

# AN APPROXIMATE FORM OF ARTIN'S HOLOMORPHY CONJECTURE AND NON-VANISHING OF ARTIN $L$ -FUNCTIONS

ROBERT J. LEMKE OLIVER, JESSE THORNER, AND ASIF ZAMAN

ABSTRACT. Let  $k$  be a number field and  $G$  be a finite group. Let  $\mathfrak{F}_k^G(Q)$  be the family of number fields  $K$  with absolute discriminant  $D_K$  at most  $Q$  such that  $K/k$  is normal with Galois group isomorphic to  $G$ . If  $G$  is the symmetric group  $S_n$  or any transitive group of prime degree, then we unconditionally prove that for all  $K \in \mathfrak{F}_k^G(Q)$  with at most  $O_\varepsilon(Q^\varepsilon)$  exceptions, the  $L$ -functions associated to the faithful Artin representations of  $\text{Gal}(K/k)$  have a region of holomorphy and non-vanishing commensurate with predictions by the Artin conjecture and the generalized Riemann hypothesis. This result is a special case of a more general theorem. As applications, we prove that:

- (1) there exist infinitely many degree  $n$   $S_n$ -fields over  $\mathbb{Q}$  whose class group is as large as the Artin conjecture and GRH imply, settling a question of Duke;
- (2) for a prime  $p$ , the periodic torus orbits attached to the ideal classes of almost all totally real degree  $p$  fields  $F$  over  $\mathbb{Q}$  equidistribute on  $\text{PGL}_p(\mathbb{Z}) \backslash \text{PGL}_p(\mathbb{R})$  with respect to Haar measure;
- (3) for each  $\ell \geq 2$ , the  $\ell$ -torsion subgroups of the ideal class groups of almost all degree  $p$  fields over  $k$  (resp. almost all degree  $n$   $S_n$ -fields over  $k$ ) are as small as GRH implies; and
- (4) an effective variant of the Chebotarev density theorem holds for almost all fields in such families.

## 1. INTRODUCTION

Let  $K/k$  be a normal extension of number fields with Galois group  $G$ . Many natural arithmetic properties of  $K$  are controlled by the Artin  $L$ -functions  $L(s, \rho)$  attached to the irreducible complex representations  $\rho$  of  $G$ . The Artin conjecture asserts that  $L(s, \rho)$  is entire for every nontrivial  $\rho$ , and the generalized Riemann hypothesis (GRH) asserts that  $L(s, \rho) \neq 0$  for  $\text{Re}(s) > \frac{1}{2}$ . Artin's conjecture is known for very few groups  $G$ , and GRH remains open. In this paper, we substantially enlarge the region of holomorphy and non-vanishing for Artin  $L$ -functions in an average sense.

We begin with work of Aramata, Artin, and Brauer towards the Artin conjecture: the quotient  $\zeta_K(s)/\zeta_k(s)$  of Dedekind zeta functions is entire, and for each Artin representation  $\rho$  of  $\text{Gal}(K/k)$ , the  $L$ -function  $L(s, \rho)$  is holomorphic and non-vanishing in any region where  $\zeta_K(s) \neq 0$ . In many applications, existing zero-free regions are not strong enough to deduce the desired results. Therefore, one might hope to average over number fields  $K$  in a family  $\mathfrak{F}$  and prove that apart from a small collection of  $K \in \mathfrak{F}$ , the ratios  $\zeta_K(s)/\zeta_k(s)$  have a large zero-free region that can be used to deduce a large region of holomorphy and non-vanishing for each  $L(s, \rho)$  associated with  $K/k$ . We fix a finite nontrivial group  $G$  and consider the family  $\mathfrak{F}_k^G$  of normal extensions  $K/k$  such that  $\text{Gal}(K/k) \cong G$ . When  $G$  is abelian, each nontrivial representation is one-dimensional and can be realized as a Hecke character whose  $L$ -function is entire, so we focus on nonabelian groups  $G$ .

Two obstacles quickly emerge. First, we do not yet know that the entire  $L$ -function  $\zeta_K(s)/\zeta_k(s)$  factors as a product of  $L$ -functions associated to cuspidal automorphic representations defined over  $k$ , as the strong Artin conjecture asserts. This hinders most methods of averaging over  $K \in \mathfrak{F}_k^G$ . The second obstacle, which we loosely term the *subfield problem*, arises from the work of Aramata, Artin, and Brauer—if  $F \subseteq K$  is a subextension of  $k$ , then a zero of  $\zeta_F(s)$  is a zero of  $\zeta_K(s)$ . Moreover, the same field  $F$  may arise as a subfield of many different  $K$  in the family  $\mathfrak{F}_k^G$ . For example, this is the case for the family of  $S_n$ -extensions of  $k$ , where different fields may share a common quadratic subfield; see (3.3) below. Consequently, any problematic zero of a single  $\zeta_F(s)$  could propagate to many different  $\zeta_K(s)$ , so our ability to study the zeros of the ratios  $\zeta_K(s)/\zeta_k(s)$  as we average over  $K \in \mathfrak{F}_k^G$  is both technically limited by one's ability to control the frequency with which fields  $K \in \mathfrak{F}_k^G$  intersect and structurally limited by the fact that such intersections do occur.

Pierce, Turnage–Butterbaugh, and Wood [44] were the first to codify the subfield problem in the context of modern arithmetic statistics by relating it to other, more understood problems. Additionally, when  $k = \mathbb{Q}$ , they use unconditional field counting results for certain nonabelian groups  $G$ , including the symmetric groups  $S_n$  for  $n \in \{3, 4, 5\}$  and the dihedral groups  $D_p$  with  $p$  an odd prime, to control the subfield problem by restricting to  $K \in \mathfrak{F}_{\mathbb{Q}}^G$  satisfying certain ramification conditions. Apart from  $G = S_5$ , the strong Artin conjecture is known for each of these groups, so the quotient  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  factors in terms of automorphic  $L$ -functions. Using a zero density estimate for automorphic  $L$ -functions due to Kowalski and Michel [32], they then proved that for almost all of the  $K \in \mathfrak{F}_{\mathbb{Q}}^G$  satisfying certain ramification conditions, the ratio  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  and each Artin  $L$ -function in the associated factorization enjoy a very wide zero-free region.

Avoiding unproven hypotheses on the automorphy of the factors of  $\zeta_K(s)$ , Thorner and Zaman [52] proved for *any* finite group  $G$  for which the subfield problem may be controlled that for almost all fields  $K \in \mathfrak{F}_{\mathbb{Q}}^G$ ,  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  has a much larger zero-free region than was known previously, commensurate with what GRH implies. This work also further clarified the subfield problem, distilling it into a question about so-called “intersection multiplicities” (see (3.2) below). As described earlier, the classical work of Aramata, Artin, and Brauer then shows that each irreducible Artin  $L$ -function must be both non-vanishing and holomorphic in this region, independent of whether it is known to be automorphic. Thus, the work in [52] avoids assumptions of automorphy, which it does by proving a new large sieve for the family  $\mathfrak{F}_{\mathbb{Q}}^G$ , but it does not address the technical and structural limitations presented by the subfield problem. In particular, their work avoids these limitations when  $G$  is simple (where the subfield problem trivially disappears) but it cannot avoid them in most other families, including the natural situation when  $G = S_n$ .

We offer a new approach to producing large regions of holomorphy and non-vanishing for Artin  $L$ -functions associated to almost all fields in a family of Galois extensions that simultaneously addresses the subfield problem and the absence of automorphy results. The novelty lies in reducing these obstacles to a group theoretic computation that is tractable for groups like  $S_n$ , but which in full generality apparently requires the complete classification of finite simple groups. Our approach has two independent components. The first component changes the averaging process in [52] in a way that avoids the subfield problem (Section 3.2). This new average, however, no longer produces a result that is amenable to the classical results of Aramata, Artin, and Brauer. The second component, therefore, is a new result in character theory that handles this complication by expressing the characters of certain Artin representations in terms of inductions of one-dimensional characters with restricted components, which neither Artin nor Brauer induction can address (Section 3.3). We view these two components together as an approximate form of Artin’s conjecture that also provides a strong zero-free region for almost all  $K \in \mathfrak{F}_k^G$  for any number field  $k$ .

Before we describe our method, we give a representative example of what our approach can prove for faithful Artin representations associated to the fields  $K \in \mathfrak{F}_k^G$ , where  $G$  is the symmetric group  $S_n$  or a transitive group of prime degree. There is little to no progress towards the Artin conjecture when the degree of  $G$  is at least 5 or towards basic counting problems in arithmetic statistics when the degree of  $G$  is at least 6. Despite these setbacks, we prove:

**Theorem 1.1.** *Let  $k$  be a number field. Let  $G$  be the symmetric group  $S_n$  for some  $n \geq 2$  or a transitive subgroup of  $S_p$  for some prime  $p$ . Let  $Q \geq 1$ . For all  $\varepsilon > 0$ , there exists an effectively computable constant  $c_1 = c_1(|G|, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all except  $O_{|G|, [k : \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  normal extensions  $K/k$  with  $\text{Gal}(K/k) \simeq G$  and absolute discriminant  $D_K$  at most  $Q$ , each irreducible faithful Artin representation  $\rho$  of  $\text{Gal}(K/k)$  satisfies*

$$\left| \sum_{N_{k/\mathbb{Q}} \mathfrak{p} \leq x} \text{tr } \rho(\text{Frob}_{\mathfrak{p}}) \right| \ll_{|G|, [k : \mathbb{Q}], \varepsilon} x \exp(-c_1 \sqrt{\log x})$$

for all  $x \geq (\log D_K)^{81|G|/\varepsilon}$ . The sum is over prime ideals of  $k$  with absolute norm at most  $x$ .

