$ if we assume the strong Artin conjecture holds for all irreducible Galois representations over $\mathbb{Q}$ with image S_5. In this case, $\tau_* = 199/200$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^{199/200+\varepsilon}$ for every $\varepsilon > 0$.)*

Remark 3.10 An alternative formulation of Theorem 3.9 uses the work of F. Calegari [12]. Let $Y_5^{\mathscr{I}}(\mathbb{Q}, S_5)$ be the family of quintic S_5-fields K such that complex conjugation in $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ has conjugacy class $(1\ 2)(3\ 4)$, $\tilde{K}/\mathbb{Q}$ is unramified at 5, and the Frobenius element at 5 has conjugacy class $(1\ 2)(3\ 4)$. By [7, Thm. 1.3], $|Y_5^{\mathscr{I}}(\mathbb{Q}, S_5; X)| \sim c_5' X$. For these fields, Calegari verifies the strong Artin conjecture for the dimension 4 and 6 irreducible representations of S_5, and reduces the verification for the dimension 5 irreducible representations to checking that a certain L-function is non-vanishing for $s \in [0, 1]$. Precisely, for $K \in Y_5(\mathbb{Q}, S_5)$, let E be the quadratic subfield of $\tilde{K}$, F be a subfield of $\tilde{K}$ of degree 6 over $\mathbb{Q}$, and H be the compositum of E and F. Then by [12, Thm. 1.2], the strong Artin conjecture holds for the dimension 5 irreducible

representations as long as $\zeta_H(s)$ is nonvanishing for $s \in [0, 1]$. (See [8], [27] for computational verification of this nonvanishing, in a finite number of cases with small discriminant.) Thus we could alternatively state Theorem 3.9 for the family $Y_5^{\mathscr{I}}(\mathbb{Q}, S_5)$, assuming in place of the strong Artin conjecture that for each field $K \in Y_5^{\mathscr{I}}(\mathbb{Q}, S_5)$ considered, the appropriate L-function $\zeta_H(s)$ is nonvanishing for $s \in [0, 1]$.

Theorem 3.11 (degree n S_n-fields) *Consider for $n \geq 6$ the family $Z_n^{\mathscr{I}}(\mathbb{Q}, S_n)$ with $\mathscr{I}$ being the conjugacy class $[(1\ 2)]$ of transpositions, in which case for all $X \geq 1$,*

$$X^{1/2+1/n} \ll_n |Z_n^{\mathscr{I}}(\mathbb{Q}, S_n; X)| \ll_n X^{\exp(C\sqrt{\log n})}.$$

The conclusions of Theorem 3.3 hold for the family $Z_n^{\mathscr{I}}(\mathbb{Q}, S_n)$ if we assume

(i) *the strong Artin conjecture for all irreducible Galois representations over $\mathbb{Q}$ with image S_n,*

(ii) *for some $\varpi_n < 1/2 + 1/n$, for every fixed integer D, there are at most $\ll_n D^{\varpi_n}$ fields $K \in Z_n(\mathbb{Q}, S_n)$ with $D_K = D$.*

In this case, $\tau_* = \varpi_n$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^{\varpi_n+\varepsilon}$ for every $\varepsilon > 0$.)

Remark 3.12 If it is known that $|Z_n^{\mathscr{I}}(\mathbb{Q}, S_n; X)| \gg_n X^{\beta_n}$, then to deduce that the possible exceptional set has density zero, we need only know (ii) for some $\varpi_n < \beta_n$.

Similarly our results for simple groups are conditional on the strong Artin conjecture; for A_n, we additionally apply our new lower bound for the number of degree n A_n-fields with bounded discriminant.

Theorem 3.13 (Alternating groups A_n, $n \geq 5$) *For each $n \geq 5$, consider the family $Z_n(\mathbb{Q}, A_n)$ (with no restriction on inertia type, that is, $\mathscr{I} = G$). In this case, there exists a positive exponent $\beta_n > 0$ such that for all $X \geq 1$,*

$$X^{\beta_n} \ll_n |Z_n^{\mathscr{I}}(\mathbb{Q}, A_n; X)| \ll_n X^{\exp(C\sqrt{\log n})}$$

for a certain absolute constant C. In fact we may take $\beta_n = (1 - 2/n!)/(4n - 4)$. Then under the assumption that the strong Artin Conjecture holds for all irreducible Galois representations over $\mathbb{Q}$ with image A_n, the conclusions of Theorem 3.3 hold with $\tau_* = 0$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_\varepsilon X^\varepsilon$ for every $\varepsilon > 0$.)

Finally, we state a result for families of fields parametrized by a fixed simple group; here we simply assume that a lower bound that grows like a power of X is known for the number of such fields (as may be obtained by Theorem 1.5 if an appropriate generating polynomial is known).

Theorem 3.14 (Simple groups) *For $n \geq 2$ and a fixed transitive simple group $G \subset S_n$, the conclusions of Theorem 3.3 hold for the family $Z_n(\mathbb{Q}, G)$ with no restriction on inertia type (that is, $\mathscr{I} = G$), if we assume*

(i) *the strong Artin conjecture holds for all irreducible representations over $\mathbb{Q}$ with image G,*
(ii) *a lower bound of the form $|Z_n(\mathbb{Q}, G; X)| \gg_{n,G} X^{\beta}$ for some $\beta > 0$, for all $X \geq 1$.*

Then $X^{\beta} \ll_n |Z_n(\mathbb{Q}, G; X)| \ll_n X^{\exp(C\sqrt{\log n})}$ for an absolute constant C, and $\tau_* = 0$. (Hence the density zero exceptional set $E(X)$ is at most of size $\ll_{\varepsilon} X^{\varepsilon}$ for every $\varepsilon > 0$.)

Remark 3.15 At present we do not treat families $Z_n(\mathbb{Q}, G)$ for G a non-cyclic abelian group, or $Z_4(\mathbb{Q}, D_4)$; we remark on difficulties encountered in these settings in Remarks 6.11 and 6.12.

We encapsulate two useful consequences in all the settings described above:

Corollary 3.16 (Quantitative counts for small primes) *Let $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ be fixed to be one of the families of fields considered in Theorems 3.3, 3.9, 3.11, 3.13 and 3.14, and correspondingly assume the hypotheses (if any) of the relevant theorem. Recall the parameters $\tau_* < \beta \leq d$ proved to exist for the family in (3.5), and for any sufficiently small $\varepsilon_0 > 0$, let $\delta \leq 1/4$ be defined as in (3.6).*

(1) *For any $\sigma > 0$, there exists a constant D_6 such that for every $X \geq 1$, every field $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ that has $D_K \geq D_6$ and is not δ-exceptional, has the property that for any fixed conjugacy class (or finite union of conjugacy classes) $\mathscr{C}$ in G,*

$$\pi_{\mathscr{C}}(D_K^{\sigma}, \tilde{K}/\mathbb{Q}) \gg_{G,n,\sigma} \frac{D_K^{\sigma}}{\log D_K}. \tag{3.7}$$

Here $\tilde{K}$ denotes the Galois closure of K over $\mathbb{Q}$.

(2) *For any $\sigma > 0$, there exists a constant D_7 such that for every $X \geq 1$, every field $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G, X)$ that has $D_K \geq D_7$ and is not δ-exceptional, has the property that for any conjugacy class $\mathscr{C}$ of G,*

$$\pi_{\mathscr{C}}(2D_K^{\sigma}, \tilde{K}/\mathbb{Q}) - \pi_{\mathscr{C}}(D_K^{\sigma}, \tilde{K}/\mathbb{Q}) \geq 1. \tag{3.8}$$

Here $\tilde{K}$ denotes the Galois closure of K over $\mathbb{Q}$.

Finally, in either case, recall that for every $\tau > \tau_*$ there exists a constant D_3 such that for every $X \geq 1$, at most $D_3 X^{\tau+\varepsilon_0}$ fields $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ are δ-exceptional.

4 A Chebotarev density theorem conditional upon a zero-free region

The main goal of this section is to prove Theorem 3.1. A nice feature of Lagarias and Odlyzko's approach to the effective Chebotarev theorem is that it does not assume the Artin conjecture, so that Theorem B is completely unconditional. Similarly, Theorem 3.1 is unconditional, aside from the assumed zero-free region. This is made possible by using Lagarias and Odlyzko's technical trick (originally due to Deuring) of expressing ζ_L as a product of Hecke L-functions, where L/k is a Galois extension of number fields with $\mathrm{Gal}(L/k) \simeq G$. Fixing an element $g \in G$ and letting $H = \langle g \rangle$ be the cyclic subgroup of G generated by g, then upon setting E to be the fixed field L^H, Lagarias and Odlyzko obtain the product expression on the left, in which χ varies over the irreducible characters of H:

$$\prod_{\chi \text{ irred}} L(s, \chi, L/E) = \zeta_L(s) = \prod_{\rho_j} L(s, \rho_j, L/k)^{\dim \rho_j}. \tag{4.1}$$

Each such factor is a Hecke L-function and hence is known to be entire if χ is nontrivial. On the other hand, once we have Theorem 3.1, to deduce the assumed zero-free region via Kowalski-Michel, we will also factor $\zeta_L(s)$ as on the right-hand side, as a product of Artin L-functions, which we then need to show (or assume) are automorphic L-functions with certain properties.

If one is willing to assume the Artin conjecture, so that each factor on the right-hand side of (4.1) with ρ_j nontrivial is entire, a Chebotarev density theorem with an effective error term is relatively quick to prove, since either a standard zero-free region (or the GRH zero-free region) may be applied to each of these Artin L-functions, obviating the alternative Hecke factorization; see for example, [42, §5.13 and Thm. 4.13]. (The conjugacy class $\mathscr{C}$ of interest is picked out via trace functions, much as in Dirichlet's theorem on primes $p \equiv a \pmod q$, the residue class of interest is picked out via Dirichlet characters.) In our application to families of fields we do indeed assume the strong Artin conjecture (or it is known). Nevertheless, to prove Theorem 3.1 we have used the Lagarias-Odlyzko approach, as we expect its unconditionality to be useful for other applications.

4.1 Standard lemmas on zeroes

We recall the currently best known zero free region for $\zeta(s)$, due to Vinogradov [79] and Korobov [47].

Lemma 4.1 (Vinogradov–Korobov zero-free region for $\zeta(s)$) *There exists an absolute constant $c_{\mathbb{Q}} > 0$ such that $\zeta(s)$ has no zero $s = \sigma + it$ in the region*

$$\sigma \geq 1 - \frac{c_{\mathbb{Q}}}{(\log(|t|+2))^{2/3}(\log\log(|t|+3))^{1/3}}. \tag{4.2}$$

We will also use a standard zero-free region for any Dedekind zeta function [42, Theorem 5.33].

Lemma 4.2 (Standard zero-free region for $\zeta_k(s)$) *Let $k/\mathbb{Q}$ be a number field of degree $n_k \geq 1$ and with absolute discriminant D_k. There exists an absolute constant $c_k > 0$ such that $\zeta_k(s)$ has no zero $s = \sigma + it$ in the region*

$$\sigma \geq 1 - \frac{c_k}{n_k^2 \log(D_k(|t|+3)^{n_k})}, \tag{4.3}$$

except possibly a simple real "exceptional" zero $\beta_0^{(k)} < 1$.

We also recall a standard count for zeroes of Dedekind zeta functions at a fixed height:

Lemma 4.3 ([42, Theorem 5.31, Proposition 5.7]) *Let $k/\mathbb{Q}$ be a number field of degree $n_k \geq 1$ and with absolute discriminant D_k. For a real variable t, let $n_k(t)$ denote the number of zeroes $\rho = \beta + i\gamma$ of $\zeta_k(s)$ with $0 < \beta < 1$ and $|\gamma - t| \leq 1$. For all real t, $n_k(t) \ll \log D_k + n_k \log(|t|+4)$.*

The corresponding result for Hecke L-functions is:

Lemma 4.4 ([50, Lemma 5.4]) *Let $n_\chi(t)$ denote the number of zeroes $\rho = \beta + i\gamma$ of a Hecke L-function $L(s, \chi, L/E)$ with $0 < \beta < 1$ and $|\gamma - t| \leq 1$. Let $F(\chi)$ denote the conductor of χ, and $A(\chi) = D_E \mathrm{Nm}_{E/\mathbb{Q}}(F(\chi))$. For all t, $n_\chi(t) \ll \log A(\chi) + n_E \log(|t|+2)$.*

4.2 Explicit description of assumed zero-free region

We now prove Theorem 3.1, using in particular the assumption, in the theorem statement, that $\zeta_L(s)/\zeta_k(s)$ is zero-free in the region

$$[1-\delta, 1] \times [-(\log D_L)^{2/\delta}, (\log D_L)^{2/\delta}]. \tag{4.4}$$

For use in potential computational applications, we specify the dependencies of all parameters on k, δ, etc., although we do not now optimize them (e.g. compared to recent work conditional on GRH in [35]), as it is not relevant for our current applications.

We may assume that L has degree $n_L > 1$ over $\mathbb{Q}$, since in the case $L = k = \mathbb{Q}$, $\pi_{\mathscr{C}}(x, L/k)$ is simply counting rational primes $p \leq x$. Our proof will proceed in two stages: first, we deduce from Theorem B of Lagarias and Odlyzko that the conclusion of Theorem 3.1 is true if x is sufficiently large. Second, for small x, we refine the method of Lagarias and Odlyzko, keeping track of the assumed zero-free region. (This manner of partitioning into large and small x has appeared in the proof of the prime ideal theorem of [17, Theorem 2.6].)

At each step, when we state that something holds for a number field k, it also applies to $k = \mathbb{Q}$; separately, we give refined statements so far applicable only to $k = \mathbb{Q}$. We do not rule out *a priori* the possibility of an exceptional zero of $\zeta_L(s)$, say β_0. Instead, in our application of Theorem B, the main idea is to assume that D_L is sufficiently large that the real interval within the region (1.3) in Theorem B is contained inside the assumed zero-free region (4.4), and thus ζ_L cannot have an exceptional zero β_0. In order to carry this out rigorously, we must be more careful, since (4.4) is an assumed zero-free region for ζ_L/ζ_k and not just ζ_L.

The function $\zeta_k(s)$ may have an exceptional (real) zero in the standard region (4.3) given in Lemma 4.2; we will denote this, if it exists, $\beta_0^{(k)}$. (Of course when $k = \mathbb{Q}$, $\zeta_k(s) = \zeta(s)$, and no such exceptional zero exists.) Since k is fixed, $\beta_0^{(k)}$ is fixed. We now fix a new parameter δ_0 so that

$$1 - \delta_0 \geq 1 - \delta, \qquad \text{and} \qquad 1 - \delta_0 > \beta_0^{(k)}; \tag{4.5}$$

we set $\delta_0 = \delta$ if $k = \mathbb{Q}$. (Throughout this section we will use the notation δ_0; in the statement of Theorem 3.1, any dependence on δ_0 is equivalently a dependence on $\beta_0^{(k)}$ and δ.) From now on, instead of the zero-free region (4.4), we work with the possibly smaller region

$$[1 - \delta_0, 1] \times [-(\log D_L)^{2/\delta}, (\log D_L)^{2/\delta}], \tag{4.6}$$

which excludes the possible fixed zero $\beta_0^{(k)}$.

By our hypothesis, the Artin L-function $\zeta_L(s)/\zeta_k(s)$ has no zeroes in the region (4.6), and it is an entire function by the Aramata-Brauer theorem; $\zeta_k(s)$ has no zeroes in the intersection of regions (4.3) and (4.6) (respectively, no zeroes in the intersection of the regions (4.2) and (4.6) if $k = \mathbb{Q}$) and is holomorphic there. Thus $\zeta_L(s)$ has no zeroes in the intersection of (4.3) and (4.6) (respectively, (4.2) and (4.6) if $k = \mathbb{Q}$).

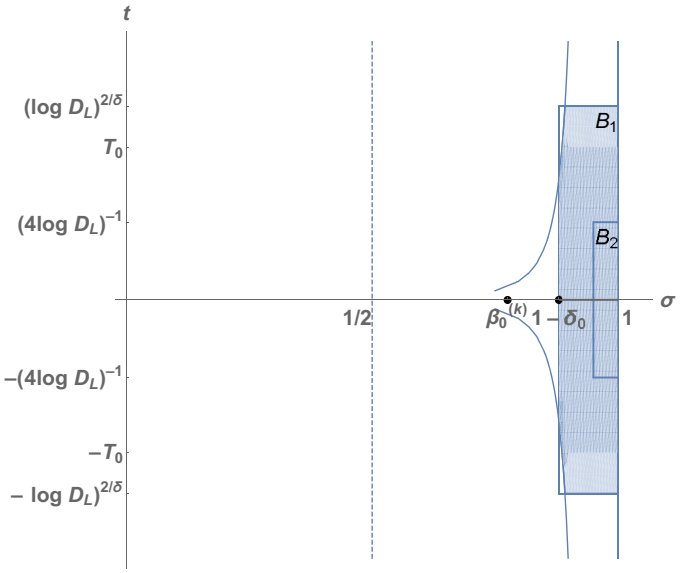


Fig. 1 The curved region represents the standard zero-free region for ζ_k and the point $\beta_0^{(k)}$ denotes the possible (real) exceptional zero of ζ_k. The larger box B_1 is the assumed zero-free region (4.6) for ζ_L/ζ_k. The shaded region represents the consequent (assumed) zero-free region for ζ_L, determined by the intersection of the known standard zero-free region for ζ_k and B_1. The box B_2 is the zero-free region (1.3) known to hold for ζ_L, aside from a possible exceptional (real) zero; we will conclude no such zero can exist in B_2 as long as D_L is sufficiently large

Thus we now specify (under the above hypotheses) the zero-free region of $\zeta_L(s)$ (see Fig. 1):

$$\begin{cases} \sigma \geq 1 - \delta_0 & \text{if } |t| \leq T_0, \\ \sigma \geq 1 - \mathscr{L}(t) & \text{if } T_0 \leq |t| \leq (\log D_L)^{2/\delta}, \end{cases} \tag{4.7}$$

where

$$\mathscr{L}(t) = \begin{cases} \dfrac{c_k}{n_k^2 \log(D_k(|t|+3)^{n_k})} & \text{general } k \\ \dfrac{c_{\mathbb{Q}}}{(\log(|t|+2))^{2/3}(\log\log(|t|+3))^{1/3}} & \text{if } k = \mathbb{Q}, \end{cases} \tag{4.8}$$

and T_0 is the height at which the zero-free region (4.3) for ζ_k (respectively (4.2) for ζ) intersects the line $\Re(s) = 1 - \delta_0$. In our Chebotarev theorems we are interested in the range where $D_L \to \infty$, so there is no harm in always assuming (for simplicity) that D_L is sufficiently large that the left-hand boundary $\Re(s) = 1 - \delta_0$ of (4.6) intersects the boundary of (4.3) (respectively (4.2) if $k = \mathbb{Q}$) at a height $T_0 \leq (\log D_L)^{2/\delta}$. For example, for a field k and the zero-free region (4.3), we compute that

$$T_0 = D_k^{-1/n_k} \exp\left(\frac{c_k}{\delta_0 n_k^3}\right) - 3. \tag{4.9}$$

A similar computation may be done to find T_0 in the case $k = \mathbb{Q}$ with the improved zero-free region (4.2). In either case, to have $T_0 \le (\log D_L)^{2/\delta}$ it is sufficient to have

$$D_L \ge \begin{cases} \exp\{\exp(c_k\delta/\delta_0)\} & \text{general } k \\ \exp\{(\exp\exp(c_{\mathbb{Q}}/\delta))^{2/\delta}\} & \text{if } k = \mathbb{Q}; \end{cases} \tag{4.10}$$

we refer to this lower bound as $D_0' = D_0'(c_k, \delta_0, \delta)$.

4.3 The proof of Theorem 3.1 for large x

With this zero-free region in mind, we dispatch the case of our Chebotarev theorem for large x, that is, for $x \ge \exp(10n_L(\log D_L)^2)$. Recall the standard zero-free region (1.3) which is known to hold for $\zeta_L(s)$, aside from a possible real exceptional zero. We may define a constant $D_1 = D_1(\delta_0)$ so that

$$1 - \delta_0 < 1 - (4\log D_1(\delta_0))^{-1}. \tag{4.11}$$

For later purposes, we also assume $D_1(\delta_0) \ge 4$. Our conclusion now is that for $D_L \ge D_1(\delta_0)$, ζ_L can have no (real, exceptional) zero in the region (1.3), and thus under the hypotheses of Theorem 3.1, the result of Theorem B holds without the β_0 term.