*Remark.* Under GRH, the exponent  $81|G|/\varepsilon$  may be replaced by  $2 + \varepsilon$  for all  $K$ .

*Remark.* The constant  $c_1$  is the same as in Lemma 7.4 below.

*Remark.* We use the notation  $f \ll_\nu g$  and  $f = O_\nu(g)$  to denote the existence of an effectively computable constant  $c_\nu > 0$ , depending at most on  $\nu$ , such that  $|f| \leq c_\nu |g|$  in the range indicated. We use the notation  $f \asymp_\nu g$  to indicate that  $f \ll_\nu g$  and  $g \ll_\nu f$ .

## 2. APPLICATIONS

Theorem 1.1 and the ideas leading to it produce several desirable arithmetic results. We will now sample a few of them. In Section 3, we will discuss the ideas leading to Theorem 1.1.

**2.1. The extremal order of class numbers.** Let  $\mathcal{K}_n$  be the family of totally real number fields  $F$  with  $[F : \mathbb{Q}] = n$  whose normal closure over  $\mathbb{Q}$  has the full symmetric group  $S_n$  as its Galois group. Using lower bounds on the regulator of  $F$  due to Remak [45], Duke [17] proved under GRH and the Artin conjecture that if  $F \in \mathcal{K}_n$ , then

$$|\text{Cl}(F)| \ll_n \frac{D_F^{1/2} (\log \log D_F)^{n-1}}{(\log D_F)^{n-1}},$$

where  $D_F$  is the absolute discriminant of  $F$ . Furthermore, still under the assumption of GRH and the Artin conjecture, Duke showed that this upper bound is sharp, in that

$$(2.1) \quad \text{there exist } F \in \mathcal{K}_n \text{ with } D_F \text{ arbitrarily large and } |\text{Cl}(F)| \asymp_n \frac{D_F^{1/2} (\log \log D_F)^{n-1}}{(\log D_F)^{n-1}}.$$

The conclusion (2.1) is proved without recourse to unproven hypotheses when  $n \in \{2, 3, 4\}$  [10, 12, 40]. Cho [10] proved that (2.1) holds when  $n \geq 5$  using only the strong Artin conjecture, removing the reliance of Duke's argument on GRH. We use Theorem 1.1 to prove the following unconditional result that removes the hypotheses of Artin's conjecture and GRH as well as the requirement that  $F$  be totally real.

**Theorem 2.1.** *For any fixed integers  $r_1, r_2 \geq 0$  with  $n := r_1 + 2r_2 \geq 2$ , there are number fields  $F$  of signature  $(r_1, r_2)$  with arbitrarily large discriminant  $D_F$  whose normal closure has the full symmetric group  $S_n$  as its Galois group, for which*

$$(2.2) \quad |\text{Cl}(F)| \asymp_{r_1, r_2} \frac{D_F^{1/2} (\log \log D_F)^{r_1 + 2r_2 - 1}}{(\log D_F)^{r_1 + r_2 - 1}}.$$

*Remark.* Fix  $0 < \tau < 1/(n^2 - n)$ . Our proof shows that there exists a constant  $c_2 = c_2(n, \tau) > 0$  such that if  $Q \geq c_2$ , then there are at least  $Q^\tau$  number fields  $F$  that satisfy the conclusion of Theorem 2.1. See Theorem 10.5.

**2.2. Distribution of periodic torus orbits and subconvexity.** Let  $F/\mathbb{Q}$  be a totally real field of degree  $n$  with ring of integers  $\mathcal{O}_F$ . Then  $F$  may be naturally embedded into  $\mathbb{R}^n$  by the product of its real embeddings, and in this embedding, the integers  $\mathcal{O}_F$  form a full rank lattice. More generally, a subset  $\Lambda \subseteq F$  is a lattice if it is a free  $\mathbb{Z}$ -submodule of rank  $n$ . The  $F$ -equivalence class of  $\Lambda$ , or the  $F$ -homothety class, is the set of lattices  $\Lambda' \subseteq F$  for which  $\Lambda' = \alpha\Lambda$  for some  $\alpha \in F^\times$ . If we let  $\mathcal{O} = \mathcal{O}_\Lambda := \{\alpha \in F : \alpha\Lambda \subseteq \Lambda\}$ , then  $\mathcal{O}$  is an order in  $\mathcal{O}_F$ , and two equivalent lattices have the same associated order  $\mathcal{O}$ . Moreover, there is a representative of the class of  $\Lambda$  that is an ideal  $\mathfrak{a}$  in  $\mathcal{O}$ , and the set of such ideal representatives constitute the ideal class of  $\mathfrak{a}$  in  $\mathcal{O}$ . Thus, equivalence classes of lattices in  $F$  are naturally identified with ideal classes in orders  $\mathcal{O} \subseteq \mathcal{O}_F$ .

The space of lattices in  $\mathbb{R}^n$  is naturally identified with  $\text{GL}_n(\mathbb{Z}) \backslash \text{GL}_n(\mathbb{R})$ . By considering its action via multiplication,  $F^\times$  embeds into the maximal split torus  $H_n \subseteq \text{GL}_n(\mathbb{R})$  consisting of diagonal matrices. Thus,  $F$ -equivalent lattices give rise to elements of the manifold  $\text{PGL}_n(\mathbb{Z}) \backslash \text{PGL}_n(\mathbb{R})$

equivalent under the action of  $H_n$ . By the above discussion, we may think of an ideal class in an order  $\mathcal{O} \subseteq \mathcal{O}_F$  as parametrizing a full  $H_n$ -orbit in  $\mathrm{PGL}_n(\mathbb{Z}) \backslash \mathrm{PGL}_n(\mathbb{R})$ . In a pair of papers [21, 22], Einsiedler, Lindenstrauss, Michel, and Venkatesh showed that every closed  $H_n$ -orbit on  $\mathrm{PGL}_n(\mathbb{Z}) \backslash \mathrm{PGL}_n(\mathbb{R})$  arises as a periodic torus orbit in this manner. When  $n$  is prime, they connected the equidistribution of these torus orbits as the discriminant  $\mathrm{disc}(\mathcal{O}) \rightarrow \infty$  to the problem of proving a discriminant-aspect subconvexity bound for  $\zeta_F(s)$  of the form

$$(2.3) \quad |\zeta_F(\tfrac{1}{2} + it)| \ll_{[F:\mathbb{Q}]} D_F^{\frac{1}{4}-\theta} (1 + |t|)^A,$$

where  $\theta \in (0, \frac{1}{4})$  and  $A > 0$  are constants that depend at most on  $[F : \mathbb{Q}]$ . In the case  $n = 2$ , this leads to a reinterpretation of Duke's theorem [15] on equidistribution of geodesics on the modular curve associated to real quadratic fields. When  $n = 3$ , there was enough progress toward subconvexity that Einsiedler, Lindenstrauss, Michel, and Venkatesh could prove that the analogous equidistribution result holds on  $\mathrm{PGL}_3(\mathbb{Z}) \backslash \mathrm{PGL}_3(\mathbb{R})$ .

Despite tremendous progress on proving subconvexity bounds for various families of automorphic  $L$ -functions, the bound (2.3) is only known when  $F$  is a normal extension over a fixed base field  $k$  with either an abelian or generalized dihedral Galois group, as well as the case when  $F$  is an arbitrary cubic extension of a fixed field  $k$ . In these cases, the Dedekind zeta function factors as a product of standard  $L$ -functions associated to cuspidal automorphic representations of  $\mathrm{GL}_1(\mathbb{A}_k)$  or  $\mathrm{GL}_2(\mathbb{A}_k)$ , and the bound (2.3) follows from work of Michel and Venkatesh [37] (see also [6, 8, 18]).

We produce many new number fields  $F$  that are extensions of  $k$  satisfying (2.3) even if we do not yet know whether  $\zeta_F(s)$  factors into a product of  $L$ -functions that are automorphic over  $k$ . To state our result, we introduce some notation. Let  $k$  be a number field,  $p$  be a prime,  $n \geq 2$  be an integer, and  $Q \geq 1$ . We define the families

$$(2.4) \quad \begin{aligned} \mathcal{F}_k^p &:= \{F : [F : k] = p\}, & \mathcal{F}_k^p(Q) &:= \{F \in \mathcal{F}_k^p : D_F \leq Q\} \\ \mathcal{F}_k^{n,S_n} &:= \{F : [F : k] = n, \mathrm{Gal}(\tilde{F}/k) \cong S_n\}, & \mathcal{F}_k^{n,S_n}(Q) &:= \{F \in \mathcal{F}_k^{n,S_n} : D_F \leq Q\}, \end{aligned}$$

where  $\tilde{F}$  is the Galois closure of  $F$  over  $k$ . The ideas leading to Theorem 1.1 (see Section 3.4) enable us to prove the following unconditional result.

**Theorem 2.2.** *Let  $t \in \mathbb{R}$ ,  $Q \geq 1$ , and  $k$  be a number field. Let  $p$  be prime and  $n \geq 2$ .*

(1) *Let  $\varepsilon > 0$ . For all except  $O_{p,[k:\mathbb{Q}],\varepsilon}(Q^\varepsilon)$  of the fields  $F \in \mathcal{F}_k^p(Q)$ , we have*

$$|\zeta_F(\tfrac{1}{2} + it)| \ll_{p,[k:\mathbb{Q}]} D_k^{O(\varepsilon)} D_F^{\frac{1}{4}(1 - \frac{\varepsilon}{10^{10}(p!)^2})} (1 + |t|)^{O(p[k:\mathbb{Q}])}.$$

(2) *Let  $\varepsilon > 0$ . For all except  $O_{n,[k:\mathbb{Q}],\varepsilon}(Q^\varepsilon)$  of the fields  $F \in \mathcal{F}_k^{n,S_n}(Q)$ , we have*

$$|\zeta_F(\tfrac{1}{2} + it)| \ll_{n,[k:\mathbb{Q}]} D_k^{O(\varepsilon)} D_F^{\frac{1}{4}(1 - \frac{\varepsilon}{10^{10}(n!)^2})} (1 + |t|)^{O(n[k:\mathbb{Q}])}.$$

*Remark.* Ellenberg and Venkatesh [24, Theorem 1.1] proved that there exist effectively computable constants  $c_3 = c_3(n, k) > 0$  and  $c_4 = c_4(p, k) > 0$  such that if  $Q \geq 1$ , then

$$(2.5) \quad |\mathcal{F}_k^{n,S_n}(Q)| \geq c_3 Q^{\frac{1}{2}}, \quad |\mathcal{F}_k^p(Q)| \geq c_4 Q^{\frac{1}{2}}.$$

This ensures that Theorem 2.2 is not vacuous.

Taking  $k = \mathbb{Q}$  in part 1 of Theorem 2.2, we deduce our next result.

**Theorem 2.3.** *Let  $p \geq 5$  be prime and let  $\mathcal{F}_{\mathbb{Q}}^{p,+} \subseteq \mathcal{F}_{\mathbb{Q}}^p$  be the set of totally real degree  $p$  extensions of  $\mathbb{Q}$ . For any  $\varepsilon > 0$ , there exists a set  $\mathcal{E}_\varepsilon^p \subseteq \mathcal{F}_{\mathbb{Q}}^{p,+}$  such that*

(1)  *$|\{F : F \in \mathcal{E}_\varepsilon^p \cap \mathcal{F}_{\mathbb{Q}}^{p,+}(Q)\}| \ll_{p,\varepsilon} Q^\varepsilon$  for all  $Q \geq 1$ , and*

- (2) if  $(\mathcal{O}_j)_{j=1}^\infty$  is a sequence of orders in  $\{\mathcal{O} : \text{there exists } F \in \mathcal{F}_\mathbb{Q}^{p,+} - \mathcal{E}_\varepsilon^p \text{ such that } \mathcal{O} \subseteq \mathcal{O}_F\}$  with  $\lim_{j \rightarrow \infty} \text{disc}(\mathcal{O}_j) = \infty$ , then as  $j \rightarrow \infty$ , the union of  $H_p$ -orbits associated to the ideal classes of  $\mathcal{O}_j$  described above becomes equidistributed with respect to Haar measure on  $\text{PGL}_p(\mathbb{Z}) \backslash \text{PGL}_p(\mathbb{R})$ .

In particular, if  $(F_j)_{j=1}^\infty$  is a sequence of fields in  $\mathcal{F}_\mathbb{Q}^{p,+} - \mathcal{E}_\varepsilon^p$  ordered by discriminant, then the measures  $\mu_{F_j}$  on  $\text{PGL}_p(\mathbb{Z}) \backslash \text{PGL}_p(\mathbb{R})$  associated to the  $H_p$ -orbits of the ideal classes of  $\mathcal{O}_{F_j}$  converge to Haar measure on  $\text{PGL}_p(\mathbb{Z}) \backslash \text{PGL}_p(\mathbb{R})$  in the weak-\* limit as  $j \rightarrow \infty$ .

*Remark.* It follows from minor modifications to the work of Ellenberg and Venkatesh [24] that for all primes  $p$ , there exists a constant  $c_5 = c_5(p) > 0$  such that for all  $Q \geq 1$ , we have  $|\mathcal{F}_\mathbb{Q}^{p,+}(Q)| \geq c_5 Q^{\frac{1}{2}}$ . Consequently, this result is not vacuous.

**2.3.  $\ell$ -torsion in class groups.** Let  $F/k$  be an extension of number fields, and let  $\text{Cl}(F)$  denote the class group of  $F$ . For any integer  $\ell \geq 2$  and any  $\varepsilon > 0$ , it is expected that the  $\ell$ -torsion subgroup  $\text{Cl}(F)[\ell]$  satisfies  $|\text{Cl}(F)[\ell]| \ll_{\ell, [F:\mathbb{Q}], \varepsilon} D_F^\varepsilon$  [16]. This is known only for prime  $\ell$  when the normal closure of  $F$  has a Galois group that is an  $\ell$ -group [31]. The trivial bound  $|\text{Cl}(F)[\ell]| \leq |\text{Cl}(F)| \ll_{[F:\mathbb{Q}], \varepsilon} D_F^{1/2+\varepsilon}$  follows from Minkowski's bound. Ellenberg and Venkatesh [25, Proposition 3.1] showed that GRH implies for all  $\varepsilon > 0$  the improvement

$$(2.6) \quad |\text{Cl}(F)[\ell]| \ll_{[F:\mathbb{Q}], \ell, \varepsilon} D_F^{\frac{1}{2} - \frac{1}{2\ell([F:k]-1)} + \varepsilon}.$$

The fields  $F$  for which there unconditionally exists a constant  $\delta > 0$  (depending at most on  $\ell$  and  $[F:k]$ ) such that  $|\text{Cl}(F)[\ell]| \ll_{[F:\mathbb{Q}], \ell, \varepsilon} D_F^{1/2-\delta}$  are scarce [4, 25, 29, 43, 54, 55]. The key to the  $\ell$ -torsion bounds in [25, 54, 55] is a lemma of Ellenberg and Venkatesh [25, Lemma 2.3] that exploits non-inert primes of norm at most  $D_F^{1/2\ell([F:k]-1)}$ .

The works of An [1]; Ellenberg, Pierce, and Wood [23]; Pierce, Turnage-Butterbaugh, and Wood [44]; and Thorner and Zaman [52] consider the problem of proving that (2.6) holds for  $k = \mathbb{Q}$  and all number fields  $F$  with  $D_F \leq Q$  in certain families, provided that an exceptional set of relative density zero is omitted. Each of these results uses the work of Ellenberg and Venkatesh [25, Lemma 2.3] to reduce the problem to the study of small primes that split completely in the fields under consideration. Table 1 below summarizes the current progress that makes no recourse to unproven hypotheses (with  $n \geq 2$  denoting an integer and  $p$  denoting a prime).

TABLE 1. On-average  $\ell$ -torsion results for extensions of  $\mathbb{Q}$  from [1, 23, 44, 52]

Source	Galois structure	Restrictions	Family size	Exceptional set size
[44]	degree $n$ $\mathbb{Z}/n\mathbb{Z}$ -fields	on tamely ramified primes	$\sim c_n Q^{\frac{1}{n-1}}$	$Q^\varepsilon$
[1]	degree 4 $D_4$ -fields	none	$\sim b_4 Q$	$Q^{\frac{1}{2}+\varepsilon}$
[44]	degree $p$ $D_p$ -fields, $p \geq 3$	on tamely ramified primes	$\gg_p Q^{\frac{2}{p-1}}$	$Q^{\frac{1}{p-1}+\varepsilon}$
[23]	degree 3 $S_3$ -fields	none	$\sim c_3 Q$	$Q^{1-\frac{1}{4\ell}+\varepsilon}$
[44]	degree 3 $S_3$ -fields	squarefree discriminants	$\sim d_3 Q$	$Q^{\frac{1}{3}+\varepsilon}$
[23]	degree 4 $S_4$ -fields	$\ell \geq 8$	$\sim c_4 Q$	$Q^{1-\frac{1}{6\ell}+\varepsilon}$
[44]	degree 4 $S_4$ -fields	squarefree discriminants	$\sim d_4 Q$	$Q^{\frac{1}{2}+\varepsilon}$
[23]	degree 5 $S_5$ -fields	$\ell \geq 25$	$\sim c_5 Q$	$Q^{1-\frac{1}{8\ell}+\varepsilon}$
[52]	degree $n$ $A_n$ -fields, $n \geq 5$	none	$\gg_n Q^{\frac{1}{30}}$	$Q^\varepsilon$

Using Theorem 1.1 in concert with [25, Lemma 2.3] we obtain the following result.

**Theorem 2.4.** *Let  $\ell \geq 2$  be an integer,  $k$  be a number field, and  $Q \geq 1$ . Let  $p$  be prime,  $n \geq 2$  be an integer, and the families  $\mathcal{F}_k^p(Q)$  and  $\mathcal{F}_k^{n, S_n}(Q)$  be as in (2.4).*

(1) Let  $\varepsilon > 0$  and  $\eta > 0$ . For all except  $O_{p,[k:\mathbb{Q}],\varepsilon}(Q^\varepsilon)$  fields  $F \in \mathcal{F}_k^p(Q)$ , there holds

$$|\mathrm{Cl}(F)[\ell]| \ll_{p,k,\ell,\varepsilon,\eta} D_F^{\frac{1}{2} - \frac{1}{2\ell([F:k]-1)} + \eta}.$$

(2) Let  $\varepsilon > 0$  and  $\eta > 0$ . For all except  $O_{n,[k:\mathbb{Q}],\varepsilon}(Q^\varepsilon)$  fields  $F \in \mathcal{F}_k^{n,S_n}(Q)$ , there holds

$$|\mathrm{Cl}(F)[\ell]| \ll_{n,k,\ell,\varepsilon,\eta} D_F^{\frac{1}{2} - \frac{1}{2\ell([F:k]-1)} + \eta}.$$

*Remark.* Unlike the work in [1, 23, 44, 52], Theorem 2.4 crucially relies on the fact that the lemma of Ellenberg and Venkatesh exploits non-inert primes, not just primes that split completely.

*Remark.* The lower bounds in (2.5) ensure that Theorem 2.4 is not vacuous.