Now in order to show the remaining error term in Theorem B (with absolute constants C_1, C_2) is sufficiently small, as claimed in Theorem 3.1, we need only verify that there exists a constant $D_1' = D_1'(C_1, C_2, n_L, A)$ such that as long as $D_L \ge D_1'$, for all $x \ge \exp(10n_L(\log D_L)^2)$,

$$C_1 x \exp(-C_2 n_L^{-1/2}(\log x)^{1/2}) \le \frac{|\mathscr{C}|}{|G|} x(\log x)^{-A}. \tag{4.12}$$

In fact it suffices that D_L is sufficiently large that (4.12) holds at the endpoint $x = \exp(10n_L(\log D_L)^2)$, which is equivalent to requiring $D_L \ge c_2(\log D_L)^{c_3}$ with $c_2 = (c_1^{-1/(2A)}(10n_L)^{1/2})^{(2A)C_2^{-1}10^{-1/2}}$ and $c_3 = 2AC_2^{-1}10^{-1/2}$; this provides the necessary threshold D_1'. As a consequence, the conclusion of Theorem 3.1 holds for $x \ge \exp(10n_L(\log D_L)^2)$, as long as $D_L \ge \max\{D_1, D_1'\}$.

4.4 Small x

In the remaining region of small x (that is, for $x < \exp(10n_L(\log D_L)^2)$) we return to the original strategy of Lagarias and Odlyzko, which will be our focus for the remainder of Sect. 4. As in the classical prime number theorem, it is convenient to work originally with a weighted prime-counting function, defined in this case by

$$\psi_{\mathscr{C}}(x, L/k) = \sum_{\substack{\mathfrak{p},m \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}^m \le x \\ \left[\frac{L/k}{\mathfrak{p}}\right]^m = \mathscr{C}}}{}' \log(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p});$$

the final result for $\pi_{\mathscr{C}}(x, L/k)$ will then follow from partial summation. Here Σ' denotes that the sum is restricted to those prime ideals $\mathfrak{p}$ in $\mathcal{O}_k$ that are unramified in $\mathcal{O}_L$. The notation $\left[\frac{L/k}{\mathfrak{p}}\right]^m = \mathscr{C}$ denotes the requirement that if we pick any prime ideal $\mathfrak{q} \subset \mathcal{O}_L$ lying above $\mathfrak{p}$, then $\mathscr{C}$ is the conjugacy class of the m-th power $(\sigma_{\mathfrak{q}})^m$ of the Frobenius element $\sigma_{\mathfrak{q}}$ inside G. (This is well-defined no matter which prime $\mathfrak{q}$ is chosen above $\mathfrak{p}$, since if $\mathfrak{q}' = \tau(\mathfrak{q})$ for some nontrivial automorphism $\tau \in G$, then $(\sigma_{\mathfrak{q}'})^m = (\tau\sigma_{\mathfrak{q}}\tau^{-1})^m = \tau(\sigma_{\mathfrak{q}})^m\tau^{-1}$, so that they lie in the same conjugacy class in G.)

Our main result for $\psi_{\mathscr{C}}$ in the region of small x is as follows:

Proposition 4.5 *Let k be a fixed number field. Fix $A \ge 2$, $0 < \delta \le 1/(2A)$, and an integer $n \ge 1$. Let G be a fixed transitive subgroup of S_n. Then for any absolute constant $0 < c_0 \le 1$ of our choice, there exists a constant D_2 and constants $\kappa_1', \kappa_2', \kappa_3'$ such that for any Galois extension of number fields L/k with $\mathrm{Gal}(L/k) \simeq G$ such that $D_L \ge \max\{D_0', D_1, D_2\}$, and such that the Artin L-function $\zeta_L(s)/\zeta_k(s)$ is zero-free in the region*

$$[1-\delta, 1] \times [-(\log D_L)^{2/\delta}, (\log D_L)^{2/\delta}], \tag{4.13}$$

we have for every conjugacy class $\mathscr{C}$ in G that

$$\left|\psi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}x\right| \le c_0\frac{|\mathscr{C}|}{|G|}\frac{x}{(\log x)^{A-1}},$$

as long as

$$\kappa_1' \exp\{\kappa_2'(\log\log(D_L^{\kappa_3'}))^2\} \le x \le \exp\{10n_L(\log D_L)^2\}. \tag{4.14}$$

If moreover $k = \mathbb{Q}$ we may take x in the range

$$\kappa_1' \exp\left\{\kappa_2'(\log\log D_L^{\kappa_3'})^{5/3}(\log\log\log(D_L^2))^{1/3}\right\} \le x \le \exp\{10 n_L (\log D_L)^2\}. \tag{4.15}$$

Remark 4.6 Recall that D_0' was fixed by (4.10), D_1 was fixed by (4.11); we will construct D_2 explicitly in Lemma 4.10. The constants $\kappa_1', \kappa_2', \kappa_3'$ depend on c_0, D_k, n_k, n_L, δ_0, δ, A and are chosen in (4.38).

4.5 The passage to sums over zeroes of Hecke L-functions

To prove this proposition, we rebuild the argument of Lagarias and Odlyzko, inserting the zero-free region (4.7) at a key point. With $\mathscr{C}$ the fixed conjugacy class of interest, we fix any element $g \in \mathscr{C}$ and let $H = \langle g \rangle$ be the cyclic group generated by g. Then H defines a fixed field $E = L^H$ with $k \subseteq E \subseteq L$, and the cyclic group H has an associated family of irreducible one-dimensional characters. For any such character χ, we consider the Hecke L-function $L(s, \chi, L/E)$; in particular if $\chi = \chi_0$ is the trivial character on H then $L(s, \chi, L/E) = \zeta_E(s)$. The following statement provides the key framework for proving Proposition 4.5:

Proposition 4.7 (Theorem 7.1 of [50]) *For L/k a finite Galois extension of number fields with $\mathrm{Gal}(L/k) \simeq G$, cyclic subgroup $H \subseteq G$, and $k \subseteq E \subseteq L$ as described above, there exists an absolute constant $C_5 \ge 1$ such that if $x \ge 2$ and $T \ge 2$, then*

$$\left|\psi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}x\right| \le C_5 \frac{|\mathscr{C}|}{|G|}\{S(x,T) + E_1 + E_2\}, \tag{4.16}$$

in which

$$S(x,T) = \sum_{\chi} \overline{\chi}(g) \left(\sum_{\substack{\rho = \beta + i\gamma \\ |\gamma| < T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho = \beta + i\gamma \\ |\rho| < 1/2}} \frac{1}{\rho} \right),$$

where the sum is over irreducible characters χ of H, and for each character χ the inner sums are over nontrivial zeroes $\rho = \beta + i\gamma$ of the Hecke L-function $L(s, \chi, L/E)$, and

$$E_1 = xT^{-1}\log x \log D_L + \log D_L + n_L \log x + n_L x T^{-1} \log x \log T, \tag{4.17}$$

$$E_2 = \log x \log D_L + n_L x T^{-1} (\log x)^2. \tag{4.18}$$

Remark 4.8 Note that we may assume that $C_5 \geq 1$, by enlarging it if necessary. As stated in (4.18), E_2 is slightly refined over [50, Theorem 7.1], which in place of $|\mathscr{C}||G|^{-1}E_2$ has

$$E_2' = \log x \log D_L + n_k x T^{-1} (\log x)^2,$$

(without a factor of $|\mathscr{C}||G|^{-1}$). As noted in [68, Théorème 4], the first term in E_2' may be replaced by

$$|G|^{-1} \log x \log D_L \leq |\mathscr{C}||G|^{-1} \log x \log D_L,$$

by a refined estimate for a sum over prime ideals $\mathfrak{p} \subset \mathcal{O}_k$ that ramify in L. For the second term in E_2', we use the trivial observation that $n_k|G| = n_L$, so that

$$n_k x T^{-1} (\log x)^2 = |G|^{-1} n_L x T^{-1} (\log x)^2 \leq |\mathscr{C}||G|^{-1} n_L x T^{-1} (\log x)^2,$$

as claimed.

With Proposition 4.7 in hand, Lagarias and Odlyzko use zero-free regions (either unconditional or on GRH) to deduce a bound for $S(x, T)$, which indicates an appropriate choice for the height T that guarantees all the error terms are sufficiently small. We proceed with a different zero-free region and a different choice for T, namely

$$T = (\log D_L)^{2/\delta}, \tag{4.19}$$

where δ is provided from our assumed zero-free region (4.7). (In particular, we may assume that $T \geq 2$ as long as $D_L \geq 3 > \exp(2^{\delta/2})$, upon recalling $\delta \leq 1/4$.)

4.6 Bounding the contribution of zeroes $|\rho| < 1/2$ in $S(x, T)$

The contribution to $S(x, T)$ from $|\rho| < 1/2$ (so that certainly $|\gamma| \leq T$ with T as in (4.19)) is bounded by:

$$\sum_{\chi} \sum_{\substack{|\rho|<1/2 \\ |\gamma|\leq T}} \left\{ \left| \frac{x^\rho}{\rho} \right| + \left| \frac{1}{\rho} \right| \right\} \ll x^{1/2} \sum_{\chi} \sum_{|\rho|<1/2} \left| \frac{1}{\rho} \right| \ll x^{1/2} n_L (\log D_L)^2, \tag{4.20}$$

in which the implied constant is absolute. The first inequality is clear; to prove the second inequality, recall the factorization (4.1) into Hecke L-functions,

$$\zeta_L(s) = \zeta_E(s) \prod_{\chi \neq \chi_0} L(s, \chi, L/E), \tag{4.21}$$

with the product over non-trivial irreducible characters of H. The Hecke L-functions are entire, and $\zeta_E(s)$ and $\zeta_L(s)$ each have their only pole at $s = 1$; thus (rigorously by multiplying both sides of the identity by $(s-1)$), it follows that none of the factors on the right hand side of (4.21) have a zero in the region (4.7). Recalling that (4.7) contains the region (1.3) since $D_L \geq D_1(\delta_0)$ we may conclude (by the functional equation) that each $L(s, \chi, L/E)$ is zero-free both in (1.3) and in $0 \leq \sigma \leq (4 \log D_L)^{-1}$, $|t| \leq (4 \log D_L)^{-1}$. Thus the only zeroes that can appear in (4.20) must have $|\rho| \geq (4 \log D_L)^{-1}$; recalling the notation of Lemmas 4.3 and 4.4, we then see that for each χ,

$$\sum_{|\rho|<1/2} \left| \frac{1}{\rho} \right| \leq 4(\log D_L) n_\chi(1) \ll (\log D_L)(\log A(\chi) + n_E \log 3) \tag{4.22}$$

with the implied constant being absolute. The conductor-discriminant formula [61, Ch. VII 11.9] shows

$$\begin{aligned} \sum_\chi \log A(\chi) &= \log \left[D_E^{|H|} \mathrm{Nm}_{E/\mathbb{Q}} \left(\prod_\chi F(\chi) \right) \right] \\ &= \log \left[D_E^{[L:E]} \mathrm{Nm}_{E/\mathbb{Q}}(D_{L/E}) \right] = \log D_L. \end{aligned} \tag{4.23}$$

Thus, summing (4.22) over χ we have

$$\sum_\chi \sum_{|\rho|<1/2} \left| \frac{1}{\rho} \right| \ll (\log D_L)^2 + n_E |H| \log 3 \ll n_L (\log D_L)^2,$$

with an absolute implied constant, verifying (4.20).

4.7 Bounding the contribution of $|\gamma| \leq T$ in $S(x, T)$

Suppose that $\rho = \beta + i\gamma$ is a nontrivial zero of $L(s, \chi, L/E)$ with $|\gamma| \leq T$ and $|\rho| > 1/2$. Recalling the definition (4.9) of the height T_0, by the assumption of the zero-free region (4.7), we know that *without exception,* all zeroes ρ with $|\gamma| \leq T_0$ have $\beta \leq 1 - \delta_0$, so that $|x^\rho| = x^\beta \leq x^{1-\delta_0}$. Similarly, all zeroes ρ with $T_0 \leq |\gamma| \leq T$ have $\beta \leq 1 - \mathscr{L}(T)$, so that $|x^\rho| = x^\beta \leq x^{1-\mathscr{L}(T)}$. We also note that for any fixed χ, by Lemma 4.4,

$$\begin{aligned} \sum_{|\gamma| \leq T_0} \left| \frac{x^\rho}{\rho} \right| &\ll x^{1-\delta_0} \sum_{j \leq T_0} \frac{n_\chi(j)}{j} \\ &\ll x^{1-\delta_0} (\log T_0)(\log A(\chi) + n_E \log T_0) \end{aligned}$$

$$\ll x^{1-\delta_0}(\log T)(\log A(\chi) + n_E \log T);$$

similarly,

$$\sum_{T_0 \le |\gamma| \le T} \left| \frac{x^\rho}{\rho} \right| \ll x^{1-\mathscr{L}(T)}(\log T)(\log A(\chi) + n_E \log T).$$

Summing over all χ as in (4.23), we see that

$$x^{1-\delta_0} \sum_{\chi} (\log T)(\log A(\chi) + n_E \log T) \ll x^{1-\delta_0}(\log T)\{\log D_L + n_L \log T\},$$

and, likewise,

$$\begin{aligned} x^{1-\mathscr{L}(T)} \sum_{\chi} (\log T)(\log A(\chi) + n_E \log T) \\ \ll x^{1-\mathscr{L}(T)}(\log T)\{\log D_L + n_L \log T\}. \end{aligned}$$

Combining these estimates with (4.20), we may conclude

$$|S(x, T)| \le C_6 \{E_3 + E_4 + E_5\}, \tag{4.24}$$

for an absolute constant C_6 (which we may assume satisfies $C_6 \ge 1$), and

$$\begin{aligned} E_3 &= x^{1/2} n_L (\log D_L)^2 \\ E_4 &= x^{1-\delta_0}(\log T) \log(D_L T^{n_L}) \\ E_5 &= x^{1-\mathscr{L}(T)}(\log T) \log(D_L T^{n_L}). \end{aligned}$$

The proof of Proposition 4.5 will then be complete, upon verification of two lemmas, which we record as Lemmas 4.9 and 4.10 below.

Lemma 4.9 *Let k be a fixed number field. Let $A \ge 2$ be fixed and let $0 < \delta \le 1/(2A)$ be a fixed positive constant; define δ_0 from δ as in (4.5) according to whether or not $\zeta_k(s)$ has an exceptional zero. Let L/k be a Galois extension of number fields with $\mathrm{Gal}(L/k) \simeq G$, and assume that the Artin L-function $\zeta_L(s)/\zeta_k(s)$ is zero-free in the region*

$$[1 - \delta, 1] \times [-(\log D_L)^{2/\delta}, (\log D_L)^{2/\delta}]. \tag{4.25}$$

For $D_L \ge D_1(\delta_0)$ (as defined in (4.11)), for any choice of absolute constant $0 < c_1 \le 1$, we have

$$|S(x, T)| \le 3 c_1 C_6 x (\log x)^{-(A-1)} \tag{4.26}$$

for all

$$\kappa_1'' \exp\{\kappa_2''(\log\log(D_L^{\kappa_3''}))^2\} \le x \le \exp\{10 n_L (\log D_L)^2\}, \tag{4.27}$$

where

$$\begin{aligned} \kappa_1'' &:= (6c_1^{-1} 10^{A-1} n_L^A)^{1/\delta_0} \delta^{-2/\delta_0} \\ \kappa_2'' &:= \max\{2A\delta_0^{-1}, 4Ac_k^{-1} n_k^3 \delta^{-1}\} \\ \kappa_3'' &:= 6c_1^{-1/(2A)} D_k n_L \delta^{-1/A}. \end{aligned} \tag{4.28}$$

Moreover, if $k = \mathbb{Q}$ we may consider all

$$\kappa_1'' \exp\left\{\kappa_2''(\log\log(D_L^{\kappa_3''}))^{5/3} (\log\log\log(D_L^2))^{1/3}\right\} \le x \le \exp\{10 n_L (\log D_L)^2\}. \tag{4.29}$$

It is in Lemma 4.9 that we fully utilize the fact that the zero-free region (4.6) has a width that is independent of D_L; this is key to obtaining a small lower threshold on x.

Proof The lemma is proved by simple computations. For any field k, we see that in the range $x \le \exp(10 n_L (\log D_L)^2)$, to guarantee $|E_3| \le c_1 x (\log x)^{-(A-1)}$ it suffices that

$$x \ge c_1^{-2} (10)^{2(A-1)} n_L^{2A} (\log D_L)^{4A};$$

here we have explicitly used the upper bound $x \le \exp(10 n_L (\log D_L)^2)$. Similarly for such an upper bound for E_4 it suffices to have

$$x \ge (6c_1^{-1} (10)^{A-1} n_L^A)^{1/\delta_0} \delta^{-2/\delta_0} (\log D_L)^{2A/\delta_0},$$

provided that $T = (\log D_L)^{2/\delta}$ and $x \le \exp(10 n_L (\log D_L)^2)$. Since $\delta_0 \le \delta \le 1/4$, both of the lower bounds for x displayed above are satisfied if

$$x \ge (6c_1^{-1} 10^{A-1} n_L^A)^{1/\delta_0} \delta^{-2/\delta_0} \exp\{2A\delta_0^{-1} \log\log D_L\}. \tag{4.30}$$

The distinction of $k = \mathbb{Q}$ only appears in the treatment of E_5; in the case of $k = \mathbb{Q}$, it suffices to find a lower bound on x such that

$$x^{1 - \frac{c_{\mathbb{Q}}}{(\log(T+2))^{2/3} (\log\log(T+3))^{1/3}}} (\log T) \log(D_L T^{n_L}) \le c_1 x (\log x)^{-(A-1)},$$

as long as $x \le \exp(10 n_L (\log D_L)^2)$, $T = (\log D_L)^{2/\delta}$ and $D_L \ge D_1(\delta_0)$. Here one sees that it would suffice to have

$$x \geq \exp\{2Ac_{\mathbb{Q}}^{-1}(\log(2(\log D_L)^{2/\delta}))^{2/3}(\log\log(2(\log D_L)^{2/\delta}))^{1/3} \cdot \log[c_2^{1/(2A)}\delta^{-1/A}(\log D_L)]\},$$

with $c_2 = 6c_1^{-1}(10)^{A-1}n_L^A$, which can be simplified as the requirement that x is at least

$$\exp\left\{4Ac_{\mathbb{Q}}^{-1}\delta^{-2/3}(\log(2\delta^{-1})+1)^{1/3}\left(\log\log D_L^{\max\{2^{\delta/2},c_2^{1/(2A)}\delta^{-1/A}\}}\right)^{5/3}\left(\log\log\log D_L^{2^{\delta/2}}\right)^{1/3}\right\}. \tag{4.31}$$

Note that $2^{\delta/2} \leq 2$, $\log(2\delta^{-1})+1 \leq \delta^{-1}$ for all $\delta \leq 1/4$, and $c_2^{1/2A}\delta^{-1/A} \leq 6c_1^{-1/(2A)}n_L\delta^{-1/A}$. Thus upon comparing (4.30) and (4.31), we see that (4.29) suffices with κ_i'' defined as above (specialized to the case $k = \mathbb{Q}$); the case of other fields k follows from analogous computations. □

Lemma 4.10 *Let k be a fixed number field. Let $A \geq 2$ be fixed and let $0 < \delta \leq 1/(2A)$ be a fixed positive constant. Let L/k be a Galois extension of number fields with $\mathrm{Gal}(L/k) \simeq G$. Set $T = (\log D_L)^{2/\delta}$. Given any absolute constant $0 < c_1' \leq 1$, there exists a constant D_2 such that for $D_L \geq D_2$,*

$$|E_1| + |E_2| \leq 6c_1' x(\log x)^{-(A-1)} \tag{4.32}$$

for all

$$(c_1')^{-1}10^A n_L^{A+1}(\log D_L)^{2A+1} \leq x \leq \exp(10n_L(\log D_L)^2). \tag{4.33}$$

Proof This is proved by simple computations checking error terms in the range of "small" x, that is $x \leq \exp(10n_L(\log D_L)^2)$, and recalling $T = (\log D_L)^{2/\delta}$. Writing $E_1 = E_{1,a} + \cdots + E_{1,d}$ and $E_2 = E_{2,a} + E_{2,b}$ we see that for example $|E_{1,a}| \leq c_1' x(\log x)^{-(A-1)}$ for $x \leq \exp(10n_L(\log D_L)^2)$ if $\delta < 2/(2A+1)$ and

$$D_L \geq \exp\{(c_1'^{-1}(10n_L)^A)^{(1/\delta-2A-1)^{-1}}\}. \tag{4.34}$$

Similarly, $E_{1,b}$, $E_{1,c}$, $E_{2,a}$ are seen to be sufficiently small if x is bounded below as in (4.33). The remaining two terms $E_{1,d}$ and $E_{2,b}$ impose (respectively) the constraints $\delta < 2/(2A+1)$ and

$$D_L \geq \exp\{(2 \cdot 10^A n_L^{A+1}c_1'^{-1})^{(2/\delta-2A-1)^{-1}}\}, \tag{4.35}$$

and $\delta < 1/(A+1)$,

$$D_L \geq \exp\{(10^{A+1}n_L^{A+2}c_1'^{-1})^{(2/\delta-2(A+1))^{-1}}\}. \tag{4.36}$$