Theorem 2.4 is new for degree  $p$  fields over a base field  $k \neq \mathbb{Q}$ , and it is new when  $k = \mathbb{Q}$  and  $p \geq 7$ . When  $p = 3$  or  $5$ , Theorem 2.4 greatly reduces the sizes of the exceptional sets in [23, 44]. Theorem 2.4 is new for degree  $n$   $S_n$ -fields over any given base field  $k \neq \mathbb{Q}$  when  $n \geq 4$  (see An [2] for  $n = 3$ ), and it is new when  $k = \mathbb{Q}$  for  $n \geq 6$ . When  $n \leq 5$ , Theorem 2.4 greatly reduces the sizes of the exceptional sets in [23, 44].

We also prove a mutual refinement of Theorem 2.1 and Theorem 2.4 wherein we produce an infinitude of number fields  $F$  with a given signature  $(r_1, r_2)$  whose Galois closure over  $\mathbb{Q}$  has Galois group  $S_n$  and whose class group satisfies both (2.6) for any fixed integer  $\ell \geq 2$  and (2.2). This gives the first examples of number fields of high degree whose class groups have a nontrivial upper bound on the  $\ell$ -torsion subgroup that provably does not hold for the full class group. See Theorem 10.5 below. Additionally, when we choose  $r_2 = 0$  so that such  $F$  are totally real, we can show that each of the aforementioned fields have a point of exact order  $\ell_0$  in their class group, where  $\ell_0 \geq 2$  is an arbitrary fixed integer. When  $\ell = \ell_0$ , this gives the first examples of number fields of high degree with a nontrivial upper bound on the  $\ell$ -torsion subgroup when the  $\ell$ -torsion subgroup itself is nontrivial. See Theorem 10.6 below.

**2.4. An effective Chebotarev density theorem for fibers.** Let  $x \geq 1$ . For a normal extension  $K/k$ , let  $\mathcal{C} \subseteq G \simeq \mathrm{Gal}(K/k)$  be a conjugacy class, and define

$$\pi_{\mathcal{C}}(x; K/k) := \#\{\mathfrak{p} \subseteq \mathcal{O}_k \text{ prime: } N_{k/\mathbb{Q}}\mathfrak{p} \leq x, \mathrm{Frob}_{\mathfrak{p}} \in \mathcal{C}\},$$

where  $\mathcal{O}_k$  denotes the ring of integers of  $k$ . The Chebotarev density theorem asserts that

$$(2.7) \quad \pi_{\mathcal{C}}(x; K/k) \sim \frac{|\mathcal{C}|}{|G|} \pi_k(x) \quad \text{as } x \rightarrow \infty,$$

where  $\pi_k(x)$  is the prime ideal counting function of  $k$ . When  $\zeta_K(s)$  has no Landau–Siegel zero, Thorner and Zaman [53, Corollary 1.2] proved a stronger result, namely

$$\pi_{\mathcal{C}}(x; K/k) \sim \frac{|\mathcal{C}|}{|G|} \pi_k(x) \quad \text{as } \frac{\log x}{\log([K:\mathbb{Q}]^{[K:\mathbb{Q}]} D_K)} \rightarrow \infty.$$

A similar result holds when a Landau–Siegel zero exists. This improves previous work of Lagarias and Odlyzko [33] and V. K. Murty [42].

Let  $n \geq 5$  be an integer, let  $G$  be the full symmetric group  $S_n$ , and define

$$\mathfrak{F}_k^{S_n}(Q) := \{K: K/k \text{ is normal, } \mathrm{Gal}(K/k) \cong S_n, D_K \leq Q\}.$$

Using Theorem 1.1, we obtain an effective variant of the Chebotarev density theorem that holds in a much wider range for almost all  $K \in \mathfrak{F}_k^{S_n}(Q)$ . However, since Theorem 1.1 imposes the restriction that the representations  $\rho$  be *faithful*, we do not obtain an equidistribution result in the sense of (2.7). Instead, we show that as  $\mathfrak{p}$  varies, the conjugacy class of  $\mathrm{Frob}_{\mathfrak{p}}$  is equidistributed in each fiber of the projection  $S_n \rightarrow S_n/A_n$ .

**Theorem 2.5.** *Let  $n \geq 5$  be an integer and  $k$  be a number field. Let  $\mathcal{C} \subseteq S_n$  be a conjugacy class. Given  $K \in \mathfrak{F}_k^{S_n}(Q)$ , let  $k(\sqrt{\Delta_K})/k$  be the unique quadratic extension contained in  $K/k$ . Let  $Q \geq 1$ . For all  $\varepsilon > 0$ , there exists a constant  $c_1 = c_1(|S_n|, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all except  $O_{n, [k : \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  fields  $K \in \mathfrak{F}_k^{S_n}(Q)$ , one has that for any  $x \geq (\log D_K)^{81n!/\varepsilon}$ , there holds*

$$\pi_{\mathcal{C}}(x; K/k) = \frac{2|\mathcal{C}|}{n!} \pi_{\text{sgn}(\mathcal{C})}(x; k(\sqrt{\Delta_K})/k) + O_{n, [k : \mathbb{Q}], \varepsilon}(x \exp(-c_1 \sqrt{\log x})).$$

We highlight two immediate corollaries of Theorem 2.5. First, the Chebotarev density theorem implies that  $\pi_{\text{sgn}(\mathcal{C})}(x; k(\sqrt{\Delta_K})/k) \sim \frac{1}{2} \pi_k(x)$ , so Theorem 2.5 is consistent with (2.7). Indeed, by fixing the quadratic subfield  $k(\sqrt{\Delta_K})$ , we find the following.

**Corollary 2.6.** *Let  $n \geq 5$  be an integer,  $k$  be a number field, and  $\Delta \in k$  be a non-square element. Let  $\varepsilon > 0$  and  $Q \geq 1$ . For all except  $O_{n, [k : \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  of the fields  $K \in \mathfrak{F}_k^{S_n}(Q)$  whose quadratic subfield is  $k(\sqrt{\Delta})$ , there holds for any  $x \geq (\log D_K)^{81n!/\varepsilon}$ ,*

$$\pi_{\mathcal{C}}(x; K/k) = \frac{|\mathcal{C}|}{n!} \text{Li}(x) + O_{n, k, \Delta, \varepsilon}(x \exp(-c_1 \sqrt{\log x})).$$

*Remark.* For all non-square  $\Delta \in k$  and all integers  $n \geq 5$ , it follows from [34, Theorem 1.3] that there exist effectively computable constants  $c_6 = c_6(n, k, \Delta) > 0$  and  $c_7 = c_7(n) > 0$  such that the number of  $K \in \mathfrak{F}_k^{S_n}(Q)$  that contain the quadratic subfield  $k(\Delta)/k$  is at least  $c_6 Q^{c_7}$ . This ensures that Corollary 2.6 is not vacuous.

In the full family  $\mathfrak{F}_k^{S_n}(Q)$ , where the quadratic resolvent is not assumed fixed, Theorem 2.5 does not directly permit access to primes whose Frobenius element lies in a single conjugacy class  $\mathcal{C}$ . However, in many applications of effective Chebotarev density theorems (e.g., to bounding  $\ell$ -torsion subgroups of the class group), it is desirable to produce primes whose Frobenius element lies in one of several conjugacy classes. Theorem 2.5 provides access to such primes, provided that not all of the desired classes have the same sign. As a particularly simple instance of this, we have:

**Corollary 2.7.** *Let  $n \geq 5$  be an integer and  $k$  be a number field. Let  $\mathcal{C}, \mathcal{C}' \subseteq S_n$  be conjugacy classes of opposite parity. Let  $Q \geq 1$  and  $\varepsilon > 0$ . For all except  $O_{n, [k : \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  fields  $K \in \mathfrak{F}_k^{S_n}(Q)$ , one has that for any  $x \geq (\log D_K)^{81n!/\varepsilon}$ , there holds*

$$\frac{n!}{|\mathcal{C}|} \pi_{\mathcal{C}}(x; K/k) + \frac{n!}{|\mathcal{C}'|} \pi_{\mathcal{C}'}(x; K/k) = 2\pi_k(x) + O_{n, [k : \mathbb{Q}], \varepsilon}(x \exp(-c_1 \sqrt{\log x})).$$

Finally, we note that while we have stated Theorem 2.5 for the family of  $S_n$  extensions, an analogous result will hold for the family of fields  $K$  whose Galois group  $G$  is a given transitive group of prime degree. Such groups have a unique minimal normal subgroup  $N$ , and the role of the quadratic subfield  $k(\sqrt{\Delta_K})$  will instead be played by the subfield of  $K$  fixed by  $N$ . An analogue of Corollary 2.7 will hold for any set of conjugacy classes that surjects onto the set of conjugacy classes of the quotient  $G/N$ .

## ORGANIZATION

In Section 3, we state and give context for our main technical results (Theorems 3.1, 3.3 and 3.7 and Corollary 3.8) after summarizing the work in [44, 52].

In Section 4, we recall the definition and basic properties of Artin  $L$ -functions.

In Section 5, we prove Theorem 3.3, which ensures that a zero-free region for the quotient  $\zeta_K(s)/\zeta_{K^N}(s)$  “transfers” to Artin  $L$ -functions not coming from  $K^N$ .

Section 6 and 7 contain the main analytic results of this paper, including the proofs of Theorems 3.1 and 3.7.

In Section 8, we discuss how our results apply to the family of degree  $p$  extensions, regardless of Galois structure.

In Section 9, we prove the fibered Chebotarev density theorem in Theorem 3.10.

In Section 10, we prove the applications to class groups in Theorems 2.1 and 2.4.

In Section 11, we prove the applications to subconvexity and the equidistribution of periodic torus orbits in Theorems 2.2 and 2.3.

In Section 12, we give heuristics for a key quantity called the intersection multiplicity introduced below and use this discussion to contrast our results with those of [44] and [52].

#### ACKNOWLEDGEMENTS

The authors would like to thank William Duke, John Friedlander, Boris Hasselblatt, Peter Humphries, George McNinch, Philippe Michel, Ken Ono, David Rohrlich, Kannan Soundararajan, Frank Thorne, Akshay Venkatesh, and Jiuya Wang for helpful conversations. RJLO was partially supported by NSF grant DMS-1601398.

### 3. MAIN RESULTS: HOLOMORPHY AND NON-VANISHING OF ARTIN $L$ -FUNCTIONS

We now describe the ideas leading to Theorem 1.1. As above, let  $k$  be a number field and let  $G$  be a finite group. We let  $\mathfrak{F}_k^G$  denote the family of number fields  $K$  inside a fixed choice of the algebraic closure  $\bar{k}$  that are normal extensions of  $k$  with Galois group  $\text{Gal}(K/k)$  isomorphic to  $G$ . For any  $Q \geq 1$ , let

$$\mathfrak{F}_k^G(Q) := \{K \in \mathfrak{F}_k^G : D_K \leq Q\},$$

where  $D_K$  denotes the absolute discriminant of  $K$  over  $\mathbb{Q}$ .

**3.1. Summary of preceding work.** It is instructive to briefly review the ideas in [44, 52]. Let  $k = \mathbb{Q}$ . The approach of Pierce, Turnage-Butterbaugh, and Wood in [44] relied on the zero density estimate for  $L$ -functions of families of cuspidal automorphic representations proved by Kowalski and Michel [32]. Assuming the strong Artin conjecture, the  $L$ -function  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  associated to each  $K \in \mathfrak{F}_{\mathbb{Q}}^G$  is the  $L$ -function associated to an isobaric *non-cuspidal* automorphic representation  $\Pi_K$  defined over  $\mathbb{Q}$ . Note that if  $K_1, K_2 \in \mathfrak{F}_{\mathbb{Q}}^G(Q)$  are distinct, then  $\Pi_{K_1}$  and  $\Pi_{K_2}$  might have some cuspidal constituents in common (as would happen if  $K_1$  and  $K_2$  share a common subfield), in which case there exists a cuspidal automorphic representation  $\pi_0$  such that  $L(s, \Pi_{K_1})/L(s, \pi_0)$  and  $L(s, \Pi_{K_2})/L(s, \pi_0)$  are entire. If one studies the zeros of the  $L$ -functions  $L(s, \Pi_K)$  with  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q)$  and many of the  $L(s, \Pi_K)$  share a particular common factor  $L(s, \pi_0)$ , then the zeros of  $L(s, \pi_0)$  are counted with high multiplicity. If this multiplicity is too high, then the zero density estimate is rendered trivial.

Let  $\mathcal{R}_G$  denote a particular condition on the primes that tamely ramify in a normal extension  $K/\mathbb{Q}$  with  $\text{Gal}(K/\mathbb{Q}) \cong G$ , and let  $\mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)$  be the subset of  $\mathfrak{F}_{\mathbb{Q}}^G(Q)$  whose fields satisfy  $\mathcal{R}_G$ . For certain groups  $G$ , Pierce, Turnage-Butterbaugh, and Wood find conditions  $\mathcal{R}_G$  that enable them to relate the distribution of fields  $K_1, K_2 \in \mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)$  such that  $\Pi_{K_1}$  and  $\Pi_{K_2}$  share some cuspidal constituents to the arithmetic-statistical problem of counting number fields  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)$  that share a given discriminant. In the situations where their approach works (see Section 6.3 and Theorems 3.1 and 3.3 in [44]), they prove that if one assumes the strong Artin conjecture for  $G$ , then for all  $\varepsilon > 0$  and all  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)$  with at most

$$O_{|G|, \varepsilon}(Q^\varepsilon \max_{D \leq Q} |\{K \in \mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G) : D_K = D\}|)$$

exceptions, the ratio  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  (and all of the Artin  $L$ -functions in its factorization, which are assumed to be automorphic, hence entire) is nonvanishing in the region

$$\text{Re}(s) \geq 1 - \varepsilon, \quad |\text{Im}(s)| \leq (\log D_K)^{2/\varepsilon}.$$



A “discriminant multiplicity conjecture” of Duke [16] implies that

$$(3.1) \quad \max_{D \leq Q} |\{K \in \mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G) : D_K = D\}| \ll_{G, \varepsilon} Q^\varepsilon.$$

Since the strong Artin conjecture is assumed in [44], this would imply that for all except  $O_{|G|, \varepsilon}(Q^\varepsilon)$  of the  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)$ , the  $L$ -functions of the Artin representations attached to  $\text{Gal}(K/\mathbb{Q})$  have a strong zero-free region for the low-lying zeros, provided that there exists a constant  $\tau = \tau(G) > 0$  such that  $|\mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)| \gg_{|G|} Q^\tau$ . Much of the work in [44] centers around making progress towards (3.1) for groups  $G$  for which the strong Artin conjecture holds and for which  $|\mathfrak{F}_{\mathbb{Q}}^G(Q, \mathcal{R}_G)| \gg_{|G|} Q^\tau$  with  $\tau$  suitably large, including cyclic groups, dihedral groups of order  $2p$  for odd primes  $p$ ,  $S_3$ , and  $S_4$ .

Note, however, that if the ramification restriction  $\mathcal{R}_G$  is non-empty then the results of Pierce, Turnage-Butterbaugh, and Wood do not quantify the number of exceptional fields in the full family  $\mathfrak{F}_{\mathbb{Q}}^G(Q)$ , even assuming the full force of Duke’s discriminant multiplicity conjecture (3.1) and the strong Artin conjecture. See Section 12 for a discussion of the limitations.

Let  $\rho_K$  be the Artin representation of  $\text{Gal}(K/\mathbb{Q})$  such that  $L(s, \rho_K) = \zeta_K(s)/\zeta_{\mathbb{Q}}(s)$ . The approach of Thorner and Zaman [52] removes the need to assume the strong Artin conjecture by proving the first unconditional large sieve for the Artin representations  $\rho_K$  as  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q)$  varies. They used character theory for the tensor products  $\rho_{K_1} \otimes \rho_{K_2}$  and Galois theory in lieu of automorphy. In the process, they simplified the arithmetic-statistical problem that one must solve to address the subfield problem. Defining the “intersection multiplicity”

$$(3.2) \quad \mathfrak{m}_k^G(Q) := \max_{K_1 \in \mathfrak{F}_k^G(Q)} |\{K_2 \in \mathfrak{F}_k^G(Q) : K_1 \cap K_2 \neq k\}|,$$

they unconditionally proved that for all  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q)$  with at most  $O_{G, \varepsilon}(\mathfrak{m}_{\mathbb{Q}}^G(Q)Q^\varepsilon)$  exceptions, the ratio  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  is nonvanishing in a region containing the box

$$1 - \frac{\varepsilon}{10^8 |G|^3} \leq \text{Re}(s) \leq 1, \quad |\text{Im}(s)| \leq D_K^{1000}.$$

This result is nontrivial if there exists a constant  $\delta > 0$  such that

$$\mathfrak{m}_{\mathbb{Q}}^G(Q) \ll_{G, \delta} Q^{-\delta} |\mathfrak{F}_{\mathbb{Q}}^G(Q)|.$$

Since two normal extensions meet in a normal extension, if  $G$  is simple, then  $\mathfrak{m}_{\mathbb{Q}}^G(Q) = 1$ . Otherwise, the best bounds on  $\mathfrak{m}_{\mathbb{Q}}^G(Q)$  follow from progress toward (3.1) and typically also require restrictions  $\mathcal{R}_G$  on ramification. Therefore, the need for the strong Artin conjecture is removed, but the subfield problem still remains unaddressed apart from a handful of special cases. If a suitable bound for  $\mathfrak{m}_{\mathbb{Q}}^G(Q)$  is known, then for all  $K \in \mathfrak{F}_{\mathbb{Q}}^G(Q)$  with few exceptions, the large zero-free region of  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$  will translate to a large region of holomorphy and non-vanishing for all of  $L$ -functions associated to the nontrivial Artin representations of  $\text{Gal}(K/\mathbb{Q})$ . This last step crucially uses Artin induction to express  $L(s, \rho)$  in terms of  $L$ -functions of one-dimensional representations of cyclic subgroups of  $G$ , each of which inherits the zero-free region of  $\zeta_K(s)/\zeta_{\mathbb{Q}}(s)$ .

For an arbitrary group  $G$ , and in particular those for which Malle’s conjecture is not known, it seems quite difficult to prove that there exists a constant  $\delta = \delta(|G|, k) > 0$  such that  $\mathfrak{m}_k^G(Q) \ll_{|G|, k} Q^{-\delta} |\mathfrak{F}_k^G(Q)|$ , regardless of whether  $k = \mathbb{Q}$ . (Recall that Malle’s conjecture predicts an asymptotic formula for the growth of  $|\mathfrak{F}_k^G(Q)|$  as  $Q \rightarrow \infty$ , and this is known only in few cases.) This is the technical limitation that we discussed in Section 1.