It suffices to assume $\delta \le 1/(2A)$ and to take $D_2 = D_2(c_1', \delta, n_L, A)$ to be the maximum of (4.34), (4.35) and (4.36). □

4.8 Proof of Proposition 4.5

To deduce Proposition 4.5, for a fixed absolute constant c_0, from these lemmas, we will apply Lemmas 4.9 and 4.10 with the respective choices

$$c_1 = c_0/(6C_5C_6), \qquad c_1' = c_0/(12C_5), \tag{4.37}$$

where C_5 and C_6 are the absolute constants arising in (4.16) and (4.24) from the Lagarias-Odlyzko argument. After this choice in Lemma 4.10, we could denote the dependencies of $D_2(c_1', \delta, n_L, A)$ by $D_2(c_0, C_5, \delta, n_L, A)$. The last step of the proof of Proposition 4.5 is to check that we can ensure that the parameters are such that (4.33) holds whenever (4.27) (or (4.29) respectively) is satisfied. Note that the lower bound in (4.33) will hold if we have

$$\begin{aligned} x &\ge \exp\{(2A+1)\log\log(D_L^{(c_1')^{-1/(2A+1)}10^{1/2}n_L})\} \\ &\ge \exp\{(2A+1)\log\log(D_L^{((c_1')^{-1}10^A n_L^{A+1})^{1/(2A+1)}})\}. \end{aligned}$$

Thus either for general k or $k = \mathbb{Q}$ it suffices to set

$$\kappa_1' = \kappa_1'' \ge 1, \quad \kappa_2' = \kappa_2'' = \max\{\kappa_2'', 2A+1\}, \quad \kappa_3' = (c_1')^{-1/(2A+1)}\kappa_3''. \tag{4.38}$$

4.9 Partial summation back to prime counting

There are two remaining steps to pass from Proposition 4.5 to Theorem 3.1 (in the regime of small x). First, we define the function

$$\theta_{\mathscr{C}}(x, L/k) = \sum_{\substack{\mathfrak{p} \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \le x \\ \left[\frac{L/k}{\mathfrak{p}}\right] = \mathscr{C}}}{}' \log(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}) = \sum_{\substack{\mathfrak{p} \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \le x}}{}' \mathbf{1}_{\mathscr{C}}(\sigma_{\mathfrak{q}}) \log(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}),$$

in which the sum is restricted to prime ideals $\mathfrak{p} \subset \mathcal{O}_k$ that are unramified in L, and we fix any prime ideal $\mathfrak{q}$ in $\mathcal{O}_L$ above $\mathfrak{p}$ and let $\mathbf{1}_{\mathscr{C}}$ detect whether the conjugacy class of the Frobenius element $\sigma_{\mathfrak{q}}$ is $\mathscr{C}$. A Chebyshev argument shows that $\theta_{\mathscr{C}}(x, L/k)$ is well-approximated by $\psi_{\mathscr{C}}(x, L/k)$ and then partial summation passes from $\theta_{\mathscr{C}}(x, L/k)$ back to $\pi_{\mathscr{C}}(x, L/k)$; we only mention the highlights. We note that

$$\psi_{\mathscr{C}}(x, L/k) - \theta_{\mathscr{C}}(x, L/k) = \sideset{}{'}\sum_{\substack{\mathfrak{p}, m \geq 2 \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}^m \leq x}} \mathbf{1}_{\mathscr{C}}(\sigma_{\mathfrak{q}}^m) \frac{1}{m} \log(\mathrm{Nm}_{k/\mathbb{Q}}(\mathfrak{p}^m)),$$

so that upon setting m to be the smallest integer such that $x^{1/m} \geq 2$ (so in particular $m \leq \log x / \log 2$), the above difference is at most

$$\frac{\log x}{\log 2} \left(\frac{1}{2} \pi(x^{1/2}, L/k) + \cdots + \frac{1}{m} \pi(x^{1/m}, L/k) \right) \leq \frac{3}{2 \log 2} n_k x^{1/2} \log x,$$

where we have denoted by $\pi(x, L/k)$ the counting function for prime ideals (unramified in L) with $\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x$. Thus we see that the statement of Proposition 4.5 holds for $\theta_{\mathscr{C}}(x, L/k)$ in place of $\psi_{\mathscr{C}}(x, L/k)$, with an additional error term of size at most $3n_k x^{1/2} \log x$, which is no bigger than $c_0 |\mathscr{C}| |G|^{-1} x (\log x)^{-(A-1)}$ (for an absolute constant $c_0 \leq 1$ we will choose later) as soon as the sufficient condition $3|G| n_k = 3n_L \leq c_0 x^{1/2} (\log x)^{-A}$ is met. It is simple to check that this holds in the regimes (4.14) or (4.15) we consider in Proposition 4.5, with the parameters κ_i' as already defined. Thus for x in either range we have

$$\left| \theta_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|} x \right| \leq 2c_0 \frac{|\mathscr{C}|}{|G|} \frac{x}{(\log x)^{A-1}}. \tag{4.39}$$

Let x_0 denote the lower bound for x in (4.14) for general k and for x in the range (4.15) for $k = \mathbb{Q}$, respectively. To pass from $\theta_{\mathscr{C}}(x)$ to $\pi_{\mathscr{C}}(x)$ (temporarily suppressing the notational dependence on L/k for simplicity), we let λ_n be an increasing sequence of positive real numbers running over the norms $\mathrm{Nm}_{k/\mathbb{Q}}(\mathfrak{p})$ attained by prime ideals of k (unramified in L). By partial summation, for any $x_0 \leq x \leq \exp\{10 n_L (\log D_L)^2\}$,

$$\pi_{\mathscr{C}}(x) = \sum_{\lambda_n \leq x} \left(\sideset{}{'}\sum_{\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} = \lambda_n} \mathbf{1}_{\mathscr{C}}(\sigma_{\mathfrak{q}}) \log \lambda_n \right) (\log \lambda_n)^{-1} = \int_{\lambda_1}^{x} \frac{\theta_{\mathscr{C}}(t) dt}{t \log^2 t} + \frac{\theta_{\mathscr{C}}(x)}{\log x}. \tag{4.40}$$

We split the integral into the region $\lambda_1 \leq t \leq x_0$, in which the asymptotic (4.39) has not been verified, and the region $x_0 \leq t \leq x$, in which it has. For the first portion of the integral we apply the trivial bound $\theta_{\mathscr{C}}(t) \leq n_k t \log t$ to see that this integral contributes at most $n_k \mathrm{Li}(x_0)$. In the remaining contributions to (4.40), we may replace $\theta_{\mathscr{C}}(t)$ by $|\mathscr{C}||G|^{-1} t$ as in (4.39) (deferring the error terms for a moment), and similarly for $\theta_{\mathscr{C}}(x)$; this main contribution becomes after integration by parts

$$\frac{|\mathscr{C}|}{|G|}\left[\int_{x_0}^{x} t\frac{d}{dt}\left(-\frac{1}{\log t}\right)dt+\frac{x}{\log x}\right]=\frac{|\mathscr{C}|}{|G|}\left[\mathrm{Li}(x)-\left(\mathrm{Li}(x_0)-\frac{x_0}{\log x_0}\right)\right]. \tag{4.41}$$

The error terms accrued via this replacement are (in absolute value) at most

$$2c_0\frac{|\mathscr{C}|}{|G|}\int_{x_0}^{x}\frac{dt}{(\log t)^{A+1}}+2c_0\frac{|\mathscr{C}|}{|G|}\frac{x}{(\log x)^A}. \tag{4.42}$$

In the first term of (4.42) we may bound the contribution from, say, $x_0 \le t \le x^{1/2}$ trivially by $2c_0|\mathscr{C}||G|^{-1}x^{1/2}$ while in the remaining portion we have $\log t \ge (1/2)\log x$, yielding a total contribution of at most $2^{A+2}c_0|\mathscr{C}||G|^{-1}x(\log x)^{-(A+1)}$; we trivially dominate this from above by $2^{A+2}c_0|\mathscr{C}||G|^{-1}x(\log x)^{-A}$ so that we may combine it with the second term in (4.42). Finally, we crudely bound the last two terms in (4.41), in absolute value, by $2\mathrm{Li}(x_0)$. In total, we have represented $\pi_{\mathscr{C}}(x)$ as $|\mathscr{C}||G|^{-1}\mathrm{Li}(x)+E$ where

$$\begin{aligned}|E| &\le (n_k+2)\mathrm{Li}(x_0)+2c_0|\mathscr{C}||G|^{-1}x^{1/2}+(2^{A+2}+2)c_0|\mathscr{C}||G|^{-1}x(\log x)^{-A}\\ &\le (n_k+2)\mathrm{Li}(x_0)+(2^{A+2}+4)c_0|\mathscr{C}||G|^{-1}x(\log x)^{-A}.\end{aligned} \tag{4.43}$$

Here we have used that $x^{1/2} \le x(\log x)^{-A}$ in the regime of $x \le \exp\{10n_L(\log D_L)^2\}$ as soon as $x \ge \exp\{4A\log\log(D_L^{10^{1/2}n_L^{1/2}})\}$, which holds for all $x \ge x_0$. The first term on the right-hand side of (4.43) is certainly dominated by the second as long as

$$\frac{x}{(\log x)^A} \ge \frac{|G|(n_k+2)}{(2^{A+2}+4)|\mathscr{C}|c_0}\mathrm{Li}(x_0), \tag{4.44}$$

for which it suffices to have $x \ge n_L c_0^{-1}x_0(\log x)^A$. Of course, we are already assuming that $x \ge x_0$; recalling that we presently only consider $x \le \exp\{10n_L(\log D_L)^2\}$ we see that (4.44) holds as long as

$$x \ge 10^A n_L^{A+1}c_0^{-1}x_0(\log D_L)^{2A} = 10^A n_L^{A+1}c_0^{-1}\exp\{2A\log\log D_L\}\cdot x_0. \tag{4.45}$$

Under this condition, we have shown that

$$|E| \le 2(2^{A+2}+4)c_0|\mathscr{C}||G|^{-1}x(\log x)^{-A} \le |\mathscr{C}||G|^{-1}x(\log x)^{-A},$$

upon making the choice

$$c_0 = (2^{A+3}+8)^{-1}. \tag{4.46}$$

We may accommodate the requirement (4.45) simply by enlarging the parameters κ_i' by setting $\kappa_1 = c_0^{-1}\kappa_1'$, $\kappa_2 = \kappa_2' + 2A$, $\kappa_3 = \kappa_3' \geq 1$. We record the definitions here, with c_0 as in (4.46):

$$\begin{aligned}\kappa_1 &= c_0^{-1}(6(\frac{c_0}{12C_5C_6})^{-1}10^{A-1}n_L^A)^{1/\delta_0}\delta^{-2/\delta_0}\\ \kappa_2 &= \max\{2A\delta_0^{-1}, 4Ac_k^{-1}n_k^3\delta^{-1}\} + 2A\\ \kappa_3 &= 6(\frac{c_0}{12C_5})^{-1/(2A+1)}(\frac{c_0}{12C_5C_6})^{-1/(2A)}D_k n_L\delta^{-1/A}.\end{aligned} \tag{4.47}$$

To conclude, for x in the ranges (4.14) and (4.15) with κ_i' replaced by κ_i, we have verified the effective error term in the asymptotic for $\pi_{\mathscr{C}}(x, L/k)$. This completes the treatment of small x, and combining this with the result of Sect. 4.3 for large x, we may conclude that Theorem 3.1 holds.

Remark 4.11 The threshold $D_0 = D_0(\delta, c_k, \beta_0^{(k)}, n_L, C_1, C_2, A)$ appearing in Theorem 3.1 is the maximum of D_0' in (4.10), D_1 in (4.11), D_1' defined in Sect. 4.3, and D_2 defined as the most restrictive of (4.34), (4.35), (4.36) (with the imposed choices $c_1' = c_0/12C_5$ and $c_0 = (2^{A+3}+8)^{-1}$).

4.10 Remark: A Chebotarev theorem for fields without quadratic subfields

In the introduction, we stated that one of our two goals was to remove the β_0 term in Theorem B. As an aside, we note that for certain fields, the existence of an exceptional zero can already be ruled out, so that an immediate application of Theorem B yields:

Theorem 4.12 *Let k be a number field such that $\zeta_k(s)$ has no real zeroes. Let L/k be a Galois extension of relative degree at least 3 such that L/k contains no quadratic extension of k. Then there exist absolute effectively computable constants C_1, C_2 such that for all $x \geq \exp(10n_L(\log D_L)^2)$,*

$$\left|\pi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x)\right| \leq C_1 x\exp(-C_2 n_L^{-1/2}(\log x)^{1/2}). \tag{4.48}$$

Remark 4.13 In particular, if $k = \mathbb{Q}$ this theorem holds unconditionally for any $L/\mathbb{Q}$ such that $G = \mathrm{Gal}(L/\mathbb{Q})$ with $|G| \geq 3$ has no subgroup of index 2 (for example, $G \simeq C_p$ for p an odd prime).

Theorem 4.12 is an application of a nice idea of Stark [73, Theorem 3], in turn a refinement of a theorem of Heilbronn [39]. (See also further work on eliminating Siegel zeroes in towers of fields in [58,63].)

Theorem D ([73, Theorem 3]) *Let L be a Galois extension of k with $\mathrm{Gal}(L/k) \simeq G$ and let χ be a character of G. Suppose ρ is a simple zero of $\zeta_L(s)$. Then $L(s, \chi, L/k)$ is analytic at $s = \rho$. Furthermore, there is a field F with $k \subseteq F \subseteq L$ such that F/k is cyclic and for any field E with $k \subseteq E \subseteq L$, $\zeta_E(\rho) = 0$ if and only if $F \subseteq E$. If in particular ρ is real, then either $F = k$ or F is quadratic over k.*

By Theorem B, we need only consider a possible real zero of $\zeta_L(s)$, which by Theorem D (and the assumption that $\zeta_k(s)$ has no real zero) can only occur if there is a quadratic extension F of k contained in L. No such F can exist if $\mathrm{Gal}(L/k)$ has no index 2 subgroup. Nevertheless, as remarked before, the lower bound on x in Theorem 4.12 is too large for our ultimate application to ℓ-torsion, a problem which Theorem 3.1 alleviates via careful attention to the assumed box-shaped zero-free region.

5 A zero density result for families of Dedekind zeta functions

We have proved a Chebotarev density theorem conditional on a box-shaped zero-free region for $\zeta_L(s)/\zeta_k(s)$. Now we restrict our attention to $k = \mathbb{Q}$ and show that within appropriate families of Galois extensions of $\mathbb{Q}$, except for a possible exceptional subfamily of density zero within the family, each $\zeta_L(s)/\zeta(s)$ is in fact zero-free in the desired region. To do so we will build on the result of Kowalski and Michel [45, Thm. 2] on the density of zeroes among a family of cuspidal automorphic L-functions. We describe our approach somewhat generally to facilitate future applications, and then specialize to our present setting.

5.1 The Kowalski-Michel zero density estimate

Let $m \geq 1$ be fixed. For any cuspidal automorphic representation ρ of $\mathrm{GL}(m)/\mathbb{Q}$, define the zero-counting function for the corresponding automorphic L-function $L(s, \rho)$ in a region with $\alpha \in [1/2, 1]$, $T \geq 0$ by

$$N(\rho; \alpha, T) = |\{s = \beta + i\gamma : \beta \geq \alpha, |\gamma| \leq T, L(s, \rho) = 0\}|,$$

counting with multiplicity. For an isobaric representation $\pi = \rho_1 \boxplus \cdots \boxplus \rho_r$ with ρ_j cuspidal, define

$$N(\pi; \alpha, T) = N(\rho_1; \alpha, T) + \cdots + N(\rho_r; \alpha, T), \tag{5.1}$$

again counting each zero with multiplicity.

The main outcome of [45] is a bound for $N(\rho; \alpha, T)$ that holds on average for an appropriate family of cuspidal representations ρ. Our innovation is to

develop a means to apply their results to the case when π varies over an appropriate family of isobaric representations, in our case, obtained from Dedekind zeta functions. We first recall the original setting for cuspidal representations, which assumes the following conditions hold:

Condition 5.1 *For each $X \geq 1$ let $S(X)$ be a finite (possibly empty) set of cuspidal automorphic representations ρ of $\mathrm{GL}(m)/\mathbb{Q}$ such that the following properties hold for $(S(X))_{X\geq 1}$:*

(i) *Every $\rho \in S(X)$ satisfies the Ramanujan-Petersson conjecture at the finite places.*
(ii) *There exists $A > 0$ and a constant M_0 such that for all $X \geq 1$, for all $\rho \in S(X)$, $\mathrm{Cond}(\rho) \leq M_0 X^A$.*
(iii) *There exists $d > 0$ and a constant M_1 such that for all $X \geq 1$, $|S(X)| \leq M_1 X^d$.*
(iv) *For any $\varepsilon > 0$ there exists a constant $M_{2,\varepsilon}$ such that for all $\rho \in S(X)$ we have the convexity bound*

$$|L(s,\rho)| \leq M_{2,\varepsilon}(\mathrm{Cond}(\rho)(|t|+2)^m)^{(1-\Re(s))/2+\varepsilon}, \qquad \text{for } 0 \leq \Re(s) \leq 1.$$

For any $\varepsilon > 0$ there exists a constant $M_{3,\varepsilon}$ such that for all $\rho \not\simeq \rho' \in S(X)$ we have the convexity bound

$$|L(s,\rho\otimes\rho')| \leq M_{3,\varepsilon}(\mathrm{Cond}(\rho\otimes\rho')(|t|+2)^{m^2})^{(1-\Re(s))/2+\varepsilon}, \quad \text{for } 0 \leq \Re(s) \leq 1.$$

Remark 5.2 Kowalski and Michel call $(S(X))_{X\geq 1}$ a *family* of automorphic representations, with associated automorphic L-functions; following their convention we will call the associated collection of constants $\{m, A, d, M_0, M_1, M_{2,\varepsilon}, M_{3,\varepsilon}\}$ the family parameters.

Remark 5.3 It is worth comparing precisely Condition 5.1 to the hypotheses originally stated in the work of [45]. We note that the above criteria (i)–(iii) reduce to exactly the criteria of [45, Thm. 2]; Condition (iv) above replaces their assumption that all the L-functions in $(S(X))_{X\geq 1}$ have the same gamma factors at infinity. That condition is only used in order to attain the uniform convexity bounds of [45, Lemma 10] (Kowalski, personal communication), and thus we merely assume the relevant uniform convexity bounds directly.

In this context, we recall Kowalski and Michel's original theorem:

Theorem E ([45, Theorem 2]) *Let $(S(X))_{X\geq 1}$ be a family of cuspidal automorphic representations of* $\mathrm{GL}(m)/\mathbb{Q}$ *satisfying Condition 5.1. Let $\alpha \geq 3/4$ and $T \geq 2$. Then there exists a constant $c_0' = c_0'(m, A, d)$, in particular*

$$c_0' = \frac{5mA}{2} + d \tag{5.2}$$

and a constant $B \geq 0$, depending only on the family parameters, such that for every choice of $c_0 > c_0'$ we have that there exists a constant M_{4,c_0} depending only on c_0 such that for all $X \geq 1$,

$$\sum_{\rho \in S(X)} N(\rho; \alpha, T) \leq M_{4,c_0} T^B X^{c_0 \frac{1-\alpha}{2\alpha-1}}.$$

5.2 Defining a family of automorphic representations

Fix $n \geq 2$ and a transitive subgroup $G \subseteq S_n$. Let $\mathscr{F}(\mathbb{Q}, G) \subset Z_{|G|}(\mathbb{Q}, G)$ be a set of Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$, and let $\mathscr{F}(\mathbb{Q}, G; X)$ denote the finite subset comprised of those fields with $D_L = |\mathrm{Disc}\, L/\mathbb{Q}| \leq X$. (Momentarily we will construct such a set from each of the families $Z_n^{\mathscr{J}}(\mathbb{Q}, G)$ of degree n fields considered in our main theorems.)