If  $G$  is simple, then this issue disappears as  $\mathfrak{m}_k^G(Q) = 1$ , but if  $G$  is not simple, then one should expect  $\mathfrak{m}_k^G(Q) \gg_{G, k} Q^c$  for some constant  $c$  depending on  $G$  (see Conjecture 12.1 below). This is the structural limitation discussed in Section 1. For example, for the family  $\mathfrak{F}_k^{S_n}(Q)$ , it follows from

[34, Theorem 1.3] that

$$(3.3) \quad \mathfrak{m}_k^{S_n}(Q) \gg_{n,k} Q^{\left(\frac{1}{8} - \frac{27}{32n}\right)\frac{1}{n!}}.$$

In fact, it follows from Conjecture 12.1 below that we should expect that for all  $\varepsilon > 0$ , we have  $\mathfrak{m}_k^{S_n}(Q) \gg_{k,n,\varepsilon} Q^{-\varepsilon} |\mathfrak{F}_k^{S_n}(Q)|$ . Thus, the desired bound  $\mathfrak{m}_k^G(Q) \ll_{G,k,\varepsilon} Q^{-\delta} |\mathfrak{F}_k^G(Q)|$  is not expected to hold when  $G = S_n$ , nor is it expected to hold in many other natural situations.

**3.2. Changing the average.** As we mentioned earlier, our new approach that circumvents the technical and structural limitations of the approach in [52] has two independent components. To describe them, let  $N \trianglelefteq G$  be a nontrivial normal subgroup and, for any  $K \in \mathfrak{F}_k^G$ , let  $K^N$  denote the subfield of  $K$  fixed by  $N$  under the given isomorphism  $\text{Gal}(K/k) \simeq G$ . Note that  $N = G$  is permissible, in which case  $K^N = k$ . In our current setting, we no longer require our base field  $k$  to equal  $\mathbb{Q}$ .

The first component of our new method is to study the  $L$ -function  $\zeta_K(s)/\zeta_{K^N}(s)$  as  $K \in \mathfrak{F}_k^G(Q)$  varies instead of the  $L$ -functions  $\zeta_K(s)/\zeta_k(s)$ . The quotient  $\zeta_K(s)/\zeta_{K^N}(s)$  is entire by the Artin–Brauer theorem. With suitable modifications to the ideas in [52], the work of Brauer in [7] and Galois theory will once again alleviate the need for unproven analytic hypotheses such as the Artin conjecture. The crux of our new average is that we trade the intersection multiplicity  $\mathfrak{m}_k^G(Q)$  in (3.2) that arises in [52] for a new multiplicity, namely

$$(3.4) \quad \mathfrak{m}_k^{G,N}(Q) := \max_{K_1 \in \mathfrak{F}_k^G(Q)} |\{K_2 \in \mathfrak{F}_k^G(Q) : K_1 \cap K_2 \neq K_1^N \cap K_2^N\}|.$$

The first component of our new approach is summarized in the following theorem.

**Theorem 3.1.** *Let  $Q \geq 1$ . Let  $G$  be a finite group,  $N \trianglelefteq G$  be a nontrivial normal subgroup, and  $k$  be a number field. Let  $\mathfrak{m}_k^{G,N}(Q)$  be as in (3.4). There exists an absolute and effectively computable constant  $c_8 > 0$  such that for all  $\varepsilon > 0$  and all number fields  $K \in \mathfrak{F}_k^G(Q)$  with  $O_{|G|,[k:\mathbb{Q}],\varepsilon}(\mathfrak{m}_k^{G,N}(Q)Q^\varepsilon)$  exceptions, the quotient  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in the region  $\Omega_K(\varepsilon)$  defined by*

$$(3.5) \quad 1 - \text{Re}(s) \leq \begin{cases} \frac{\varepsilon}{10|G|} \frac{\log D_K}{\log D_K + [k:\mathbb{Q}] \log(3 + |\text{Im}(s)|)} & \text{if } |\text{Im}(s)| \leq \exp(D_K^{\varepsilon/(6C_G[k:\mathbb{Q}])}), \\ \frac{c_8}{\log D_K + |G|[k:\mathbb{Q}] \log(3 + |\text{Im}(s)|)} & \text{if } |\text{Im}(s)| > \exp(D_K^{\varepsilon/(6C_G[k:\mathbb{Q}])}). \end{cases}$$

The constant  $C_G$ , which depends at most on  $|G|$ , is the same as in Theorem 6.1 below.

*Remark.* It follows from work of Lagarias and Odlyzko [33, Section 8] that  $\zeta_K(s)/\zeta_{K^N}(s)$  does not vanish in the region

$$(3.6) \quad 1 - \text{Re}(s) \leq \frac{c_8}{\log D_K + |G|[k:\mathbb{Q}] \log(3 + |\text{Im}(s)|)}$$

apart from at most one exceptional zero of  $\zeta_K(s)$ , which (if it exists) is necessarily real and simple. By comparison, the zero-free region  $\Omega_K(\varepsilon)$  defined by (3.5) contains the box

$$1 - \frac{\varepsilon}{20|G|} \leq \text{Re}(s) \leq 1, \quad |\text{Im}(s)| \leq D_K^{1000/[k:\mathbb{Q}]}$$

when  $D_K$  is sufficiently large with respect to  $\varepsilon$  and  $|G|$ . Thus, the zero-free region  $\Omega_K(\varepsilon)$  constitutes a substantial improvement over (3.6), and it applies for the vast majority of  $K \in \mathfrak{F}_k^G(Q)$  when we can prove that  $\mathfrak{m}_k^{G,N}(Q)$  is small.

Note that  $\mathfrak{m}_k^{G,G}(Q) = \mathfrak{m}_k^G(Q)$ . Therefore, our new results subsume all of the work in [52]. The novelty of Theorem 3.1 is that when  $N \neq G$ , the quantity  $\mathfrak{m}_k^{G,N}(Q)$  can often be controlled independently of one’s ability to estimate the size of the family  $\mathfrak{F}_k^G(Q)$ . Notably, if  $G$  has a *unique*

minimal nontrivial normal subgroup  $N$ , then  $m_k^{G,N}(Q) = 1$  for all  $Q \geq 1$ . This is the case for many groups of interest, including:

- all transitive permutation groups of prime degree, including the dihedral groups  $D_p$ ;
- the affine linear group  $\text{AGL}_d(\mathbb{F}_p)$  for any integer  $d \geq 1$  and any prime  $p$ ;
- the full symmetric group  $S_n$  for any  $n \geq 2$ ; and
- the non-simple alternating group  $A_4$ .

In fact, generalizing these examples, any primitive permutation group has at most 2 minimal normal subgroups [14, Theorem 4.3B]. The determination of which of these has a unique minimal normal is a consequence of the O’Nan–Scott theorem [14, Theorem 4.1A]. As a consequence of this, for example, if  $n$  is not equal to  $|T|^k$  for some nonabelian simple group  $T$  and integer  $k \geq 1$ , then every primitive group of degree  $n$  has a unique minimal normal subgroup. Many imprimitive groups have unique minimal normal subgroups as well, corresponding to subgroups stabilizing the nontrivial blocks, but these are not our main focus.

**3.3. Character theory with restricted components.** Let  $K \in \mathfrak{F}_k^G$ . Suppose that  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in some region  $\Omega \subseteq \mathbb{C}$ , e.g., the region  $\Omega_K(\varepsilon)$  in Theorem 3.1. In light of the factorization

$$(3.7) \quad \frac{\zeta_K(s)}{\zeta_{K^N}(s)} = \prod_{\substack{\rho \in \text{Irr}(G) \\ \ker \rho \not\supseteq N}} L(s, \rho)^{\dim \rho},$$

it is reasonable to hope that the zero-free region  $\Omega$  extends to each of the irreducible Artin  $L$ -functions  $L(s, \rho)$  whose associated representation has kernel not containing  $N$ . However, since it is not known that the  $L$ -functions  $L(s, \rho)$  appearing in this factorization are holomorphic, this does not immediately follow, nor does it follow in general from any existing result on Artin  $L$ -functions. The second component of our approach, therefore, is a new conjecture in the character theory of finite groups that would accommodate such a transfer of zero-free regions. We prove this conjecture in many cases of interest (including for the symmetric group and groups of prime degree), and we provide a reduction that suggests a general attack based on the classification of finite simple groups.

To describe this conjecture, we begin by recalling classical work of Artin. In particular, for each representation  $\rho$  of a finite group  $G$ , none of whose irreducible constituents is trivial, Artin showed that there are rational constants  $c_{\rho, \chi}$  such that

$$(3.8) \quad \text{tr } \rho = \sum_H \sum_{\substack{\chi \in \text{Irr}(H) \\ \dim \chi = 1}} c_{\rho, \chi} \text{Ind}_H^G \chi,$$

where the summation over  $H$  runs over the cyclic subgroups of  $G$ . This leads to a corresponding factorization of the Artin  $L$ -function in terms of Hecke  $L$ -functions,

$$(3.9) \quad L(s, \rho) = \prod_H \prod_{\substack{\chi \in \text{Irr}(H) \\ \dim \chi = 1}} L(s, \chi)^{c_{\rho, \chi}},$$

from which Artin deduced that some integral power of  $L(s, \rho)$  possesses meromorphic continuation to all of  $\mathbb{C}$ . This work was later extended by Brauer to show that each  $L(s, \rho)$  itself is meromorphic by using a different class of subgroups (namely, so called “elementary” subgroups) but the decomposition of  $L(s, \rho)$  into Hecke  $L$ -functions, or equivalently of  $\text{tr } \rho$  into the induction of 1-dimensional characters, remains essentially the only general way of inferring analytic properties of Artin  $L$ -functions outside the region of absolute convergence.

To infer consequences toward non-vanishing, we note that in the factorization of the quotient  $\zeta_K(s)/\zeta_k(s)$  in (3.9), every  $L(s, \chi)$  associated to a cyclic subgroup can be taken to appear with a positive exponent. It follows that if  $\zeta_K(s)/\zeta_k(s)$  is non-vanishing in a region  $\Omega$ , then every  $L(s, \chi)$

is non-vanishing in  $\Omega$  as well. Consequently, every  $L(s, \rho)$  is both holomorphic and non-vanishing in  $\Omega$  by means of the factorization (3.9). For our purposes, however, we wish to assume only that  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in some region, and infer the holomorphy and non-vanishing of every irreducible Artin  $L$ -function  $L(s, \rho)$  whose kernel does not contain  $N$ . From (3.9), this only follows for those irreducible representations that are induced from  $N$ , which is typically a small subset of the irreducible representations at hand.

We propose the following hypothesis on the finite group  $G$  and normal subgroup  $N \trianglelefteq G$ .

**Hypothesis T( $G, N$ ).** *If  $\rho$  is an irreducible representation of  $G$  such that  $N \not\subseteq \ker \rho$ , then for each subgroup  $H \subseteq G$  and each one-dimensional character  $\chi$  of  $H$  for which  $H \cap N \not\subseteq \ker \chi$ , there exists  $c_{\rho, \chi} \in \mathbb{Q}$  such that*

$$\mathrm{tr} \rho = \sum_{H \subseteq G} \sum_{\substack{\chi \in \mathrm{Irr}(H) \\ \dim \chi = 1 \\ H \cap N \not\subseteq \ker \chi}} c_{\rho, \chi} \mathrm{Ind}_H^G \chi.$$

**Conjecture 3.2.** *For all finite groups  $G$  and normal subgroups  $N \trianglelefteq G$ , Hypothesis T( $G, N$ ) holds.*

Two remarks are in order. First, Conjecture 3.2 lies much deeper than (3.8), the proof of which is almost immediate from a modern perspective. In particular, Conjecture 3.2 is not amenable to standard techniques exploiting the adjointness of the induction and restriction maps. For this reason, it appears to be much more group theoretic in nature than (3.8). Additionally, the analogue of Conjecture 3.2 does not hold if the subgroups  $H$  are required to be cyclic or even abelian. For this reason, a wider set of subgroups is required, analogous to how Brauer enlarged the set of subgroups to obtain a version of (3.8) with integral coefficients. We note that most, or perhaps all, proofs of Brauer induction rely on the module structure of the character ring of  $G$  and proceed by finding a representation of the trivial character in terms of inductions of characters from elementary subgroups. However, such an approach cannot work for Conjecture 3.2—there is less inherent module structure at play and the trivial character is not in the subspace under consideration.

Second, the 1-dimensional characters appearing in Conjecture 3.2, namely those  $\chi$  such that  $\ker \chi \not\supseteq H \cap N$ , are precisely those whose induction to  $G$  may be decomposed solely in terms of the characters of irreducible representations  $\rho$  of  $G$  whose kernel does not contain  $N$ . Thus, this is the largest set of 1-dimensional characters to which a zero-free region of  $\zeta_K(s)/\zeta_{K^N}(s)$  might plausibly transfer. Indeed, we show in Lemma 5.5 that such a transfer always occurs; thus, the importance of Conjecture 3.2 is made clear by the following result.

**Theorem 3.3.** *Let  $G$  be a finite group,  $N \trianglelefteq G$  be a nontrivial normal subgroup for which Hypothesis T( $G, N$ ) holds, and  $k$  be a number field. For any  $K \in \mathfrak{F}_k^G$ , if  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-zero in a region  $\Omega \subseteq \mathbb{C}$ , then for each irreducible Artin representation  $\rho$  of  $\mathrm{Gal}(K/k)$  whose kernel does not contain  $N$ , the Artin  $L$ -function  $L(s, \rho)$  is holomorphic and non-vanishing on  $\Omega$ .*

*Remark.* It is worthwhile to compare Theorem 3.3 with a well known theorem of Stark [51, Theorem 3]. Let  $K/k$  be a normal extension of number fields. Stark shows that if  $\zeta_K(s)$  has a simple zero, then this zero must be inherited from the Dedekind zeta function of a cyclic extension of  $k$ , and that it is not a zero or pole of any Artin  $L$ -function that does not factor through this cyclic extension. (If this simple zero is also real, then the cyclic extension must in fact be at most a quadratic extension. This is how Stark’s theorem is most commonly invoked.) Since cyclic extensions of  $k$  contained in  $K$  correspond to normal subgroups  $N$  for which  $G/N$  is cyclic, Stark’s theorem may be interpreted as showing that simple zeros of  $\zeta_K(s)$  are constrained to arise from zeros of Dedekind zeta functions  $\zeta_{K^N}(s)$  for cyclic extensions  $K^N/k$ , and that these zeros do not propagate to Artin  $L$ -functions attached to representations whose kernel does not contain  $N$ . By contrast, a simple consequence of Theorem 3.3 is that if  $s_0$  is a zero of  $\zeta_K(s)$  of any order that is “explained” by  $\zeta_{K^N}(s)$  in the sense that  $\zeta_K(s)/\zeta_{K^N}(s)$  is analytic and non-vanishing at  $s_0$ , then this zero does not propagate, i.e. every Artin  $L$ -function that does not factor through  $K^N$  must be analytic and non-vanishing at  $s_0$ .

We now record our progress toward Conjecture 3.2.

**Theorem 3.4.** *Let  $G$  be a finite group and let  $N \trianglelefteq G$  be a nontrivial normal subgroup. Then Hypothesis  $\mathsf{T}(G, N)$  holds if the index  $[G : N]$  is a prime power or if  $N$  is solvable (and thus also if  $G$  is solvable). Additionally, it holds if the order of  $G$  is at most 2000 or if  $G$  is a transitive permutation group of degree at most 31.*

*Proof.* When  $N$  is solvable or the index  $[G : N]$  is a prime power, this follows from Theorem 5.6 below. The remaining claims follow from a computation in `Magma`.  $\square$

The following corollary to Theorem 3.4 is crucial for the applications in Section 2.

**Corollary 3.5.** *Let  $n \geq 2$  be an integer and  $p$  be prime. Then Hypothesis  $\mathsf{T}(G, N)$  holds when  $G$  is the symmetric group  $S_n$  or a transitive group of degree  $p$ , and  $N$  is any normal subgroup of  $G$ .*

*Proof.* If  $n \neq 4$ , the only nontrivial normal subgroups of  $S_n$  are  $S_n$  itself and the alternating group  $A_n$ . Both of these have prime power index. If  $n = 4$ , there is also the Klein four subgroup, which is abelian (hence solvable). If  $p$  is prime, then the transitive groups of degree  $p$  have been classified; see Lemma 8.2 below. It follows from this classification that either  $G$  is solvable or the unique minimal normal subgroup of  $G$  has prime power index, in which case every nontrivial normal subgroup will also have prime power index.  $\square$

Finally, we have succeeded in reducing the general conjecture, Conjecture 3.2, to the case that  $N$  is a minimal normal subgroup and  $G \subseteq \text{Aut}(N)$ . Exploiting the characterization of minimal normal subgroups, along with the techniques used in Theorem 3.4, gives the following.

**Theorem 3.6.** *Let  $T$  be a nonabelian simple group and let  $p$  be a prime. If Hypothesis  $\mathsf{T}(G, N)$  holds for all groups  $G \subseteq \text{Aut}(T) \wr C_p$  containing  $N = T^p$  for which the quotient  $G/N$  is cyclic, then it holds for all finite groups.*

**3.4. Holomorphy and non-vanishing.** Our main result follows from the combination of Theorems 3.1 and 3.3. In what follows, we define  $\chi_\rho(\mathfrak{p}) := \text{tr } \rho(\text{Frob}_\mathfrak{p})$ .

**Theorem 3.7.** *Let  $G$  be a finite group, and let  $N \trianglelefteq G$  be a nontrivial normal subgroup such that Hypothesis  $\mathsf{T}(G, N)$  holds. Let  $Q \geq 1$ , let  $k$  be a number field, and recall  $\mathfrak{m}_k^{G, N}(Q)$  is defined by (3.4). For all  $\varepsilon > 0$ , there exists an effectively computable constant  $c_1 = c_1(|G|, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all  $K \in \mathfrak{F}_k^G(Q)$  apart from at most  $O_{|G|, [k : \mathbb{Q}], \varepsilon}(\mathfrak{m}_k^{G, N}(Q)Q^\varepsilon)$  exceptions, the following properties hold for the Artin representations  $\rho$  of  $\text{Gal}(K/k)$  whose kernel does not contain  $N$ :*

- (1)  $L(s, \rho)$  is holomorphic and non-vanishing in the region  $\Omega_K(\varepsilon)$  defined by (3.5), and
- (2) if  $x \geq (\log D_K)^{81|G|/\varepsilon}$ , then

$$(3.10) \quad \left| \sum_{N_k/\mathbb{Q} \mathfrak{p} \leq x} \chi_\rho(\mathfrak{p}) \right| \ll_{|G|, [k : \mathbb{Q}], \varepsilon} x \exp(-c_1 \sqrt{\log x}).$$

If  $N$  is the unique minimal nontrivial normal subgroup of  $G$ , then  $\mathfrak{m}_k^{G, N}(Q) = 1$ .

*Remark.* One of the primary benefits of a strong zero-free region for an  $L$ -function is that one can typically prove a correspondingly strong analogue of the prime number theorem, provided that one can suitably bound the logarithmic derivative. This is usually done by exploiting the full analytic continuation of the  $L$ -function, but this is not something afforded by Theorem 3.3. However, using the central ideas of its proof, we are still able to prove the strong effective prime number theorem (3.10) for the  $L(s, \rho)$  considered in Theorem 3.3. This is why we list the region of holomorphy and non-vanishing separately from the effective prime number theorem in Theorem 3.7.