Denote the irreducible representations of G by $\rho_0, \rho_1, \ldots, \rho_s$, with ρ_0 being the trivial representation. For each field $L \in \mathscr{F}(\mathbb{Q}, G; X)$, the Dedekind zeta function may be written as

$$\zeta_L(s) = \zeta(s) \prod_{j=1}^{s} L(s, \rho_j, L/\mathbb{Q})^{m_j}. \tag{5.3}$$

The regular representation, of total dimension $|G| = 1 + \sum_{1\leq j\leq s} m_j^2$, may be written as an isobaric sum

$$\mathrm{reg}_G = \rho_0 \boxplus (\rho_1 \boxplus \cdots \boxplus \rho_1) \boxplus \cdots \boxplus (\rho_s \boxplus \cdots \boxplus \rho_s)$$

in which ρ_j appears $m_j = \dim \rho_j$ times. Thus for each field $L \in \mathscr{F}(\mathbb{Q}, G; X)$ we may consider the Artin L-function $L(s, \pi) = \zeta_L(s)/\zeta(s)$ for the representation

$$\pi = (\rho_1 \boxplus \cdots \boxplus \rho_1) \boxplus \cdots \boxplus (\rho_s \boxplus \cdots \boxplus \rho_s) \tag{5.4}$$

in which ρ_j appears $m_j = \dim \rho_j$ times. Additionally, assuming the Strong Artin Conjecture (see Sect. 6.2), to each field $L \in \mathscr{F}(\mathbb{Q}, G; X)$ and each representation ρ_j, there is an associated cuspidal automorphic representation $\pi_{L,j}$ of $\mathrm{GL}(m_j)/\mathbb{Q}$; we then have

$$L(s, \pi_{L,j}) = L(s, \rho_j, L/\mathbb{Q}).$$

Now fix $1 \le j \le s$. For each $X \ge 1$, let $\mathscr{L}_j(X)$ be the set of cuspidal automorphic representations $\pi_{L,j}$ of $\mathrm{GL}(m_j)/\mathbb{Q}$ associated by the Strong Artin Conjecture to the fields $L \in \mathscr{F}(\mathbb{Q}, G; X)$ and the representation ρ_j.

The main result of this section, and the key result underlying our effective Chebotarev theorem in families, relates to the following phenomenon. For each j, under appropriate assumptions, we show that Theorem E applies to the family $(\mathscr{L}_j(X))_{X \ge 1}$, so that for each $X \ge 1$, aside from very few possible "bad" exceptional representations, for each representation $\pi \in \mathscr{L}_j(X)$ the associated L-function $L(s, \pi)$ possesses a certain zero-free region. Now a key difficulty arises: in general, depending on the group G and the family $\mathscr{F}(\mathbb{Q}, G; X)$, it could happen that a given L-function $L(s, \pi)$ corresponding to a representation $\pi \in \mathscr{L}_j(X)$ occurs as a factor in $\zeta_L(s)/\zeta(s)$ for "many" fields $L \in \mathscr{F}(\mathbb{Q}, G; X)$, indeed even possibly a positive proportion of such fields (see Sect. 6.3.2). We need to rule out this possibility that a "bad" exceptional representation in $\mathscr{L}_j(X)$ could lead to an L-function that "contaminates" ζ_L/ζ for a positive proportion of fields in $\mathscr{F}(\mathbb{Q}, G; X)$. In this section, we state appropriate conditions on a set $\mathscr{F}(\mathbb{Q}, G; X)$ of Galois extensions that allow us to rule out this problem (see in particular the condition (5.5) below). In Sect. 6, we show that the families of fields that we consider in our main theorems obey these conditions.

Now we state the conditions we assume on the set $\mathscr{F}(\mathbb{Q}, G)$ of Galois extensions and the associated families $(\mathscr{L}_j(X))_{X \ge 1}$ of automorphic representations $(1 \le j \le s)$, building on Condition 5.1. (Note that we explicitly assume the Strong Artin Conjecture below, but for certain groups G it is known; see Sect. 6.2.)

Condition 5.4 *Let $\mathscr{F}(\mathbb{Q}, G)$ be a set of Galois extensions as specified above. For each $1 \le j \le s$ and each $X \ge 1$, define the set $\mathscr{L}_j(X)$ of automorphic representations as above, assuming the Strong Artin Conjecture.*

Assume that for each $1 \le j \le s$, the family $(\mathscr{L}_j(X))_{X \ge 1}$ satisfies Condition 5.1, with corresponding parameters $\{m_j, A_j, d_j, M_{0,j}, M_{1,j}, M_{2,j,\varepsilon}, M_{3,j,\varepsilon}\}$. In particular, for $1 \le j \le s$, $(\mathscr{L}_j(X))_{X \ge 1}$ is a family in the sense of Theorem E.

Let $A \ge 0$, M_0 be such that for all $X \ge 1$, for every field $L \in \mathscr{F}(\mathbb{Q}, G; X)$, the representation π associated to $L(s, \pi) = \zeta_L(s)/\zeta(s)$ has $\mathrm{Cond}(\pi) \le M_0 X^A$.

Let d, M_1 be such that for all $X \geq 1$, $|\mathscr{F}(\mathbb{Q}, G; X)| \leq M_1 X^d$.

We assume that for each $1 \leq j \leq s$, there exists $0 \leq \tau_j < d$ and a constant $M_{5,j}$ such that for all $X \geq 1$, for any fixed $\pi \in \mathscr{L}_j(X)$,

$$\#\{L \in \mathscr{F}(\mathbb{Q}, G; X) : \pi_{L,j} = \pi\} \leq M_{5,j} X^{\tau_j}. \tag{5.5}$$

We will call $\{M_0, M_1, A, d\}$ and $\{m_j, A_j, d_j, M_{1,j}, M_{2,j,\varepsilon}, M_{3,j,\varepsilon}, M_{5,j}\}$ for $1 \leq j \leq s$ the family parameters for $\mathscr{F}(\mathbb{Q}, G)$.

5.3 A zero density theorem for L-functions associated to the family $\mathscr{F}(\mathbb{Q}, G)$

To bound on average the number of zeroes of L-functions $\zeta_L(s)/\zeta(s)$ in a certain region, as the field L varies over the family $\mathscr{F}(\mathbb{Q}, G)$, we will apply Theorem E repeatedly, under the assumption of Condition 5.4.

Theorem 5.5 *Let $\mathscr{F}(\mathbb{Q}, G)$ be a set of Galois extensions as specified above. For each $1 \leq j \leq s$ and each $X \geq 1$, define the set $\mathscr{L}_j(X)$ of automorphic representations as above, assuming the Strong Artin Conjecture.*

Assume that $\mathscr{F}(\mathbb{Q}, G)$ and the families $(\mathscr{L}_j(X))_{X \geq 1}$ for $j = 1, \ldots, s$, satisfy Condition 5.4.

Set $\tau = \max_j \tau_j$ and $m = \max m_j$. Then for any $0 < \Delta < 1$ sufficiently small that $\Delta < 1 - \tau/d$, and for any $\eta < 1/4$, there exists B depending only on the family parameters for $\mathscr{F}(\mathbb{Q}, G)$, and $0 < \delta \leq 1/4$ depending only on A, m, d, Δ, τ, such that for all $X \geq 1$, at most $O(X^{(1-(1-\eta)\Delta)d})$ fields $L \in \mathscr{F}(\mathbb{Q}, G; X)$ can have the property that $\zeta_L(s)/\zeta(s)$ has a zero in the region

$$[1 - \delta, 1] \times [-X^{\eta\Delta d/B}, X^{\eta\Delta d/B}].$$

The implied constant in the $O(\cdot)$ notation depends only on A, m, d, Δ, τ and s (the number of nontrivial irreducible representations of G).

Remark 5.6 We see that in the hypotheses there is a non-empty range of $0 < \Delta < 1 - \tau/d$ since each $\tau_j < d$.

To deduce Theorem 5.5 we first apply Theorem E to the family $(\mathscr{L}_j(X))_{X \geq 1}$ for each $1 \leq j \leq s$. Let $1 \leq j \leq s$ be fixed. By Theorem E, for any $\alpha_j \geq 3/4$ and $T_j \geq 2$, for all $X \geq 1$,

$$\sum_{\pi \in \mathscr{L}_j(X)} N(\pi; \alpha_j, T_j) \ll_{c_{j,0}} T_j^{B_j} X^{c_{j,0} \frac{1-\alpha_j}{2\alpha_j - 1}}, \tag{5.6}$$

in which we may choose any $c_{j,0} > c'_{j,0}$, with $c'_{j,0} = c'_{j,0}(m_j, A_j, d_j)$ as shown to exist in Theorem E; the particular form is not critical, but we may for example take

$$c'_{j,0} = \frac{5m_jA_j}{2} + d_j.$$

In the spirit of [45, Remark 3], we pause to observe that although the parameter d_j assumed to exist in the upper bound (iii) of Condition 5.1 may not provide a sharp upper bound, this does not cause any contradictions in terms of its role in $c'_{j,0}$; if d_j is an over-estimate, then the right-hand side of (5.6) is similarly an overestimate (and similarly with respect to the possibly non-sharp parameter A_j). Indeed, for convenience we may choose $c_{j,0} = c''_{j,0} + \varepsilon_1$ (for a certain ε_1 to be chosen later) with

$$c''_{j,0} = \frac{5m_jA}{2} + d. \tag{5.7}$$

Note that $A \geq \max_j A_j$, $d \geq \max_j d_j$ so that this choice is valid.

Set $\tau = \max_{1\leq j\leq s} \tau_j$. Recalling that Δ is given, we fix α_j to be such that

$$\frac{c_{j,0}(1-\alpha_j)}{(2\alpha_j - 1)} = (1-\Delta)d - \tau.$$

We see that the right-hand side is positive, so that $\alpha_j < 1$, since $\Delta < 1 - \tau/d$. Theorem E applies when $\alpha_j \geq 3/4$; if necessary one could simply impose this using monotonicity of the estimates, but in fact it is simple to check that this holds in our scenario. (This will also easily be satisfied in our ultimate applications, in which we will be working very close to the line $\Re(s) = 1$.) We compute that

$$\alpha_j = \frac{c_{j,0} + (1-\Delta)d - \tau}{c_{j,0} + 2((1-\Delta)d - \tau)},$$

so that $\alpha_j \geq 3/4$ as long as

$$c_{j,0} \geq 2((1-\Delta)d - \tau). \tag{5.8}$$

By assumption, $\Delta < 1 - \tau/d$; let $\varepsilon_2 > 0$ be such that

$$\Delta = 1 - \tau/d - \varepsilon_2/2d. \tag{5.9}$$

Then (5.8) is equivalent to the requirement that $c_{j,0} \geq \varepsilon_2$, which will always hold as long as we choose $\varepsilon_1 \geq \varepsilon_2$, according to the definition (5.7), upon recalling that $A, d \geq 0$. Upon setting $T_j = X^{\eta\Delta d/B_j}$, we conclude that

$$\sum_{\pi\in\mathscr{L}_j(X)} N(\pi;\alpha_j,T_j) \ll_{c_{j,0}} X^{\eta\Delta d}X^{(1-\Delta)d-\tau} \ll_{c_{j,0}} X^{(1-(1-\eta)\Delta)d-\tau}. \tag{5.10}$$

Now we assemble these results together for $1 \le j \le s$. For notational convenience, given an L-function $L(s)$ (which could be an Artin L-function $L(s,\rho,L/\mathbb{Q})$ or an automorphic L-function $L(s,\pi)$ corresponding to an automorphic representation π), we will let $N'(L(s);\alpha,T)$ denote the number of zeros $\beta+i\gamma$ with $L(\beta+i\gamma)=0$, and $\beta\ge\alpha$, $|\gamma|\le T$. Set $\alpha=\max_j\alpha_j$ and $T=\min_j T_j$. (Note that $\alpha\ge 3/4$.) Then for each $X\ge 1$, assuming the Strong Artin Conjecture,

$$\begin{aligned}\sum_{L\in\mathscr{F}(\mathbb{Q},G;X)} N'(\zeta_L/\zeta;\alpha,T) &= \sum_{L\in\mathscr{F}(\mathbb{Q},G;X)}\sum_{j=1}^{s} m_j N'(L(s,\rho_j,L/\mathbb{Q});\alpha,T)\\ &= \sum_{L\in\mathscr{F}(\mathbb{Q},G;X)}\sum_{j=1}^{s} m_j N'(L(s,\pi_{L,j},L/\mathbb{Q});\alpha,T)\\ &= \sum_{j=1}^{s} m_j \sum_{\pi\in\mathscr{L}_j(X)} N'(L(s,\pi);\alpha,T) \sum_{\substack{L\in\mathscr{F}(\mathbb{Q},G;X)\\ \pi_{L,j}=\pi}} 1.\end{aligned}$$

Using condition (5.5), we can bound the right-hand side from above by

$$\ll \sum_{j=1}^{s} m_j X^{\tau_j} \sum_{\pi\in\mathscr{L}_j(X)} N'(L(s,\pi);\alpha,T).$$

Thus by applying (5.10) for each $1\le j\le s$, we see that

$$\sum_{L\in\mathscr{F}(\mathbb{Q},G;X)} N'(\zeta_L/\zeta;\alpha,T) \ll_{c_0,s,m} X^{(1-(1-\eta)\Delta)d},$$

where $c_0=\max_j c_{j,0}$. From this we conclude that at most $O_{c_0,s,m}(X^{(1-(1-\eta)\Delta)d})$ fields $L\in\mathscr{F}(\mathbb{Q},G;X)$ can have the property that $\zeta_L(s)/\zeta(s)$ has a zero in the region $[\alpha,1]\times[-X^{\eta\Delta d/B},X^{\eta\Delta d/B}]$, where $B=\max B_j$. The implied constant depends on c_0,s,m, and hence on $A,m,d,\tau,\Delta,s,\varepsilon_1$. Now from (5.9), ε_2 is defined, and then we can choose $\varepsilon_1=\varepsilon_2$ in the definition of $c_{j,0}$. Then we may compute that upon setting $\delta=1-\alpha=1-\max_j\{\alpha_j\}$ (which we have therefore verified satisfies $0<\delta\le 1/4$), we have

$$\delta=\frac{\varepsilon_2}{5\max_j\{m_j\}A+2d+4\varepsilon_2}=\frac{\varepsilon_2}{5mA+2d+4\varepsilon_2} \tag{5.11}$$

as an allowable choice. Since ε_2 is determined by Δ, τ, d we can write the dependencies in terms of these parameters. This yields the result of Theorem 5.5, moreover with a specific description of δ.

Remark 5.7 This argument shows that although the parameters A, d are only assumed to yield valid upper bounds (not necessarily sharp) in Condition 5.4, it is advantageous to make them as small as possible. In a similar vein, it is worth asking why, if making $1-\Delta$ smaller gives better control on the exceptional set, we do not in (5.9) artificially inflate the size of d. The reason is that $1-\Delta$ only controls the density (roughly $O(X^{(1-\Delta)d})$) of the exceptional set relative to the assumed upper bound $O(X^d)$ for the family; thus in this instance also, it is advantageous to make d as sharp as possible.

Remark 5.8 We see that the size of Δ, and hence of the possible exceptional set of bad fields in $\mathscr{F}(\mathbb{Q}, G; X)$ depends on the largest value of τ_j with $1 \leq j \leq s$ coming from the condition (5.5). The larger $\max_j \tau_j$ is, the smaller we must take Δ, and the less savings we have for the possible exceptional set in $\mathscr{F}(\mathbb{Q}, G; X)$.

Remark 5.9 We recall that Cho and Kim (e.g. [15, Theorem 3.1] and other works) have also applied [45] to certain families of isobaric representations, say $\pi = \pi_1 \boxplus \cdots \boxplus \pi_r$ of $\mathrm{GL}(m)/\mathbb{Q}$, with $m = m_1 + \cdots + m_r$, and each π_j a cuspidal automorphic representation of $\mathrm{GL}(m_j)/\mathbb{Q}$. Let us momentarily call the family of such π by $S(X)$ and for each j the family of such π_j by $S_j(X)$. In their work, item (iv) of Condition 5.1 is replaced by the requirement that for each $1 \leq j \leq r$, for all $\rho_j \in S_j(X)$ the gamma factor of $L(s, \pi_j)$ is of the form $\prod_{i=1}^{m_j} \Gamma(s + \alpha_i)$, where $\alpha_i \in \mathbb{R}$ are fixed; this is a special case of the version of (iv) stated here. More importantly, instead of the key item (5.5) in Condition 5.4, Cho and Kim assume that for any two inequivalent $\pi, \pi' \in S(X)$ with $\pi = \pi_1 \boxplus \cdots \boxplus \pi_r$ and $\pi' = \pi'_1 \boxplus \cdots \boxplus \pi'_r$, they have $\pi_j \not\simeq \pi'_k$ for all $1 \leq j, k \leq r$. Relative to (5.5), this would be the statement that for each j, for any fixed $\rho \in S_j(X)$, precisely one $\pi \in S(X)$ has $\pi_j \simeq \rho$, which in our notation is even stronger than the case $\tau_j = 0$ for all $1 \leq j \leq r$. Cho and Kim used this to deduce that $|S_j(X)| = |S(X)|$ for each j, which was crucial to their proof, but also limited the types of families $S(X)$ they could consider.

6 Verifying the conditions of the zero density theorem for families of Dedekind zeta functions

The main result of this section is that Theorems 3.3, 3.9, 3.11, 3.13 and 3.14 may be deduced from Theorem 5.5 by verifying that for each of the families of fields considered in these theorems, Condition 5.4 is satisfied. Accordingly, in

this section we fix $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ to be one of the families specified in the above theorems, under the associated hypotheses of the theorem (if any).

6.1 Passage to a family of Galois closures

We now pass from considering the original set of the degree n fields in $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ to considering the set of Galois closures $\tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G) = \{\tilde{K} : K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G)\}$; each Galois closure corresponds to a constant number of fields in $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ (only depending on G as a permutation group). We now recall the notation of Sect. 5.2. Using that notation, we define $\mathscr{F}(\mathbb{Q}, G) = \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G)$ to be the set of Galois extensions we consider, and we accordingly define the sets $\mathscr{L}_j(X)$ for each $1 \leq j \leq s$ and every $X \geq 1$, and thereby the corresponding families $(\mathscr{L}_j(X))_{X \geq 1}$ of automorphic representations.

6.2 Verification of Condition 5.1 (i)–(iv)

Now that we have constructed the appropriate families $\mathscr{F}(\mathbb{Q}, G) = \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G)$ and $(\mathscr{L}_j(X))_{X \geq 1}$ for each $1 \leq j \leq s$, we must verify that Condition 5.4 is satisfied. We first note that for each family $\tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G)$ we consider, either the strong Artin conjecture is known to apply to all the Galois representations considered (this is the case in Theorem 3.3) or it is explicitly assumed (this is the case in Theorems 3.9, 3.11, 3.13 and 3.14). To be precise, let us write the Euler product of an Artin L-function as $L(s, \rho) = \prod_v L(s, \rho_v)$, and the Euler product for an automorphic L-function as $L(s, \pi) = \prod_v L(s, \pi_v)$.

Conjecture F (Strong Artin Conjecture) *Let L be a finite Galois extension of a number field k, with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$. Let ρ be an m-dimensional complex representation of G. There exists an automorphic representation $\pi(\rho)$ of $\mathrm{GL}(m)/\mathbb{Q}$ such that the L-functions $L(s, \rho)$ and $L(s, \pi)$ agree almost everywhere, i.e. except at a finite number of places v, $L(s, \rho_v) = L(s, \pi_v)$. Moreover, if ρ is irreducible, then π is cuspidal.*

This is known to hold for: 1-dimensional representations ρ, due to Artin [2]; nilpotent Galois extensions L/k, due to Arthur and Clozel [1]; A_4 and S_4, due to Langlands [48] and Tunnell [76], respectively; dihedral groups (and in particular S_3), due to Langlands [48]. We also note that in the setting we will work in, a stronger identity is known. (See, for example, [24, Theorem 4.6], [54, Proposition 2.1], [55, Appendix A], and [57, Proposition 1.5].)

Theorem G *If π is cuspidal and $L(s, \pi_v) = L(s, \rho_v)$ for almost all v, then in fact $L(s, \pi) = L(s, \rho)$.*

These considerations guarantee that in the settings we consider (with the relevant hypotheses we assume), each $\mathscr{L}_j(X)$ is a set of cuspidal automorphic representations.

We next confirm that for each $1 \le j \le s$, the family $(\mathscr{L}_j(X))_{X \ge 1}$ satisfies the four items in Condition 5.1. For item (i), since the Ramanujan-Petersson conjecture holds for automorphic L-functions associated to Artin L-functions once they are known to exist (see e.g. the comment following [45, Thm. 5]), under the assumption (or known truth) of the strong Artin conjecture, the Ramanujan-Petersson conjecture holds for all the cuspidal automorphic L-functions in each set $\mathscr{L}_j(X)$.

For item (ii), note that if $K \in Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)$ then by construction $D_K \le X$. The following standard lemma relates to discriminants of a field and its Galois closure.

Lemma 6.1 (Discriminant comparisons) *Let G be a transitive subgroup of S_n. There exist constants $C_1 = C_1(G)$ and $C_2 = C_2(G)$ such that for every field $K \in Z_n(\mathbb{Q}, G)$,*

$$C_1 D_K^{|G|/n} \le D_{\tilde{K}} \le C_2 D_K^{|G|/2}.$$

(The lemma follows from Lemmas 6.9 and 6.10, recorded below, and for the left-hand inequality, the fact that every cycle length in a permutation is at most the order of the permutation.)

Recall that in general for an Artin L-function $L(s, \rho, L/k)$, if $F(\chi)$ denotes the Artin conductor of $\chi = \mathrm{Tr}(\rho)$, then the conductor of $L(s, \rho, L/k)$ is given by $A(\chi) = D_k^{\chi(1)} \mathrm{Nm}_{k/\mathbb{Q}} F(\chi)$. According to the multiplicativity relation $D_L = D_k \prod_{\chi_j} A(\chi_j)^{\chi_j(1)}$ for the conductors in the identity (5.3), we see that for each $1 \le j \le s$, the conductors of $L(s, \rho_j, L/\mathbb{Q})$ are bounded by $\ll_{n,G} X^{|G|/2}$ and we may take $A_j = A = |G|/2$ for all j.

For (iii), to control the size of the family of fields $\tilde{Z}_n^{\mathscr{J}}(\mathbb{Q}, G; X)$ it suffices to control the sizes of the families $Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)$ (and moreover it suffices to bound from above the sizes of the families $Z_n(\mathbb{Q}, G; X)$ without the ramification restriction). Thus we may apply the following known unconditional upper bounds to show the existence of $d_j = d$ for all j: G cyclic, Proposition 2.1; $G \simeq S_n$ see (2.6); $G \simeq D_p$ see (2.4); $G \simeq A_4$ see (2.8); $G \subseteq S_n$ simple, we simply embed $Z_n(\mathbb{Q}, G; X)$ in the family of all fields of degree n and apply (2.6).

For item (iv), we use the known convexity bounds for automorphic L-functions, which apply to our Artin L-functions under the strong Artin conjecture. Briefly, to be precise, we recall for $t \in \mathbb{R}$ the analytic conductor of $L(s, \pi)$ (in terms of the arithmetic conductor $\mathrm{Cond}(\pi)$ and the local parameters at infinity, $\mu_\pi(j)$),

$$Q_\pi(t) = \mathrm{Cond}(\pi) \prod_{j=1}^{m} (1 + |it - \mu_\pi(j)|).$$

Then via the functional equation, Stirling's formula, and an application of the Phragmen-Lindelöf principle, one may derive the classical convexity bound (see e.g. [36, page 5]):

$$L(s, \pi) \ll_{\pi,\varepsilon} Q_\pi(t)^{\frac{1-\Re(s)}{2}+\varepsilon}, \qquad 0 \le \Re(s) \le 1.$$

For π, π' unitary cuspidal automorphic representations of $\mathrm{GL}(m)/\mathbb{Q}$, $\mathrm{GL}(m')/\mathbb{Q}$, the Rankin-Selberg L-function $L(s, \pi \otimes \tilde{\pi})$ (see e.g. [56, §1.1.2]) has a corresponding arithmetic conductor $\mathrm{Cond}(\pi \otimes \pi')$ and analytic conductor, given for $t \in \mathbb{R}$ by

$$Q_{\pi\otimes\pi'}(t) = \mathrm{Cond}(\pi \otimes \pi') \prod_{j=1}^{mm'} (1 + |it - \mu_{\pi\otimes\pi'}(j)|).$$

The convexity bound for $L(s, \pi \otimes \pi')$ in the critical strip is known:

$$L(s, \pi \otimes \pi') \ll_{\pi,\pi',\varepsilon} Q_{\pi\otimes\pi'}(t)^{\frac{1-\Re(s)}{2}+\varepsilon}, \qquad 0 \le \Re(s) \le 1.$$

Remark 6.2 Note that for each $1 \le j \le s$, the uniformity of the convexity bounds assumed in Condition 5.1 (iv) with respect to m_j is critically reliant on the fact that within a family $Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)$, all fields share a fixed degree and a fixed Galois group of the Galois closure.

6.3 Verification of condition (5.5): controlling the propagation of bad L-function factors

Now we turn to the most difficult task: verifying that for each choice of the family $Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)$ that we consider in our main theorems, condition (5.5) of Condition 5.4 is satisfied.

6.3.1 Reframing the question in terms of subfields

Let $Z_n^{\mathscr{J}}(\mathbb{Q}, G; X)$ be a fixed family of fields, for a fixed transitive group $G \subseteq S_n$, and let ρ be an irreducible representation of G. Let $L_1, L_2 \in \tilde{Z}_n^{\mathscr{J}}(\mathbb{Q}, G; X)$. Then $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq G$ while $\mathrm{Gal}(L_i^{\mathrm{Ker}(\rho)}/\mathbb{Q}) \simeq G/\mathrm{Ker}(\rho)$. The following proposition transforms the property of identical L-functions into a property of identical fixed fields.

Proposition 6.3 *Let ρ be a fixed representation of a fixed transitive subgroup $G \subseteq S_n$. For $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ with $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{Gal}(L_2/\mathbb{Q}) \simeq G$, then if*

$$L(s, \rho, L_1/\mathbb{Q}) = L(s, \rho, L_2/\mathbb{Q}) \tag{6.1}$$

it follows that $L_1^{\mathrm{Ker}(\rho)} = L_2^{\mathrm{Ker}(\rho)}$.

We recall a standard lemma.

Lemma 6.4 *Suppose for two Galois extensions $F_1/\mathbb{Q}$ and $F_2/\mathbb{Q}$, that, aside from finitely many exceptions, the set of rational primes that split completely in F_1 is the same as the set of rational primes that split completely in F_2. Then $F_1 = F_2$.*

Proof By the Chebotarev density theorem, the density of rational primes that are split completely in F_1, F_2, or F_1F_2 are, respectively $[F_1 : \mathbb{Q}]^{-1}$,$[F_2 : \mathbb{Q}]^{-1}$, $[F_1F_2 : \mathbb{Q}]^{-1}$. Since a prime is split completely in F_1F_2 if and only if it is split completely in F_1 and F_2, we have $[F_1 : \mathbb{Q}] = [F_2 : \mathbb{Q}] = [F_1F_2 : \mathbb{Q}]$ and so $F_1 = F_2$. □

Thus to prove Proposition 6.3, it suffices to show that for each fixed representation ρ of G, aside from finitely many exceptions, the set of rational primes that split completely in $L_1^{\mathrm{Ker}(\rho)}$ is the same as the set of rational primes that split completely in $L_2^{\mathrm{Ker}(\rho)}$, under the assumption that $L(s, \rho, L_1/\mathbb{Q}) = L(s, \rho, L_2/\mathbb{Q})$. First we assume that p is a rational prime that is unramified in L_1, L_2 (and hence is unramified in $L_1^{\mathrm{Ker}(\rho)}$, $L_2^{\mathrm{Ker}(\rho)}$) and splits completely in $L_1^{\mathrm{Ker}(\rho)}$. In particular, this means that for any $\mathfrak{p}_1$ in $L_1^{\mathrm{Ker}(\rho)}$ that lies above p, the conjugacy class of the Frobenius element $\sigma_{\mathfrak{p}_1}$ is trivial in $\mathrm{Gal}(L_1^{\mathrm{Ker}(\rho)}/\mathbb{Q}) \simeq G/\mathrm{Ker}(\rho)$, that is to say, $\rho(\sigma_{\mathfrak{p}_1})$ is the identity matrix I.

Now letting $\mathfrak{p}_2 \in L_2^{\mathrm{Ker}(\rho)}$ be any prime lying above p, by the assumption that the L-functions are equal, we have that the factors corresponding to p are equal as functions of s and therefore

$$\det(I - \rho(\sigma_{\mathfrak{p}_2})p^{-s})^{-1} = \det(I - \rho(\sigma_{\mathfrak{p}_1})p^{-s})^{-1} = \det(I - Ip^{-s})^{-1}. \tag{6.2}$$

Now recall that the Frobenius element $\sigma_{\mathfrak{p}_2}$ is necessarily finite order. We recall a simple observation. Suppose M is an $n \times n$ matrix over $\mathbb{C}$ of finite order, say $M^k = I$ for some k, such that $\det(I - Mx) = \det(I - Ix) = (1 - x)^n$ for a formal variable x. Then we claim $M = I$. Indeed, since M is finite order, M is diagonalizable, for the minimal polynomial of M divides $x^k - 1$ and so has no repeated roots. By our second assumption, all the roots of the characteristic polynomial of M are equal to 1, so that all the eigenvalues of M are 1 and $M = I$. We apply this in (6.2) to conclude that $\rho(\sigma_{\mathfrak{p}_2}) = I$

as well. Thus the conjugacy class of the Frobenius element $\sigma_{\mathfrak{p}_2}$ is trivial in $\mathrm{Gal}(L_2^{\mathrm{Ker}(\rho)}/\mathbb{Q}) \simeq G/\mathrm{Ker}(\rho)$ and p must split completely in $L_2^{\mathrm{Ker}(\rho)}$.

In this fashion we see that any prime that is unramified in L_1, L_2 and splits completely in $L_1^{\mathrm{Ker}(\rho_1)}$ must split completely in $L_2^{\mathrm{Ker}(\rho)}$. Starting from primes unramified in L_1, L_2 that split completely in $L_2^{\mathrm{Ker}(\rho)}$ we can similarly show that they must split completely in $L_1^{\mathrm{Ker}(\rho)}$, and this concludes the proof of Proposition 6.3.

Remark 6.5 Proposition 6.3 can alternatively be deduced from [46, Theorem 5], which also includes a converse, which we do not require in our application. To apply [46, Theorem 5] in our setting, one first passes as in [46, p. 162] to the case of a faithful representation $\varpi(\sigma\mathrm{Ker}(\rho)) = \rho(\sigma)$ acting on $H = G/\mathrm{Ker}(\rho)$. Klüners and Nicolae present a counterexample to the characterization deduced in Proposition 6.3 when working over $k \neq \mathbb{Q}$ [46, p. 167], but see their relative version [46, Thm. 6]. It is possible that certain other families $Z_n^{\mathscr{I}}(k, G; X)$ with $k \neq \mathbb{Q}$ and certain choices of G can be treated by an adaptation of our methods with such a relative result. (When working over $k \neq \mathbb{Q}$ one would also need to take into account the more nuanced situation that arises with regards to arithmetic equivalence.)

We now apply Proposition 6.3. As before, let G be a fixed transitive subgroup of S_n and let $\rho_1, \ldots, \rho_s$ be the nontrivial irreducible representations of G. For each $1 \leq j \leq s$, consider the set of fields

$$\{L^{\mathrm{Ker}(\rho_j)} : L \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)\}.$$

(Note that we define this as a set, not a multi-set.) Philosophically, we would like to show that the cardinality of this set is "large," or equivalently very few of the fields L share the same fixed field, which would imply that "few" collisions $L(s, \rho_j, L_1/\mathbb{Q}) = L(s, \rho_j, L_2/\mathbb{Q})$ could occur for $L_1 \neq L_2 \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$.

Formally, recall the definition of the set $\mathscr{L}_j(X)$ in Sect. 5.2 according to the family of fields $\mathscr{F}(\mathbb{Q}, G; X) = \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$. Let us first consider the special case in which ρ_j is faithful so that $\mathrm{Ker}(\rho_j)$ is trivial. Then by Proposition 6.3, for two fields $L_1 \neq L_2 \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, we cannot have $L_1^{\mathrm{Ker}(\rho_j)} = L_2^{\mathrm{Ker}(\rho_j)}$ and so we cannot have $L(s, \rho_j, L_1/\mathbb{Q}) = L(s, \rho_j, L_2/\mathbb{Q})$, and so in this case

$$|\mathscr{L}_j(X)| = |\tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)|. \tag{6.3}$$

Thus if ρ_j is faithful, we have verified (5.5) of Condition 5.4 with $\tau_j = 0$, which certainly suffices.

More generally, even if ρ_j is not a faithful representation, Proposition 6.3 shows that the number of fields $L_i \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ for which $L(s, \rho_j, L_i/\mathbb{Q})$

is identical to a specific L-function is bounded above by the number of fields $L_i \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ for which $L_i^{\mathrm{Ker}(\rho_j)}$ is identical to a specific field. Thus we have translated the problem of verifying (5.5) for a particular family $\mathscr{L}_j(X)$ to a problem of counting fields.

Precisely, we summarize the implications of Proposition 6.3 as the following statement:

Proposition 6.6 *Let $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ be a set of fields considered in Theorem 3.3, 3.9, 3.11, 3.13 or 3.14 under the associated hypotheses, if any. Let $\tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G)$ be the corresponding set of Galois closures. Let $\rho_1, \dots, \rho_s$ be the nontrivial irreducible representations of G. Define the families $(\mathscr{L}_j(X))_{X\geq 1}$ for $1 \leq j \leq s$ accordingly, as in Sect. 5.2. Then $\tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G)$ and the families $(\mathscr{L}_j(X))_{X\geq 1}$ for $1 \leq j \leq s$ satisfy (5.5) of Condition 5.4 with parameters $\{\tau_j\}_{1\leq j\leq s}$ if the following holds: for each irreducible representation ρ_j of G, given any field $F \in Z_u(\mathbb{Q}, G/\mathrm{Ker}(\rho_j); X)$ (where $u = |G/\mathrm{Ker}(\rho_j)|$), at most $O_{n,G,\mathscr{I}}(X^{\tau_j})$ fields $L \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ have $L^{\mathrm{Ker}(\rho_j)} = F$.*

6.3.2 *Rationale for the restriction on ramification types of tamely ramified primes*

For G not a simple group, Proposition 6.6 spurs us to quantify, for each proper normal subgroup H of G that appears as the kernel of at least one (non-faithful, non-trivial) irreducible representation of G, how often a particular field occurs as a fixed field L^H, as L varies over a relevant family of Galois extensions of $\mathbb{Q}$ with Galois group G.

For certain groups G, fixed fields could collide with high repetition. For example, taking $G = \mathbb{Z}/4\mathbb{Z}$, then for any fixed quadratic field such as $F = \mathbb{Q}(e^{2\pi i/3})$, a positive proportion of quartic Galois fields $K \in Z_4(\mathbb{Q}, \mathbb{Z}/4\mathbb{Z}; X)$ have $K^{\mathbb{Z}/2\mathbb{Z}} = F$. This can be seen for example via a counting argument similar to that of Sect. 2.1. (See also comments in Remarks. 6.11 and 6.12.)

To eliminate such possibilities, we will critically use our restrictions on the ramification types of the tamely ramified primes in the fields in $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$. Given G, we will select $\mathscr{I}$ so that it has two properties:

(1) For $Z_n^{\mathscr{I}}(\mathbb{Q}, G)$ to be infinite, we need the elements in $\mathscr{I}$ to generate G.
(2) We need $\mathscr{I}$ to have the property that for each proper normal subgroup H in G that is the kernel of a non-faithful irreducible representation of G, given any field $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ with associated Galois closure $\tilde{K}/\mathbb{Q}$, then $p|D_K$ implies $p|D_F$, where $F = \tilde{K}^H$.

(Of course the primes that appear in D_K are the same that appear in $D_{\tilde{K}}$ but this need not *a priori* be true of $D_{\tilde{K}}$ and D_F.) Property (2) will enable us to obtain the information we seek in Proposition 6.6, that is, to count the number of $\tilde{K} \in \tilde{Z}_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ sharing the same fixed field $F = \tilde{K}^H$, by applying

quantitative information about $\mathbf{D}_n(G;\varpi)$ (Property 1.6). This is one of the most novel features of this paper.

6.4 The counting problem

We now define the counting problem that is the heart of the matter.

Property 6.7 (Property $\mathrm{Mult}_n(G,\mathscr{I};\tau)$) *Let* $\mathrm{Mult}_n(G,\mathscr{I};\tau)$ *denote the property that for every* $X \geq 1$, *for each irreducible representation* ρ *of* G, *given any particular field* $F \in Z_u(\mathbb{Q}, G/\mathrm{Ker}(\rho))$ *(with* $u = |G/\mathrm{Ker}(\rho)|$*) that arises as a fixed field* $\tilde{K}^{\mathrm{Ker}(\rho)}$ *for at least one field* $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, *for every* $\varepsilon > 0$, *at most* $O_{n,G,\mathscr{I},\varepsilon}(X^{\tau+\varepsilon})$ *fields* $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ *have* $\tilde{K}^{\mathrm{Ker}(\rho)} = F$.

Given a family $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, if we can prove that $\mathrm{Mult}_n(G,\mathscr{I};\tau)$ holds for a sufficiently small τ, then by Proposition 6.6, the relevant effective Chebotarev density theorem for the family $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ will follow (that is, either Theorem 3.3, 3.9, 3.11, 3.13 or 3.14). Quantitatively, lowering the size of τ for which we can prove $\mathrm{Mult}_n(G,\mathscr{I};\tau)$ will allow us to better control the size of the possible exceptional set of fields.

Proposition 6.8 (Counting problem)
We can prove the following:

(1) $\mathrm{Mult}_n(G,\mathscr{I};0)$ *for* G *a simple group,* $\mathscr{I}$ *imposing no restriction.*
(2) $\mathrm{Mult}_n(G,\mathscr{I};0)$ *for* G *cyclic,* $\mathscr{I}$ *specifying totally ramified.*
(3) $\mathrm{Mult}_n(S_n,\mathscr{I};\varpi_n)$ *for* $n \geq 3$, $\mathscr{I}$ *the conjugacy class* $[(1\ 2)]$, *where* $\varpi_3 = 1/3$, $\varpi_4 = 1/2$, $\varpi_5 = 199/200$, *and for* $n \geq 6$, $\varpi_n = \varpi$ *if we assume Property* $\mathbf{D}_n(S_n,\varpi)$.
(4) $\mathrm{Mult}_p(D_p,\mathscr{I};\tau_p)$ *holds for* $\tau_p = 1/(p-1)$, p *an odd prime,* $\mathscr{I}$ *the conjugacy class of order 2 elements.*
(5) $\mathrm{Mult}_4(A_4,\mathscr{I};0.2784...)$, $\mathscr{I}$ *the two conjugacy classes of order 3 elements.*

As observed above, $\mathrm{Mult}_n(G,\mathscr{I};0)$ is tautologically true when G is a simple group ($\mathscr{I}$ imposing no restriction), since all the nontrivial irreducible representations are faithful and (6.3) applies. All the other cases of the counting problem require work. We first explicitly prove this for $S_n, n \neq 4$; in particular, to aid the reader, we include our argumentation for choosing $\mathscr{I} = [(1\ 2)]$.

6.4.1 Background lemmas on inertia groups and discriminants

We recall standard results on the powers of primes dividing D_K.

Lemma 6.9 (Powers of tamely ramified primes in discriminants) *Let* $K \subset \tilde{K} \subset \overline{\mathbb{Q}}$ *with* $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq G$ *and* $H = \mathrm{Gal}(\tilde{K}/K)$. *Let* p *be a rational prime*

that is tamely ramified in K and $\tilde{K}$, and has an inertia group in $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ *generated by $\pi \in G$. The power α such that $p^\alpha || D_K$ is*

$$[G : H] - \textit{number of orbits of } \pi \textit{ acting on the cosets } G/H. \tag{6.4}$$

Proof We have that D_K is the Artin conductor of $\tilde{K}/\mathbb{Q}$ for the permutation representation of G on G/H [61, Ch. VII, Corollary 11.8]. By definition, the Artin conductor of $\tilde{K}/\mathbb{Q}$ for a representation V of $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ is $\prod_p p^{f_p(V)}$, where the product is over rational primes and

$$f_p(V) = \sum_{i \geq 0} \frac{g_{p,i}}{g_{p,0}} \operatorname{codim} V^{G_{p,i}},$$

for $G_{p,i}$ an ith ramification group for p in $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ and $g_{p,i} := |G_{p,i}|$. Recall that $G_{p,0}$ is the inertia group I_p and that for tamely ramified p, we have $G_{p,i} = 1$ for $i \geq 1$. So for tamely ramified p, we have $f_p(V) = \operatorname{codim} V^{I_p}$. The lemma follows, since for a permutation representation V, the dimension of the fixed subspace V^π is the number of orbits of π. □

Lemma 6.10 (Maximum contribution of wild primes) *Let G be a transitive subgroup of S_n. Then for all fields $K \in Z_n(\mathbb{Q}, G)$, the total contribution to D_K from the rational primes that are wildly ramified in K is at most a certain finite constant C_G depending only on G.*

This lemma follows from [61, Ch. III, Thm. 2.6] and the fact that all wildly ramified primes divide $|G|$.

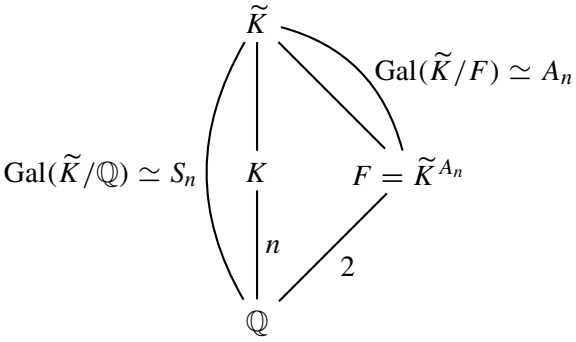
In order to consider only the tame part of the discriminant in our investigations below, it will be convenient to use the following notation. Given a finite set of primes Ω, define $D_K^{(\Omega)}$ to denote the contribution to the discriminant from primes $p \notin \Omega$, i.e. $D_K^{(\Omega)}$ is the maximal positive divisor of D_K that is not divisible by any prime in Ω. We will apply this in particular when Ω is comprised of the primes dividing $|G|$.

6.4.2 *Exemplar case: $G = S_n$, $n = 3$ or $n \geq 5$*

Recall that when $n = 3$ or $n \geq 5$, S_n has one nontrivial, proper normal subgroup, namely A_n, which certainly appears as the kernel of the sign representation. Thus we must specify a ramification type $\mathscr{I}$ so that the counting problem for fixed fields $\tilde{K}^{A_n}$ can be handled. We wish, for a fixed quadratic field $F \in Z_2(\mathbb{Q}, C_2)$, to count the number of degree n fields $K \in Z_n(\mathbb{Q}, S_n; X)$ such that $\tilde{K}^{A_n} = F$.

Table 1 Table of exponents for p when $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$, for each $p \nmid n!$

Inertia type of p	Exponent of p appearing in the discriminant of		
	K	$\widetilde{K}$	$F = \widetilde{K}^{A_n}$
[()]	0	0	0
[(1 2)]	1	$n! - n!/2$	1
[(1 2 3)] = [(1 2)(2 3)]	2	$n! - n!/3$	0
[(1 2)(3 4)]	2	$n! - n!/2$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[(1\ 2\ 3 \ldots n)]$	$n-1$	$n! - n!/n$	ε_n



Using Lemma 6.9, we can compute for fields K, $\tilde{K}$, F in such a constellation the exact power of p that appears in the absolute discriminants D_K, $D_{\tilde{K}}$, D_F, for each prime $p \nmid |G|$. We show these exponents in Table 1: the leftmost column specifies the conjugacy class of the generating element π of the (cyclic) inertia group for p, while the other columns specify the exact power of p appearing in the discriminants. We only list a few of the $p(n)$ conjugacy classes of S_n; we set $\varepsilon_n = 0$ if n is odd and $\varepsilon_n = 1$ if n is even.

From Table 1 we observe that every $p \nmid |G|$ that has inertia group generated by a transposition has $p \| D_K$, $p^{n!/2} \| D_{\tilde{K}}$, $p \| D_F$. This will allow us to control, for a fixed field F, how many K can yield a constellation including F. These observations from Table 1 motivated our choice of $\mathscr{I} = [(1\ 2)]$ for $G \simeq S_n$ ($n = 3, n \geq 5$).

Now we come to the crux of the argument. Suppose that F is fixed, and hence $D_F \geq 1$ is fixed. Set $\Omega = \{p : p | n!\}$ and recall the notation $D_K^{(\Omega)}$ defined above. Our discussion above shows that any degree n extension $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, S_n; X)$ such that $\tilde{K}^{A_n} = F$ must have

$$D_K^{(\Omega)} = D_F^{(\Omega)}. \tag{6.5}$$

Assuming Property $\mathbf{D}_n(S_n, \varpi)$ is known, then since the power of any $p \in \Omega$ dividing D_K is bounded in terms of n, for a given F there are at most $\ll_{n,G,\varepsilon} D_F^{\varpi+\varepsilon} \ll_{n,G,\varepsilon} X^{\varpi+\varepsilon}$ such K satisfying (6.5), for every $\varepsilon > 0$. Now to obtain the conclusion on $\mathrm{Mult}_n(S_n, \mathscr{I}; \varpi_n)$ of Proposition 6.8 for S_n, $n = 3$, $n \geq 5$, we simply apply the currently best known upper bounds for Property $\mathbf{D}_n(S_n, \varpi)$ in these cases, as stated in Sect. 2.3.

Having completed this exemplar case of $G = S_n$ ($n \neq 4$) in some detail, we are now more brief with the remaining groups G, which follow similarly by using Lemma 6.9 in order to fix an appropriate choice of ramification type $\mathscr{I}$ for which the counting problem can be resolved.

6.4.3 $G \simeq S_4$

Recall that S_4 has four nontrivial irreducible representations (see e.g. [67, p. 43]): two three-dimensional faithful representations (the standard representation and the product of the standard representation with the sign representation) and two non-faithful representations. The subgroup A_4 is the kernel of the one-dimensional sign representation, and $K_4 \simeq C_2 \times C_2$ the Klein four group is the kernel of the irreducible two-dimensional representation of S_4. We thus have two counting problems to consider.

Relevant to the counting problem for fixed fields under A_4, by choosing $\mathscr{I}$ to be the conjugacy class $[(1\ 2)]$ of transpositions, we may conclude that triads $K, \tilde{K}, F = \tilde{K}^{A_4}$ behave exactly as in the case of S_n in Sect. 6.4.2, so that for any $p \nmid 4!$, $p \| D_K$, $p^{12} \| D_{\tilde{K}}$, $p \| D_F$, and hence upon setting $\Omega = \{2, 3\}$, we have $D_K^{(\Omega)} = D_F^{(\Omega)}$. Thus arguing as in Sect. 6.4.2, any fixed F corresponds to at most $\ll_\varepsilon D_F^{\varpi+\varepsilon} \ll_{n,G,\varepsilon} X^{\varpi+\varepsilon}$ possibilities for $K \in Z_4^{\mathscr{I}}(\mathbb{Q}, S_4; X)$, if Property $\mathbf{D}_4(S_4, \varpi)$ is known.

Relevant to the counting problem for fixed fields under K_4, still choosing $\mathscr{I}$ to be the conjugacy class $[(1\ 2)]$ of transpositions, for triads $K, \tilde{K}, F = \tilde{K}^{K_4}$ the exponents are different: for every $p \nmid 4!$ we have $p \| D_K$, $p^{12} \| D_{\tilde{K}}$, and $p^3 \| D_F$. Thus upon setting $\Omega = \{2, 3\}$, we have

$$D_K^{(\Omega)} = (D_F^{(\Omega)})^{1/3}, \tag{6.6}$$

and so any fixed F corresponds to at most $\ll_\varepsilon D_F^{\varpi/3+\varepsilon} \ll_{n,G,\varepsilon} X^{\varpi+\varepsilon}$ possibilities (for every $\varepsilon > 0$) for $K \in Z_4^{\mathscr{I}}(\mathbb{Q}, S_4; X)$, if Property $\mathbf{D}_4(S_4, \varpi)$ is known. (Here we have used the fact that if $K \in Z_n(\mathbb{Q}, G; X)$ and (6.6) holds, then $D_F \ll_{n,G} X^3$.) We conclude that $\mathrm{Mult}_4(S_4, \mathscr{I}; 1/2)$ holds since Property $\mathbf{D}_4(S_4, 1/2)$ is known.

6.4.4 $G \simeq A_4$

Recall (see [67, Section 5.7, page 41]) that A_4 has four nontrivial irreducible representations: two faithful representations and two one-dimensional non-faithful representations, each with kernel $K_4 \simeq C_2 \times C_2$ the Klein-four group. Thus we need only complete the counting problem for triads $K, \tilde{K}, F = \tilde{K}^{K_4}$. We will require all tamely ramified primes to have inertia type belonging to either of the conjugacy classes $\mathscr{C}_1, \mathscr{C}_2$ of order 3 elements (specified e.g. in Proposition 2.5).

Suppose we restrict to primes of inertia type in the conjugacy class $\mathscr{C}_1$. The image of this inertia type in $A_4/K_4 \simeq C_3$ is nontrivial, and we see that for any $p \nmid |A_4|$, $p^2 \| D_K$, $p^8 \| \tilde{K}$, $p^2 \| D_F$. Thus upon setting $\Omega = \{2, 3\}$, within the triad we have $D_K^{(\Omega)} = D_F^{(\Omega)}$, and so, any fixed F corresponds to at most $\ll_\varepsilon D_F^{\varpi+\varepsilon} \ll_{n,G,\varepsilon} X^{\varpi+\varepsilon}$ possibilities for $K \in Z_4^{\mathscr{I}}(\mathbb{Q}, A_4; X)$, if Property $\mathbf{D}_4(A_4, \varpi)$ is known. The computation for primes of inertia type in the conjugacy class $\mathscr{C}_2$ is identical. Recalling our result of Proposition 2.5, we conclude that $\mathrm{Mult}_4(S_4, \mathscr{I}; 0.2784...)$ holds.

6.4.5 $G \simeq D_p$, p an odd prime

We think of D_p (with p an odd prime) as the group of order $2p$ of symmetries on a regular p-gon, acting in the usual way. Thus D_p has one nontrivial, proper normal subgroup, namely C_p; this subgroup certainly appears as the kernel of the (one-dimensional) sign representation. Thus we must consider the corresponding counting problem for fixed fields $\tilde{K}^{C_p}$. We restrict the inertia type $\mathscr{I}$ to the conjugacy class $[(2\ p)(3\ \ (p-1)) \cdots (\frac{p+1}{2}\ \frac{p+3}{2})]$, that is the conjugacy class of reflections (each with with $(p+1)/2$ orbits acting on p elements).

For a triad $K, \tilde{K}, F = \tilde{K}^{C_p}$ we then have for every prime $\ell \nmid 2p$ that $\ell^{(p-1)/2} \| D_K$, $\ell^p \| D_{\tilde{K}}$, $\ell \| D_F$. Thus upon setting $\Omega = \{2, p\}$ we have

$$D_K^{(\Omega)} = (D_F^{(\Omega)})^{\frac{p-1}{2}}, \tag{6.7}$$

and so any fixed F corresponds to at most $\ll_{p,D_p,\varepsilon} D_F^{(p-1)\varpi/2+\varepsilon}$ possibilities for $K \in Z_p^{\mathscr{I}}(\mathbb{Q}, D_p; X)$, if Property $\mathbf{D}_p^{\mathscr{I}}(D_p, \varpi)$ is known. Now if (6.7) is known and $K \in Z_p^{\mathscr{I}}(\mathbb{Q}, D_p; X)$ then $D_F \ll_{p,D_p} X^{2/(p-1)}$, so we have at most $\ll_{p,D_p,\varepsilon} X^{\varpi}$ choices for such K if Property $\mathbf{D}_p^{\mathscr{I}}(D_p, \varpi)$ is known. We conclude from Proposition 2.3 that $\mathrm{Mult}_p(D_p, \mathscr{I}; 1/(p-1))$ holds unconditionally.

6.4.6 *G a cyclic group*

Finally, for G a cyclic group of order n, note that $Z_n(\mathbb{Q}, G; X)$ already is comprised of Galois fields, so we do not need to pass to the Galois closures. (As a special case, if $G \simeq C_p$ with p prime, then G has no nontrivial proper (normal) subgroups, so all nontrivial representations are faithful, without the need to artificially impose a ramification restriction. But in this case, every ramified prime is naturally totally ramified, so we still group this with the general case below.) In general, consider G an arbitrary cyclic group of order n, say $G \simeq C_{p_1^{e_1}} \times \cdots \times C_{p_k^{e_k}}$ with distinct primes $p_1, \ldots, p_k$. We restrict to $\mathscr{J}$ specifying that every tamely ramified prime must be totally ramified, that is, its inertia group must be generated by an element of full order in G; in particular, such an element does not belong to any proper, nontrivial subgroup C_m of C_n.

By Lemma 6.9 the following properties hold:

(1) for every prime $\ell \nmid n$ we have $\ell^{n-1} \| D_K = D_{\tilde{K}}$;
(2) for every nontrivial proper (normal) subgroup C_m of C_n (corresponding to a proper divisor $m|n$) there exists an integer $1 \le \alpha_m \le n-1$ (depending on m and C_n) such that $\ell^{\alpha_m} \| D_F$ where $F = \tilde{K}^{C_m}$.

As a result, upon setting $\Omega = \{p : p|n\}$, for each nontrivial proper subgroup C_m of G, parametrized by divisors m, we have that

$$D_K^{(\Omega)} = (D_F^{(\Omega)})^{\frac{n-1}{\alpha_m}}$$

when $F = K^{C_m} = \tilde{K}^{C_m}$. Thus any fixed F corresponds to at most $\ll_{n,m,C_n,\varepsilon} D_F^{\varpi(n-1)/\alpha_m+\varepsilon} \ll_{n,m,C_n,\varepsilon} X^{\varpi+\varepsilon}$ possibilities (for any $\varepsilon > 0$) for $K \in Z_n^{\mathscr{J}}(\mathbb{Q}, C_n; X)$ if Property $\mathbf{D}_n(C_n, \varpi)$ is known. By Proposition 2.1 we have $\mathbf{D}_n(C_n, 0)$, so that we have verified $\mathrm{Mult}_n(C_n, \mathscr{J}; 0)$.

Remark 6.11 (Non-cyclic abelian groups) The above arguments show that we are able to pick an appropriate ramification restriction to control the propagation of bad L-function factors if there exists a set that generates G and such that none of them lies in any (nontrivial, proper, normal) subgroup H of G that appears as the kernel of at least one nontrivial irreducible representation of G. We may already observe the difficulty of adapting this general strategy to a non-cyclic abelian group by considering the simple case of $G \simeq C_{p^e} \times C_{p^f}$ for a prime p. Consider an element in the generating set of the form (a, b) with $a \neq 0$. Let p^k be the highest power of p that divides both a and b. Then for $\zeta_p = e^{2\pi i/p}$, the map $C_{p^e} \times C_{p^f} \to \mathbb{C}$ given by $(i, j) \mapsto \zeta_p^{ib/p^k - ja/p^k}$ is a non-trivial irreducible representation of $C_p^e \times C_p^f$, and our generator is in the kernel of this map.

Remark 6.12 (Quartic D_4-fields) Difficulties also arise for quartic D_4-fields: there are irreducible representations of D_4 with kernels K_4, K_4' (two different subgroups isomorphic to the Klein-four group) and C_4, but no set of generators of D_4 that avoid all three of these subgroups, and hence no choice of ramification type $\mathscr{I}$ for which the three counting problems can simultaneously be resolved. It may be possible to apply our method to a particular subfamily of quartic D_4-fields generated from a fixed biquadratic field; in this case the counting problems will be trivial, although proving a lower bound that grows with X for such a family may not be.

6.5 Deduction of Theorems 3.3, 3.9, 3.11, 3.13 and 3.14 from Theorem 5.5

We have verified Condition 5.4 for each family $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ considered in the above theorems; now we apply Theorem 5.5. The family parameters notated in Condition 5.4, namely $\{M_0, M_1, A, d\}$ and $\{m_j, A_j, d_j, M_{1,j}, M_{2,j,\varepsilon}, M_{3,j,\varepsilon}, M_{5,j}\}$ for $1 \le j \le s$, all depend only on $n, G, \mathscr{I}$, and thus in the following statements we can replace any dependence on family parameters by dependence on $n, G, \mathscr{I}$.

Proposition 6.13 *Fix a family $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ considered in Theorem 3.3, 3.9, 3.11, 3.13 or 3.14 under the associated hypotheses (if any). If it is known that $X^{\beta} \ll_{n,G,\mathscr{I}} |Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| \ll_{n,G,\mathscr{I}} X^d$ and that $\mathrm{Mult}_n(G, \mathscr{I}; \tau_*)$ holds for some $\tau_* < \beta$, then the conclusions of the relevant theorem hold for those values of τ_*, β, d.*

Let $\tau_* < \beta \le d$ be as assumed in the proposition. Fix $\tau = \tau_* + \varepsilon_3$ for some sufficiently small ε_3 (in particular so that $\tau < d$) and fix $\varepsilon_0 < \min\{1/2, 2(d-\tau)\}$ sufficiently small. We apply Theorem 5.5 with

$$\Delta = 1 - \frac{\tau}{d} - \frac{\varepsilon_0}{2d}, \tag{6.8}$$

δ chosen as in (5.11) (according to $A = |G|/2$ and $\varepsilon_2 = \varepsilon_0$ so that we obtain the expression for δ in Remark 3.4), and $\eta = \varepsilon_0/2d$. Then

$$(1 - (1-\eta)\Delta)d = \tau + \frac{\varepsilon_0}{2} + \frac{\varepsilon_0}{2}(1 - \tau/d - \varepsilon_0/2d) \le \tau + \varepsilon_0.$$

Then there exists B depending only on $n, G, \mathscr{I}$ such that for all $X \ge 1$, at most

$$O_{n,G,\mathscr{I},\tau,d,\varepsilon_0}(X^{\tau+\varepsilon_0}) \tag{6.9}$$

fields $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ are such that $\zeta_{\tilde{K}}/\zeta$ can have a zero in the region

$$[1-\delta, 1] \times [-X^{\beta}, X^{\beta}], \tag{6.10}$$

where $\beta = \varepsilon_0(1 - \tau/d - \varepsilon_0/2d)/(2B)$.

Our goal now is to express this in terms of how many δ-exceptional fields there can be. It is temporarily convenient to work in terms of families of fields with discriminant in a dyadic range; thus we set $Z_n^{\mathscr{I},\sharp}(\mathbb{Q}, G; X)$ to be the subset of $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ with $X/2 < D_K \le X$. We next verify that for X sufficiently large, for every $K \in Z_n^{\mathscr{I},\#}(\mathbb{Q}, G; X)$ the region (6.10) contains the region (3.1), which we write now in the notation

$$[1-\delta, 1] \times [-(\log D_{\tilde{K}})^{2/\delta}, (\log D_{\tilde{K}})^{2/\delta}]. \tag{6.11}$$

If $K \in Z_n^{\mathscr{I},\sharp}(\mathbb{Q}, G; X)$ then by Lemma 6.1, $C_1(n, G)(X/2)^{|G|/n} \le D_{\tilde{K}} \le C_2(n, G)X^{|G|/2}$, for certain constants $C_i(n, G)$. Thus it suffices to show that there exists a threshold $D_3 = D_3(n, G, \mathscr{I}, \tau, d, \delta, \varepsilon_0)$ such that if $X \ge D_3$ then

$$(\log(C_2(n, G)X^{|G|/2}))^{2/\delta} \le X^{\beta}. \tag{6.12}$$

This is the claim that a fixed power of X is larger than any fixed power of $\log X$, as long as X is sufficiently large; thus an appropriate threshold D_3 exists.

We have shown that for every $X \ge 1$ there are at most $O_{n,G,\mathscr{I},\tau,d,\varepsilon_0}(X^{\tau+\varepsilon_0})$ fields $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ such that $\zeta_{\tilde{K}}/\zeta$ can have a zero in (6.10); consequently if $X/2 \ge D_3$, at most $O_{n,G,\mathscr{I},\tau,d,\varepsilon_0}(X^{\tau+\varepsilon_0})$ fields in $K \in Z_n^{\mathscr{I},\#}(\mathbb{Q}, G; X)$ are such that $\zeta_{\tilde{K}}/\zeta$ can have a zero in (6.11), that is, can be δ-exceptional. Now we suppose that $A \ge 2$ has been fixed, and we recall the threshold D_0 from Theorem 3.1. As long as

$$X/2 \ge D_0, \tag{6.13}$$

any $K \in Z_n^{\mathscr{I},\#}(\mathbb{Q}, G; X)$ that is not δ-exceptional satisfies the hypothesis of Theorem 3.1, and therefore for every conjugacy class $\mathscr{C} \subseteq G$ yields (3.2) for all x sufficiently large as in (3.4). Upon taking

$$D_4 = D_4(n, G, \mathscr{I}, \tau, d, \delta, \varepsilon_0, c_{\mathbb{Q}}, C_1, C_2, A) := \max\{D_0, D_3\}$$

we have shown that for any X such that $X/2 \ge D_4$ we have that at most $O_{n,G,\mathscr{I},\tau,d,\varepsilon_0}(X^{\tau+\varepsilon_0})$ fields in $K \in Z_n^{\mathscr{I},\#}(\mathbb{Q}, G; X)$ can be δ-exceptional, and for all remaining fields, (3.2) holds for all x satisfying (3.4). We may in fact omit the dependence on δ in the notation, as it is defined in terms of the other parameters.

The final step to complete the proof of Proposition 6.13 is to sum over dyadic ranges of discriminants. Now for any $X \geq 1$ (say using $\log_2$ temporarily),

$$Z_n^{\mathscr{I}}(\mathbb{Q}, G; X) \subseteq \bigcup_{j=0}^{1+\log X} Z_n^{\mathscr{I},\sharp}(\mathbb{Q}, G; 2^j).$$

We may dissect this into two pieces: those for which j is such that $2^{j-1} \geq D_4$, in which case our work above applies, and we conclude that the number of δ-exceptional fields in

$$\bigcup_{2^{j-1} \geq D_4}^{1+\log X} Z_n^{\mathscr{I},\sharp}(\mathbb{Q}, G; 2^j)$$

is at most

$$\sum_{2^{j-1} \geq D_4}^{1+\log X} O_{n,G,\mathscr{I},\tau,d,\varepsilon_0}((2^j)^{\tau+\varepsilon_0}) = O_{n,G,\mathscr{I},\tau,d,\varepsilon_0}(X^{\tau+\varepsilon_0}). \tag{6.14}$$

For those j such that $2^{j-1} \leq D_4$, we count all the fields as possible exceptions, noting that

$$\left| \bigcup_{1 \leq 2^{j-1} \leq D_4} Z_n^{\mathscr{I},\sharp}(\mathbb{Q}, G; 2^j) \right| \leq |Z_n^{\mathscr{I}}(\mathbb{Q}, G; 2D_4)| \ll_{n,G} D_4^d.$$

We enlarge the implied constant in (6.14) to include this constant, and call the resulting implied constant D_5, as appears in the theorem statements. This completes the proof of Proposition 6.13, and in combination with the values of τ_* supplied by Proposition 6.8, we have proved Theorems 3.3, 3.9, 3.11, 3.13 and 3.14 (and the non-quantitative Theorem 1.1).

6.6 Proof of Corollary 3.16

Let $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ be a specified family, with corresponding parameters $\tau_* < \beta \leq d$, set $A = 2$ and let ε_0 (sufficiently small) be fixed, with corresponding choice $\delta \leq 1/4$. First, we verify that for $\sigma > 0$ fixed, there is a threshold $D_6' = D_6'(n, G, \mathscr{I}, d, c_{\mathbb{Q}}, C_5, C_6, \varepsilon_0, \sigma)$ such that for $D_K \geq D_6'$,

$$D_K^\sigma \geq \kappa_1 \exp\{\kappa_2 (\log\log(D_{\tilde{K}}^{\kappa_3}))^{5/3} (\log\log\log(D_{\tilde{K}}^2))^{1/3}\},$$

where this lower bound is as stated in (3.4), and the parameters κ_i have the dependencies $\kappa_i = \kappa_i(n, G, d, c_{\mathbb{Q}}, C_5, C_6, \varepsilon_0)$ (dropping the notational dependence on $A = 2$). In fact it suffices to compute a threshold above which

$$D_K^\sigma \geq \kappa_1 \exp\{\kappa_2 (\log\log(D_{\tilde{K}}^{\kappa_5}))^2\}$$

where we set $\kappa_5 = \max\{\kappa_3, 2\}$. By Lemma 6.1, $D_{\tilde{K}} \leq C_2(n, G) D_K^{|G|/2}$ for a certain constant $C_2(n, G)$, so that it further suffices to show

$$D_K^\sigma \geq \kappa_1 \exp\{\kappa_2 (\log\log(\kappa_6 D_K^{\kappa_7}))^2\}$$

where $\kappa_6 = C_2(n, G)^{\kappa_5}$ and $\kappa_7 = \kappa_5 |G|/2$. This will hold when D_K is sufficiently large that

$$\sigma \geq \frac{\log \kappa_1}{\log D_K} + \frac{\kappa_2 (\log\log(\kappa_6 D_K^{\kappa_7}))^2}{\log D_K},$$

and we denote this threshold by $D_6' = D_6'(n, G, \mathscr{I}, d, c_{\mathbb{Q}}, C_5, C_6, \varepsilon_0, \sigma)$. Finally, recall the parameter D_0 provided in Theorem 3.1. While this is used as a constraint $D_{\tilde{K}} \geq D_0$, we apply Lemma 6.1 to see that $D_{\tilde{K}} \geq C_1(n, G) D_K^{|G|/n}$ for a certain constant $C_1(n, G)$. Then $D_{\tilde{K}} \geq D_0$ is certainly satisfied if $D_K \geq D_0'$ with

$$D_0' := (C_1(n, G)^{-1} D_0)^{n/|G|}. \tag{6.15}$$

Now for part (1) of Corollary 3.16, we may conclude from Theorem 3.1 with $A = 2$ that for every $X \geq 1$, for every field in $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ that has $D_K \geq \max\{D_0', D_6'\}$ and is not δ-exceptional,

$$\left| \pi_{\mathscr{C}}(D_K^\sigma, \tilde{K}/\mathbb{Q}) - \frac{|\mathscr{C}|}{|G|} \mathrm{Li}(D_K^\sigma) \right| \leq \frac{|\mathscr{C}|}{|G|} \frac{D_K^\sigma}{(\log D_K^\sigma)^2}. \tag{6.16}$$

Finally, we enlarge $\max\{D_0', D_6'\}$ if necessary to a parameter D_6, so that for all $D_K \geq D_6$, the error term in (6.16) is at most $(1/2)|G|^{-1}\mathrm{Li}(D_K^\sigma) \leq (1/2)|\mathscr{C}||G|^{-1}\mathrm{Li}(D_K^\sigma)$. Then $\pi_{\mathscr{C}}(D_K^\sigma, \tilde{K}/\mathbb{Q}) \geq (1/2)|\mathscr{C}||G|^{-1}\mathrm{Li}(D_K^\sigma) \geq (1/2)|G|^{-1}\mathrm{Li}(D_K^\sigma)$, and we can further enlarge D_6 if necessary to write the lower bound as in (3.7).

For part (2) of Corollary 3.16, we may follow e.g. Vaaler and Widmer [81, Lemma 5.1] (but without assuming GRH, as they do). Suppose that K is not δ-exceptional and furthermore that $D_K \geq D_0'$ with parameter D_0' as above in (6.15). Then for every x satisfying the lower bound (3.4), we apply (3.2)

with $A = 2$ to both $\pi_{\mathscr{C}}(x, \tilde{K}/\mathbb{Q})$ and $\pi_{\mathscr{C}}(2x, \tilde{K}/\mathbb{Q})$. If the (non-negative) difference

$$\pi_{\mathscr{C}}(2x, \tilde{K}/\mathbb{Q}) - \pi_{\mathscr{C}}(x, \tilde{K}/\mathbb{Q}) \tag{6.17}$$

were zero, this in combination with (3.2) would imply that

$$\mathrm{Li}(2x) - \mathrm{Li}(x) \leq \frac{2x}{(\log 2x)^2} + \frac{x}{(\log x)^2} \leq \frac{3x}{(\log x)^2}. \tag{6.18}$$

Yet certainly for $x \geq 2$,

$$\int_x^{2x} \frac{dt}{\log t} \geq \frac{x}{\log 2x} \geq \frac{x}{2\log x}.$$

Thus (6.18) fails (so the difference in (6.17) must be ≥ 1) as soon as $x \geq \max\{2, e^6\}$. Given $\sigma > 0$, we apply this to $x = D_K^{\sigma}$, in which case we require $D_K \geq D_7 = \max\{D_0', D_6', 2, e^6\}$ with the parameter D_6' (depending on σ) as above. This completes the verification of Corollary 3.16.

Part III: Applications

7 Bounding ℓ-torsion in class groups

For a finite extension $K/\mathbb{Q}$, the ideal class group Cl_K is a finite abelian group that encodes information about arithmetic in K, and interest in the class number $|\mathrm{Cl}_K|$ has a long history, going back to the Gauss class number conjecture, early attempts at proving Fermat's Last Theorem, and Dirichlet's development of the class number formula, which unites class numbers with L-functions. We focus on the ℓ-torsion subgroup of Cl_K, defined for any integer $\ell \geq 1$ by

$$\mathrm{Cl}_K[\ell] := \{[\mathfrak{a}] \in \mathrm{Cl}_K : [\mathfrak{a}]^{\ell} = \mathrm{Id}\}. \tag{7.1}$$

For any number field $K/\mathbb{Q}$ of degree n and absolute discriminant $D_K = |\mathrm{Disc}\, K/\mathbb{Q}|$, we may trivially bound the ℓ-torsion subgroup by the full class group, which admits the following bound (see [59, Theorem 4.4]):

$$1 \leq |\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}, \tag{7.2}$$

for any integer $\ell \geq 1$, and $\varepsilon > 0$ arbitrarily small. We will refer to this as the trivial bound for $|\mathrm{Cl}_K[\ell]|$.

Our work on ℓ-torsion is inspired by the following well-known conjecture (e.g. see [9, "Question CL(ℓ, d)"], [26], [90, Conjecture 3.5]):

Conjecture 7.1 (ℓ-torsion Conjecture) *Let $K/\mathbb{Q}$ be a number field of degree n. Then for every integer $\ell \geq 1$ and every $\varepsilon > 0$,*

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

Now, with our new effective Chebotarev theorems for families of fields, we can make new progress toward this conjecture: we improve on the trivial bound (7.2) and in fact do as well as previous bounds that assumed GRH, for all but a possible density zero subfamily of fields. In particular, we prove the first unconditional nontrivial upper bounds for ℓ-torsion, for all $\ell \geq 1$, for almost all fields in infinite families of fields of arbitrarily high degree.

Theorem 7.2 *Let $Z_n^{\mathscr{F}}(\mathbb{Q}, G)$ be fixed to be one of the families of fields considered in Theorems 3.3, 3.9, 3.11, 3.13 and 3.14, and correspondingly assume the hypotheses (if any) of the relevant theorem. Let the parameters $\tau_* < \beta \leq d$ be those proved to exist for that family in (3.5). For every $\tau > \tau_*$ sufficiently close to τ_*, every $\varepsilon_0 > 0$ sufficiently small, and every integer $\ell \geq 1$, there exists a constant D_8 such that for for every $X \geq 1$, aside from at most $D_8 X^{\tau+\varepsilon_0}$ exceptions, every field $K \in Z_n^{\mathscr{F}}(\mathbb{Q}, G; X)$ satisfies*

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,G,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon} \tag{7.3}$$

for all $\varepsilon > 0$.

Recalling that for each family considered we have shown that $|Z_n^{\mathscr{F}}(\mathbb{Q}, G; X)| \gg_{n,G,\mathscr{F}} X^{\beta}$ with $\beta > \tau_*$, the exceptional family has density zero once τ is sufficiently close to τ_* and ε_0 is taken to be sufficiently small. (In Sect. 7.2.1, we re-state Theorem 7.2 in terms of *averages* of ℓ-torsion.)

The deduction of Theorem 7.2 follows a general approach codified by Ellenberg and Venkatesh for bounding ℓ-torsion in Cl_K by finding many small rational primes that split completely in K:

Theorem H ([31, Lemma 2.3]) *Suppose $K/\mathbb{Q}$ is an extension of degree n, and let ℓ be a positive integer. Set $0 < \delta < \frac{1}{2\ell(n-1)}$ and suppose that there are at least M rational primes with $p \leq D_K^{\delta}$ that are unramified and split completely in K. Then for any $\varepsilon > 0$,*

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

To find small primes that split completely in K it is sufficient to find small primes that split completely in the Galois closure $\tilde{K}$ of K over $\mathbb{Q}$, and to do so Ellenberg and Venkatesh applied Lagarias and Odlzyko's conditional Theorem A to obtain:

Theorem I ([31, Prop. 3.1]) *Let $K/\mathbb{Q}$ be a number field of degree n and $\ell \geq 1$ an integer. Assuming GRH, then for any $\varepsilon > 0$,*

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}. \tag{7.4}$$

The argument in Sect. 7.2 will show that any quantitative improvement to the exponent obtained in Theorems H and I is expected to be similarly reflected in the exponent obtained in (7.3).

As n, ℓ grow large, to produce the primes required in Theorem H, we must be allowed to count primes as small as any fixed positive power of D_K. This in particular illuminates why previously known lower bounds for $\pi_{\mathscr{C}}(x, L/k)$, such as obtained in the recent work of Thorner and Zaman [78], [77, Eqn. 1.6], or even the result of Theorem B (assuming no exceptional zero β_0 exists, or in the setting of Theorem 4.12), do not suffice for our application. The new results in Theorem 7.2 show that the following fields satisfy (7.3) unconditionally, for all integers $\ell \geq 1$:

(i) almost all degree p cyclic extensions of $\mathbb{Q}$ (p prime)
(ii) almost all totally ramified cyclic extensions of $\mathbb{Q}$
(iii) almost all degree p D_p-extensions ($\mathscr{I}$ the conjugacy class of order 2 elements, odd prime p)
(iv) almost all degree 4 A_4-extensions ($\mathscr{I}$ the two conjugacy classes of order 3 elements).

Furthermore, Theorem 7.2 shows that for every $n \geq 2$, almost all degree n S_n-extensions of $\mathbb{Q}$ with square-free discriminants satisfy (7.3) for all $\ell \geq 1$, where this result is

(v) unconditional if $n = 2, 3, 4$
(vi) if $n = 5$, conditional on the strong Artin conjecture
(vii) if $n \geq 6$, conditional on the strong Artin conjecture and $\mathbf{D}_n(S_n, \varpi_n)$ for some $\varpi_n < 1/2 + 1/n$.

Finally, Theorem 7.2 shows (among other results for simple groups) that (7.3) holds

(viii) for every $n \geq 5$, almost all degree n A_n-extensions of $\mathbb{Q}$ satisfy (7.3) for all $\ell \geq 1$, conditional on the strong Artin conjecture.

Remark 7.3 In fact, our proof of Theorem 7.2 works as well if we replace any of our families of fields with the family of their Galois closures.

7.1 Previous results toward Conjecture 7.1

To situate our results, we briefly review previous results in the literature toward Conjecture 7.1 in terms of a property we now define.

Property 7.4 ($\mathbf{C}_{n,\ell}(\Delta)$) *Given integers $n, \ell \geq 1$ and a fixed real number $\Delta \geq 0$, we say that property $\mathbf{C}_{n,\ell}(\Delta)$ holds if it is known that for every $\varepsilon > 0$ there is a constant $C_{\Delta,n,\ell,\varepsilon}$ such that for all fields $K/\mathbb{Q}$ of degree n,*

$$|\mathrm{Cl}_K[\ell]| \leq C_{\Delta,n,\ell,\varepsilon} D_K^{\Delta+\varepsilon}.$$

Thus in particular, (7.2) shows that $\mathbf{C}_{n,\ell}(1/2)$ is trivially true for all $n, \ell \geq 1$. The strongest type of result holds for *all* fields of a fixed degree. In this vein, Gauss [34] genus theory shows $\mathbf{C}_{2,2}(0)$ holds. This is the only case in which Conjecture 7.1 is known to hold, for a certain prime ℓ, for all fields of a fixed degree. The only other known pointwise bounds for prime ℓ are: $n = 2$ and $\ell = 3$, where initial progress occurred in [41,64,65], and [31] holds the record $\mathbf{C}_{2,3}(1/3)$; $\mathbf{C}_{3,3}(1/3)$ due to [31]; $\mathbf{C}_{4,3}(1/2-\delta)$ due to [31] where $\delta = 1/168$ if K is non-D_4; $\mathbf{C}_{n,2}(0.2784...)$ for $n = 3, 4$ and $\mathbf{C}_{n,2}(1/2 - 1/2n)$ where $n \geq 5$, due to [10]. Also in [31], there is a proof of pointwise bounds for ℓ-torsion for certain families of fields of arbitrarily high degree, where these fields always contain $\zeta_\ell + \zeta_\ell^{-1}$. Conditional on the Birch–Swinnerton–Dyer conjecture and GRH, Wong [85] has observed that $\mathbf{C}_{2,3}(1/4)$ holds.

For $n = 2, 3, 4, 5$, bounds for ℓ-torsion at least as strong as (7.3) were already known to hold, unconditionally, for *almost all* degree n S_n-fields (without any ramification condition). For imaginary quadratic fields, Soundararajan [71] showed that for each prime ℓ, the nontrivial bound $|\mathrm{Cl}_K[\ell]| \ll_{\ell,\varepsilon} D_K^{1/2-1/2\ell+\varepsilon}$ holds for all but a possible family of exceptional fields of density zero. Furthermore, Heath-Brown and the first author [37] obtained for each prime $\ell \geq 5$ the unconditional bound $|\mathrm{Cl}_K[\ell]| \ll_{\ell,\varepsilon} D_K^{1/2-3/(2\ell+2)+\varepsilon}$ for all but a possible density zero family of imaginary quadratic fields; their methods also yield upper bounds for higher moments of ℓ-torsion for all $\ell \geq 3$. For each degree $n \leq 5$, Ellenberg and the first and third authors [28] proved the bound (7.3) holds unconditionally for all but a possible density zero exceptional family of degree n extensions of $\mathbb{Q}$. (In the case $n = 4$, this work had the additional requirement that the fields be non-D_4 quartic fields and $\ell \geq 8$ and for $n = 5$, the requirement $\ell \geq 25$.) In both [37] and [28], the upper bound for the possible exceptional family becomes weaker as ℓ increases (e.g. in [28] the number of exceptional fields is at most $O_{n,\varepsilon}(X^{1-1/(2\ell(n-1))+\varepsilon})$ for ℓ large); this is noticeably different from the bound for the exceptional set in Theorem 7.2.

Remark 7.5 At the time of posting, the authors learned of the works of Frei and Widmer [33] and Widmer [83]. Frei and Widmer obtain the upper bound (7.3) for ℓ-torsion for almost all totally ramified cyclic extensions of $\mathbb{Q}$ (see our case (ii) above), albeit with a larger upper bound for the possible exceptional family of fields, analogous to that in [28]. Frei and Widmer use the sieve method of Ellenberg and the first and third authors [28] combined with new counts for the

number of totally ramified cyclic extensions with a finite number of specified local conditions. Notably, their method also works for totally ramified cyclic extensions of any fixed number field F. Moreover they remark, building on [83], on the possibility of sharpening to $1/2 - 1/(\ell(n+1))$ the exponent in (7.4) for almost all fields in a family $Z_n(\mathbb{Q}, G; X)$ that is sufficiently dense (e.g. $|Z_n(\mathbb{Q}, G; X)| \gg X$). Of the families we consider, the latter strategy could conceivably similarly improve the exponent in (7.3) only for the family $Z_n^{\mathscr{I}}(\mathbb{Q}, S_n; X)$, conditional on such a lower bound being known for the family. We thank Frei and Widmer for sharing their preprint [33].

7.2 Proof of Theorem 7.2

Theorem 7.2 is an immediate consequence of Corollary 3.16. We suppose that a family $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ and a sufficiently small $\varepsilon_0 > 0$ have been fixed. We let $0 < \delta \leq 1/4$ be defined as in (3.6). We set $\mathscr{C} = \{\mathrm{id}\}$, in which case we are counting primes that split completely in $\tilde{K}$ and hence in K. For any integer $\ell \geq 1$, we take $\tau > \tau_*$ sufficiently close and a sufficiently small $\varepsilon_1 > 0$ and we set $\sigma = 1/(2\ell(n-1)) - \varepsilon_1$. Then for every $X \geq 1$, for any field $K \in Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ with $D_K \geq D_6$ that is not one of the at most $D_3 X^{\tau+\varepsilon_0}$ δ-exceptional fields in $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, there are $\gg_{G,n,\ell,\varepsilon_1} D_K^{1/2(\ell(n-1))-\varepsilon_1}/\log D_K$ primes $p \leq D_K^{1/2(\ell(n-1))-\varepsilon_1}$ that split completely in K. Thus for such a K that is not δ-exceptional, by Theorem H,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,G,\ell,\varepsilon_1,\varepsilon_2} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}-\varepsilon_1+\varepsilon_2}, \tag{7.5}$$

for all sufficiently small $\varepsilon_1, \varepsilon_2 > 0$. Now we count all those fields that are δ-exceptional and all those fields in $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$ that have discriminant smaller than D_6, of which there are at most $\ll_{n,G,\mathscr{I}} D_6^d$, by the definition of the parameter d. Defining $D_8 = D_8(n, \ell, G, \mathscr{I}, d, \tau, \varepsilon_0)$ to be an appropriate maximum of D_3 and the above multiple of D_6^d, we see that for every $X \geq 1$ we may say that (7.5) holds for each field in $Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)$, apart from at most $D_8 X^{\tau+\varepsilon_0}$ fields. This completes the proof of Theorem 7.2.

7.2.1 *Averages of ℓ-torsion*

The results of Theorem 7.2 can alternatively be stated in terms of averages of ℓ-torsion over a fixed family of degree n extensions. If $|Z_n^{\mathscr{I}}(\mathbb{Q}, G; X)| \ll_{n,G,\mathscr{I}} X^d$, Theorem 7.2 shows that for all $X \geq 1$, $\ell \geq 1$, $\tau > \tau_*$ sufficiently close, ε_0 sufficiently small,

$$\sum_{K \in Z_n^{\mathscr{I}}(\mathbb{Q},G;X)} |\mathrm{Cl}_K[\ell]| \ll X^{d+\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon} + X^{\tau+\frac{1}{2}+\varepsilon_0+\varepsilon},$$

for every $\varepsilon > 0$, with an implied constant depending on n, ℓ, G, $\mathscr{I}$, d, τ, ε_0, ε. For $\tau_* < \tau < d$, for ℓ sufficiently large we will obtain $\tau \le d - 1/(2\ell(n-1))$, so that

$$\sum_{K \in Z_n^{\mathscr{I}}(\mathbb{Q},G;X)} |\mathrm{Cl}_K[\ell]| \ll X^{d+\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$$

for every $\varepsilon > 0$. The "trivial bound" would be $\ll_{n,G,\mathscr{I},\varepsilon} X^{d+\frac{1}{2}+\varepsilon}$ for all $\varepsilon > 0$.

8 Number fields with small generators

For our second application, we turn to a question of whether all number fields have a "small" generator. Given a number field $K/\mathbb{Q}$ of degree n (inside our fixed algebraic closure $\overline{\mathbb{Q}}$), one can ask for the element $\alpha \in K$ of smallest height $H(\alpha)$ such that $K = \mathbb{Q}(\alpha)$; here $H(\alpha)$ denotes the absolute multiplicative Weil height. Precisely, for an element $\alpha \in K$,

$$H(\alpha) = \prod_v \max\{1, |\alpha|_v\}^{\frac{d_v}{n}},$$

in which v runs over the places of K and for each place v, $|\cdot|_v$ is the unique representative that either extends the Archimedean absolute value on $\mathbb{Q}$ or a p-adic absolute value on $\mathbb{Q}$, while $d_v = [K_v : \mathbb{Q}_v]$ denotes the local degree at v. (By Northcott's theorem [62, Thm.1], there are finitely many elements in K with height at most any fixed real number, and thus a generator of smallest height does exist.)

In terms of lower bounds, it is known by Silverman [70, Thm. 1] that for each $n \ge 2$, for all fields $K/\mathbb{Q}$ of degree n, for any element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$,

$$H(\alpha) \ge B_1 D_K^{\frac{1}{2n(n-1)}}, \tag{8.1}$$

where we may take $B_1 = B_1(n) = n^{-\frac{1}{2(n-1)}}$. In fact, this lower bound led to the numerology of the savings in the exponent in Theorem I. (See [31, Lemma 2.2], with the lower bound now further explored in the recent preprints [33,83], where it is shown that improving on (8.1) for a sufficiently dense class of fields can improve on Theorem I in an average sense.)

On the other hand, regarding upper bounds, Ruppert asked two questions [66] of increasing strength:

Question 8.1 *Does there exist for each $n \geq 2$:*

(1) *a positive constant $B_2 = B_2(n)$ such that for every field $K/\mathbb{Q}$ of degree n there exists an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ and $H(\alpha) \leq B_2 D_K^{\frac{1}{2n}}$?*

(2) *a positive constant $B_3 = B_3(n)$ such that for every field $K/\mathbb{Q}$ of degree n there exists an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ and $H(\alpha) \leq B_3 D_K^{\frac{1}{2n(n-1)}}$?*

(Ruppert posed these questions in terms of the naive height, but up to constants this is equivalent to the form given here, for which we cite the presentations of [81,82].) The second question is effectively asking whether the exponent in Silverman's lower bound (8.1) is sharp. For degree $n = 2$ the two questions are equivalent, and Ruppert [66, Prop. 2] answered them in the affirmative. Moreover, [66, Prop. 3] verified (1) for totally real fields K of prime degree. Recently, Vaaler and Widmer [81, Thm. 1.2] verified (1) for all number fields with at least one real embedding, with a constant $B_2(n) \leq 1$. In contrast, they provided in [82], for each composite degree n, an infinite family of fields violating (2). Furthermore, in [83, §3 and §4], Widmer shows that for $n \geq 4$, the number of degree n fields satisfying the bound in case (2) of Question 8.1 is $o(X)$, so that the answer to this case must be no. (For clarity, note that Widmer works in terms of the relative Weil height.)

This leaves the question of whether case (1) is true. As an application of our effective Chebotarev density theorem, we show that within appropriate families of fields, (1) is true for "almost all" fields.

Theorem 8.2 *Let $Z_n^{\mathscr{F}}(\mathbb{Q}, G)$ be fixed to be one of the families of fields considered in Theorems 3.3, 3.9, 3.11, 3.13 and 3.14, and correspondingly assume the hypotheses (if any) of the relevant theorem. Let the parameters $\tau_* < \beta \leq d$ be those proved to exist for that family in (3.5). For every $\tau > \tau_*$ sufficiently close and every $\varepsilon_0 > 0$ sufficiently small, there exists a constant D_9 such that for every $X \geq 1$, aside from at most $D_9 X^{\tau+\varepsilon_0}$ exceptions, every field $K \in Z_n^{\mathscr{F}}(\mathbb{Q}, G; X)$ contains an element α with $K = \mathbb{Q}(\alpha)$ such that $H(\alpha) \leq 2 D_K^{\frac{1}{2n}}$.*

The proof is a simple adaptation of an observation of Vaaler and Widmer in [81, Thm. 1.3], which relies on finding primes that split completely in K that are of size around $D_K^{1/2}$. They showed that the bound in Question 8.1 case (1) holds whenever $\zeta_{\tilde{K}}$ satisfies GRH, via an application of Theorem A. Now, independent of GRH, for every field that is not δ-exceptional, with δ determined by (3.6), we apply part (2) of Corollary 3.16 with the choices $\mathscr{C} = \{1\}$ and $\sigma = 1/2$, in place of [81, Lemma 5.1]. Then [81, Thm. 4.1] shows that for each field K to which the conclusion (3.8) applies, there exists an element $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ and $H(\alpha) \leq p^{1/n} \leq 2 D_K^{1/2n}$. We use Theorem 3.3 to bound

the number of δ-exceptional fields, with δ determined by (3.6). We use the trivial upper bound $|Z_n^{\mathscr{J}}(\mathbb{Q}, G; D_7)| \ll_{n,G,\mathscr{J}} D_7^d$ for the number of fields in the family with discriminant smaller than the threshold D_7 required to apply part (2) of Corollary 3.16. Then upon setting $D_9 = D_9(n, G, \mathscr{J}, d, \tau, \varepsilon_0)$ to be an appropriate maximum of D_3 from Theorem 3.3 and the above multiple of D_7^d, we may then conclude Theorem 8.2 holds.

Acknowledgements The authors thank P. Sarnak for his prescient advice and consistent encouragement over many years. We thank M. Bhargava for a number of suggestions for quantitative results for families of number fields, and A. Venkatesh and M. Bhargava for indicating a method for counting degree n A_n-fields. We thank M. Abel, D. R. Heath-Brown, J. Getz, N. Katz, E. Kowalski, M. Milinovich, M. Nastasescu, D. Ramakrishnan, Z. Rudnick, A. Sutherland, for helpful comments and F. Thorne, A. Zaman for remarks on an earlier version of the manuscript. We also thank the referees for their close reading and helpful comments. Pierce has been partially supported by NSF DMS-1402121, CAREER Grant DMS-1652173, a Sloan Research Fellowship, and as a von Neumann Fellow at the Institute for Advanced Study, by the Charles Simonyi Endowment and NSF Grant No. 1128155. Pierce thanks the Max Planck Institute for Mathematics, the Hausdorff Center for Mathematics, and MSRI (under NSF Grant No. 1440140) for providing focused research environments. Turnage-Butterbaugh is partially supported by NSF DMS-1901293 and was supported by NSF DMS-1440140 while in residence at MSRI during the Spring 2017 semester. Wood has been partially supported by an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, National Science Foundation Grant DMS-1301690 and CAREER Grant DMS-1652116, and a Vilas Early Career Investigator Award.

References

1. Arthur, J., Clozel, L.: Simple Algebras, Base Change, and the Advanced Theory of the Trace Formula. Annals of Mathematics Studies, vol. 120. Princeton University Press, Princeton (1989)
2. Artin, E.: Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren. Abh. Math. Sem. Univ. Hamburg **8**, 292–306 (1930)
3. Baily, A.M.: On the density of discriminants of quartic fields. J. Reine Angew. Math. **315**, 190–210 (1980)
4. Bhargava, M.: The density of discriminants of quartic rings and fields. Ann. Math. **162**(2), 1031–1063 (2005)
5. Bhargava, M.: Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. Int. Math. Res. Not. **2007**, 20 (2007)
6. Bhargava, M.: The density of discriminants of quintic rings and fields. Ann. Math. **172**(3), 1559–1591 (2010)
7. Bhargava, M.: The geometric sieve and the density of squarefree values of invariant polynomials (2014). arXiv:1402.0031v1
8. Booker, A.R.: Artin's conjecture, Turing's method, and the Riemann hypothesis. Exp. Math. **15**(4), 385–407 (2006)
9. Brumer, A., Silverman, J.H.: The number of elliptic curves over $\mathbb{Q}$ with conductor N. Manuscr. Math. **91**(1), 95–102 (1996)
10. Bhargava, M., Shankar, A., Taniguchi, T., Thorne, F., Tsimerman, J., Zhao, Y.: Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves (2017). arXiv:1701.02458

11. Bhargava, M., Shankar, A., Wang, X.: Squarefree values of polynomial discriminants (2016). arXiv:1611.09806v2
12. Calegari, F.: The Artin conjecture for some S_5-extensions. Math. Ann. **356**(1), 191–207 (2013)
13. Castillo, A., Dietmann, R.: On Hilbert's irreducibility theorem (2016). arXiv:1602.00314
14. Cohen, H., Diaz, F.D., Olivier, M.: Enumerating quartic dihedral extensions of $\mathbb{Q}$. Compos. Math. **133**(1), 65–93 (2002)
15. Cho, P.J., Kim, H.H.: Dihedral and cyclic extensions with large class numbers. Journal de Théorie des Nombres **24**, 583–603 (2012)
16. Cho, P.J., Kim, H.H.: Probabilistic properties of number fields. J. Number Theory **133**, 4175–4187 (2013)
17. Cho, P.J., Kim, H.H.: Effective prime ideal theorem and exponents of ideal class groups. Q. J. Math. **65**, 1179–1193 (2014)
18. Chambert-Loir, A., Tschinkel, Y.: Fonctions zêta des hauteurs des espaces fibrés. In: Rational points on algebraic varieties. Progress in Mathematics, vol. 199, pp. 71–115. Birkhäuser, Basel (2001)
19. Cohn, H.: The density of abelian cubic fields. Proc. Am. Math. Soc. **5**, 476–477 (1954)
20. Cohen, H., Thorne, F.: On D_ℓ-extensions of odd prime degree ℓ (2016). arXiv:1609.09153
21. Debaene, K.: Explicit counting of ideals and a Brun–Titchmarsh inequality for the Chebotarev density theorem (2016). arXiv:1611.10103
22. Dèbes, Pierre: On the Malle conjecture and the self-twisted cover. Israel J. Math. **218**(1), 101–131 (2017)
23. Davenport, H., Heilbronn, H.: On the density of discriminants of cubic fields II. Proc. R. Soc. Lond. A **322**, 405–420 (1971)
24. Deligne, P., Serre, J.-P.: Formes modulaires de poids 1. Ann. Sci. École Norm. Sup. (4) **7**, 507–530 (1975). 1974
25. Duke, W.: The dimension of the space of cusp forms of weight one. Int. Math. Res. Not. **2**, 99–109 (1995)
26. Duke, W.: Bounds for arithmetic multiplicities. In: Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), number extra vol. II, pp. 163–172 (1998)
27. Dwyer, J.: Real zeros of Artin L-functions corresponding to five-dimensional S_5-representations. Bull. Lond. Math. Soc. **46**(1), 51–58 (2014)
28. Ellenberg, J.S., Pierce, L.B., Wood, M.M.: On ℓ-torsion in class groups of number fields. Algebra Number Theor. **11**(8), 1739–1778 (2017). https://doi.org/10.2140/ant.2017.11.1739
29. Ellenberg, J.S., Venkatesh, A.: Counting extensions of function fields with bounded discriminant and specified Galois group. In: Geometric Methods in Algebra and Number Theory, Progress in Mathematics, vol. 235, pp. 151–168. Birkhäuser, Boston (2005)
30. Ellenberg, J.S., Venkatesh, A.: The number of extensions of a number field with fixed degree and bounded discriminant. Ann. Math. (2) **163**(2), 723–741 (2006)
31. Ellenberg, J.S., Venkatesh, A.: Reflection principles and bounds for class group torsion. Int. Math. Res. Not. IMRN (1), Art. ID rnm002, 18 (2007)
32. Frei, C., Loughran, D., Newton, R.: The Hasse norm principle for abelian extensions (2015). arXiv:1508.02518
33. Frei, C., Widmer, M.: Average bounds for the ℓ-torsion in class groups of cyclic extensions (2017). arXiv:1709.09934
34. Gauss, C.F.: Disquisitiones Arithmeticae, 1801. (Trans. Arthur A. Clarke). Yale University Press, New Haven (1965), 1801
35. Grenié, L., Molteni, G.: An effective Chebotarev density theorem under GRH (2017). arXiv:1709.07609v1

36. Harcos, G.: New bounds for automorphic L-functions. ProQuest LLC, Ann Arbor, MI (2003). Thesis (Ph.D.)–Princeton University
37. Heath-Brown, D.R., Pierce, L.B.: Averages and moments associated to class numbers of imaginary quadratic fields. Compos. Math. **153**, 2287–2309 (2017)
38. Heilbronn, H: On the 2-class group of cubic fields. In: Studies in Pure Mathematics (Presented to Richard Rado), pp. 117–119. Academic Press, London (1971)
39. Heilbronn, H.: On real simple zeros of Dedekind ζ-functions. In: Proceedings of the Number Theory Conference (University Colorado, Boulder, CO, 1972), pp. 108–110. University Colorado, Boulder, CO (1972)
40. Hilbert, D.: Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. J. Reine Angew. Math. **110**, 104–129 (1892)
41. Helfgott, H.A., Venkatesh, A.: Integral points on elliptic curves and 3-torsion in class groups. J. Am. Math. Soc. **19**(3), 527–550 (2006)
42. Iwaniec, H., Kowalski, E.: Analytic Number Theory, vol. 53. American Mathematical Society Colloquium Publications, Providence (2004)
43. Klüners, J.: Asymptotics of number fields and the Cohen–Lenstra heuristics. J. Théor. Nombres Bordeaux **18**, 607–615 (2006)
44. Klüners, J.: The number of S_4-fields with given discriminant. Acta Arith. **122**(2), 185–194 (2006)
45. Kowalski, E., Michel, P.: Zeros of families of automorphic L-functions close to 1. Pac. J. Math. **207**(2), 411–431 (2002)
46. Klüners, J., Nicolae, F.: Are number fields determined by Artin L-functions. J. Number Theory **167**, 161–168 (2016)
47. Korobov, N.M.: Estimates of trigonometric sums and their applications. Uspehi Mat. Nauk **13**(4 (82)), 185–192 (1958)
48. Langlands, R.P.: Base change for GL(2), vol. 96, Annals of Mathematics Studies. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo (1980)
49. Lagarias, J.C., Montgomery, H.L., Odlyzko, A.M.: A bound for the least prime ideal in the Chebotarev density theorem. Invent. Math. **54**(3), 271–296 (1979)
50. Lagarias, J., Odlyzko, A.: Effective versions of the Chebotarev density theorem. In: Proceedings of Symposia, pp. 409–464, Durham University, Durham (1975)
51. Mäki, S.: On the density of abelian number fields. Ann. Acad. Sci. Fenn. Ser. A I Math. Dissertationes **54**, 104 (1985)
52. Malle, G.: On the distribution of Galois groups. J. Number Theory **92**, 315–219 (2002)
53. Malle, G.: On the distribution of Galois groups II. Exp. Math. **13**, 129–135 (2004)
54. Martin, K.: A symplectic case of Artin's conjecture. Math. Res. Lett. **10**(4), 483–492 (2003)
55. Martin, K.: Four-dimensional Galois representations of solvable type and automorphic forms. Thesis (Ph.D.), California Institute of Technology (2004)
56. Michel, P.: Analytic number theory and families of automorphic L-functions. In: Automorphic forms and applications, IAS/Park City Mathematics Series, vol. 12, pp. 181–295. American Mathematical Society, Providence, RI (2007)
57. Martin, K., Ramakrishnan, D.: A comparison of automorphic and Artin L-series of GL(2)-type agreeing at degree one primes. In: Advances in the Theory of Automorphic Forms and their L-Functions. Contemporary Mathematics, vol. 664, pp. 339–350. American Mathematical Society, Providence, RI, (2016)
58. Murty, V.K.: Stark zeros in certain towers of fields. Math. Res. Lett. **6**(5–6), 511–519 (1999)
59. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, 2nd edn. Springer, Berlin (1980)
60. Narkiewicz, W.: The Development of Prime Number Theory. Springer Monographs in Mathematics. Springer, Berlin (2000). From Euclid to Hardy and Littlewood
61. Neukirch, J.: Algebraic Number Theory. Springer, Berlin (1999)

62. Northcott, D.G.: An inequality in the theory of arithmetic on algebraic varieties. Proc. Camb. Philos. Soc. **45**, 502–509 (1949)
63. Odlyzko, A.M., Skinner, C.M.: Nonexistence of Siegel zeros in towers of radical extensions. In: A Tribute to Emil Grosswald: Number Theory and Related Analysis. Contemporary Mathematics, vol. 143, pp. 499–511. American Mathematical Society, Providence, RI, (1993)
64. Pierce, L.B.: The 3-part of class numbers of quadratic fields. J. Lond. Math. Soc. **71**, 579–598 (2005)
65. Pierce, L.B.: A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. Forum Math. **18**, 677–698 (2006)
66. Ruppert, W.M.: Small generators of number fields. Manuscr. Math. **96**(1), 17–22 (1998)
67. Serre, J.-P.: Linear Representations of Finite Groups. Springer, New York (1977). Trans. by Leonard L. Scott, GTM Vol. 42
68. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Publ. Math. IHES **54**, 123–201 (1982)
69. Serre, J.-P.: Lectures on the Mordell–Weil Theorem, 3rd edn. Friedr Vieweg and Sohn, Braunschweig (1997)
70. Silverman, J.H.: Lower bounds for height functions. Duke Math. J. **51**(2), 395–403 (1984)
71. Soundararajan, K.: Divisibility of class numbers of imaginary quadratic fields. J. Lond. Math. Soc. (2) **61**(3), 681–690 (2000)
72. Shankar, A., Tsimerman, J.: Counting S_5-fields with a power saving error term. Forum Math. Sigma **2**, e13 (2014)
73. Stark, H.M.: Some effective cases of the Brauer–Siegel theorem. Invent. Math. **23**, 135–152 (1974)
74. Tate, J.T.: Global class field theory. In: Algebraic Number Theory (Proceedings of an Instructional Conference, Brighton, 1965), pp. 162–203. Thompson, Washington, D.C. (1967)
75. Tschebotareff, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann. **95**(1), 191–228 (1926)
76. Tunnell, J.: Artin's conjecture for representations of octahedral type. Bull. Am. Math. Soc. (N.S.) **5**(2), 173–175 (1981)
77. Thorner, J., Zaman, A.: A Chebotarev variant of the Brun–Titchmarsh theorem and bounds for the Lang–Trotter conjectures. IMRN (2017). https://doi.org/10.1093/imrn/rnx031
78. Thorner, J., Zaman, A.: An explicit bound for the least prime ideal in the Chebotarev density theorem. Algebra Number Theory **11**, 1135–1197 (2017)
79. Vinogradov, I.M.: A new estimate of the function $\zeta(1 + it)$. Izv. Akad. Nauk SSSR. Ser. Mat. **22**, 161–164 (1958)
80. Vershik, A.M., Kerov, S.V.: Asymptotic behavior of the maximum and generic dimensions of irreducible representations of the symmetric group. Funktsional. Anal. i Prilozhen. **19**(1), 25–36, 96 (1985)
81. Vaaler, J.D., Widmer, M.: A note on generators of number fields. In: Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms. Contemporary Mathematics, vol. 587, pp. 201–211. American Mathematical Society, Providence, RI (2013)
82. Vaaler, J.D., Widmer, M.: Number fields without small generators. Math. Proc. Camb. Philos. Soc. **159**(3), 379–385 (2015)
83. Widmer, M.: Bounds for the ℓ-torsion in class groups (2017). arXiv:1709.10137
84. Wong, S.: Automorphic forms on GL(2) and the rank of class groups. J. Reine Angew. Math. **515**, 125–153 (1999)
85. Wong, S.: On the rank of ideal class groups. In: Proceedings of the Fourth Canadian Number Theory Conference, pp. 377–383 (1999)
86. Wong, S.: Densities of quartic fields with even Galois groups. Proc. Am. Math. Soc. **133**, 2873–2881 (2005)

87. Wood, M.M.: On the probabilities of local behaviors in abelian field extensions. Compos. Math. **146**(1), 102–128 (2010)
88. Wood, M.M.: Asymptotics for Number Fields and Class Groups. Springer, Berlin (2016)
89. Wright, D.: Distribution of discriminants of abelian extensions. Proc. Lond. Math. Soc. **58**, 17–50 (1989)
90. Zhang, S.-W.: Equidistribution of CM-points on quaternion Shimura varieties. Int. Math. Res. Not. **59**, 3657–3689 (2005)