*Proof of Theorem 1.1.* Let  $G$  be  $S_n$  for some integer  $n \geq 2$  or a transitive subgroup of  $S_p$  for some prime  $p$ . By Corollary 3.5,  $G$  satisfies Conjecture 3.2. By Lemma 8.1,  $G$  has a unique nontrivial minimal normal subgroup, say  $N(G)$ . Since  $N(G)$  is nontrivial, it cannot be contained in the kernel of a faithful representation  $\rho$  of  $G$  since  $\ker \rho$  is trivial. Therefore, since  $\mathfrak{m}_k^{G, N(G)}(Q) = 1$ , Theorem 1.1 follows from Theorem 3.7.  $\square$

Let  $G$  be a finite group, and let  $N \trianglelefteq G$  be a nontrivial normal subgroup. We observe that if  $F$  is a subfield of  $K \in \mathfrak{F}_k^G(Q)$  for which  $F \cap K^N = k$ , then the kernel of the Artin representation  $\rho_F$  of  $\text{Gal}(K/k)$  associated to the Artin  $L$ -function  $\zeta_F(s)/\zeta_k(s)$  does not contain  $N$ . Therefore, Theorem 3.7 is applicable. We emphasize two widely applicable cases of this in our next result; these will enable us to prove the applications in Section 2.

**Corollary 3.8.** *Let  $k$  be a number field and  $Q \geq 1$ . For a field  $F$ , let  $\tilde{F}$  denote its normal closure over  $k$  and let  $\rho$  be the Artin representation satisfying  $L(s, \rho_F) = \zeta_F(s)/\zeta_k(s)$ .*

- (1) *Let  $n \geq 3$ . For all  $\varepsilon > 0$ , there exists an effectively computable constant  $c_9 = c_9(n, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all except  $O_{n, [k: \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  fields  $F \in \mathcal{F}_k^{n, S_n}(Q)$ ,*
- (a)  *$L(s, \rho_F)$  is holomorphic and non-vanishing in the region  $\Omega_{\tilde{F}}(\varepsilon/n!)$ , and*
  - (b) *if  $x \geq (\log D_F)^{81(n!)^2/\varepsilon}$ , then*

$$(3.11) \quad \left| \sum_{N_{k/\mathbb{Q}} \mathfrak{p} \leq x} \chi_{\rho_F}(\mathfrak{p}) \right| \ll_{n, [k: \mathbb{Q}], \varepsilon} x \exp(-c_9 \sqrt{\log x}).$$

- (2) *Let  $p$  be prime. For all  $\varepsilon > 0$ , there exists an effectively computable constant  $c_{10} = c_{10}(p, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all except  $O_{p, [k: \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  fields  $F \in \mathcal{F}_k^p(Q)$ ,*
- (a)  *$L(s, \rho_F)$  is holomorphic and non-vanishing in the region  $\Omega_{\tilde{F}}(\varepsilon/p!)$ , and*
  - (b) *if  $x \geq (\log D_F)^{81(p!)^2/\varepsilon}$ , then*

$$(3.12) \quad \left| \sum_{N_{k/\mathbb{Q}} \mathfrak{p} \leq x} \chi_{\rho_F}(\mathfrak{p}) \right| \ll_{p, [k: \mathbb{Q}], \varepsilon} x \exp(-c_{10} \sqrt{\log x}).$$

*Proof.* (1) When  $G = S_n$ , let  $N$  be the unique minimal nontrivial normal subgroup of  $G$ , which is either  $A_n$  or  $V_4$ . In either case,  $N$  is transitive, and thus its intersection with a stabilizer subgroup of  $S_n$  has index  $n$  in  $N$ . Additionally, since  $N$  is the unique minimal,  $\mathfrak{m}_k^{G, N}(R) = 1$  for all  $R \geq 1$ , and Hypothesis  $T(G, N)$  is satisfied via Corollary 3.5. Finally, there exists an effectively computable constant  $c_{11} = c_{11}(n, [k : \mathbb{Q}]) > 0$  such that  $D_{\tilde{F}} \leq c_{11} D_F^{[\tilde{F}:k]} \leq c_{11} D_F^{[F:k]!}$ . Thus, for each  $F \in \mathcal{F}_k^{n, S_n}(Q)$ , the normal closure  $\tilde{F}$  over  $k$  lies in  $\mathfrak{F}_k^{S_n}(c_{11} Q^{[F:k]!})$ . If  $F \in \mathcal{F}_k^{n, S_n}(Q)$ , then  $F \cap \tilde{F}^N = k$  because  $F$  is the fixed field of a stabilizer subgroup. The result now follows from Theorem 3.7.

(2) The proof is the same as the previous part, except that we combine the contributions from all of the transitive subgroups of  $S_p$  (of which there are  $O_p(1)$ ). We invoke Lemma 8.1 and Corollary 3.5 to each of these transitive subgroups in order to apply Theorem 3.7.  $\square$

*Remark.* The lower bounds in (2.5) ensure that Corollary 3.8 is not vacuous.

Our proofs for Theorems 2.1, 2.4 and 3.10 rely on the bounds (3.11) and (3.12). Our proof of Theorem 2.2, and hence our proof of Theorem 2.3, uses the strong zero-free region in Corollary 3.8.

**3.5. Further examples.** As is made clear in the previous sections, our results are strongest for groups  $G$  possessing a unique minimal normal subgroup  $N$  for which  $T(G, N)$  holds. In particular, we obtain the following analogue of Theorem 1.1 for such groups  $G$ .

**Theorem 3.9.** *Let  $k$  be a number field. Let  $G$  be a finite group with a unique minimal normal subgroup  $N$  such that Hypothesis  $T(G, N)$  holds. Let  $Q \geq 1$ . For all  $\varepsilon > 0$ , there exists an effectively*

computable constant  $c_1 = c_1(|G|, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all except  $O_{|G|, [k : \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  normal extensions  $K/k$  with  $\text{Gal}(K/k) \simeq G$  and absolute discriminant  $D_K$  at most  $Q$ , each irreducible faithful Artin representation  $\rho$  of  $\text{Gal}(K/k)$  satisfies

$$\left| \sum_{N_k/\mathbb{Q}, \mathfrak{p} \leq x} \text{tr } \rho(\text{Frob}_{\mathfrak{p}}) \right| \ll_{|G|, [K : \mathbb{Q}], \varepsilon} x \exp(-c_1 \sqrt{\log x})$$

for all  $x \geq (\log D_K)^{81|G|/\varepsilon}$ .

There are many groups  $G$  satisfying both hypotheses of Theorem 3.9. For example, there are 50 transitive groups of degree 8, of which 42 are subject to Theorem 3.9, and of the 1954 transitive groups of degree 16, there are 1706 subject to Theorem 3.9. We therefore do not aim to provide an exhaustive list of such groups. Instead, we highlight a few systematic examples beyond the symmetric groups  $S_n$  and transitive groups of prime degree that have played a role earlier in this paper.

- All simple groups  $G$ , with  $N = G$ .
- The non-simple alternating group  $A_4$ , with  $N = V_4$ , the Klein four subgroup.
- The affine general linear group  $\text{AGL}_d(\mathbb{F}_p)$ , with  $N = (\mathbb{Z}/p\mathbb{Z})^d$ , and more generally any group of the form  $G_0 \rtimes (\mathbb{Z}/p\mathbb{Z})^d$  with  $G_0$  an irreducible subgroup of  $\text{GL}_d(\mathbb{F}_p)$ .
- Almost simple groups  $G$  whose socle has prime power index in  $G$ .
- Wreath products  $S_3 \wr H$  and  $S_4 \wr H$  for transitive permutation groups  $H$  of degree  $d$ , with  $N = A_3^d$  and  $N = V_4^d$ , respectively.

All but the last of these are primitive permutation groups, and consequently it is straightforward to obtain a version of Theorem 2.4 for these groups equal in quality to that for  $S_n$  and groups of prime degree. It is also possible to obtain a version for imprimitive groups, but with a somewhat worse bound on the  $\ell$ -torsion subgroup. Additionally, for any group  $G$  with a unique minimal normal subgroup  $N$  for which Hypothesis  $\text{T}(G, N)$  holds, primitive or otherwise, an analogue of Theorem 2.5 holds with the quadratic resolvent replaced by the subfield  $K^N$  fixed by  $N$ .

**Theorem 3.10.** *Let  $G$  be a finite group with a unique minimal normal subgroup  $N$  for which Hypothesis  $\text{T}(G, N)$  holds. Let  $k$  be a number field. Let  $\mathcal{C} \subseteq G$  be a conjugacy class and let  $[\mathcal{C}]_{G/N}$  denote the associated conjugacy class in  $G/N$ . Let  $Q \geq 1$ . For all  $\varepsilon > 0$ , there exists a constant  $c_1 = c_1(|G|, [k : \mathbb{Q}], \varepsilon) > 0$  such that for all except  $O_{n, [k : \mathbb{Q}], \varepsilon}(Q^\varepsilon)$  fields  $K \in \mathfrak{F}_k^G(Q)$ , one has that for any  $x \geq (\log D_K)^{81|G|/\varepsilon}$ , there holds*

$$\pi_{\mathcal{C}}(x; K/k) = \frac{|\mathcal{C}|}{|N| \cdot |[\mathcal{C}]_{G/N}|} \pi_{[\mathcal{C}]_{G/N}}(x; K^N/k) + O_{n, [k : \mathbb{Q}], \varepsilon}(x \exp(-c_1 \sqrt{\log x})),$$

where  $K^N$  denotes the subfield of  $K$  fixed by  $N$ .

#### 4. PRELIMINARIES ON ARTIN $L$ -FUNCTIONS

We recall the definition of an Artin  $L$ -function following [41, Chapter 2]. Let  $K/k$  be a Galois extension of number fields with Galois group  $G = \text{Gal}(K/k)$ . Let  $\mathcal{O}_k$  be the ring of integers of  $k$ . For each prime  $\mathfrak{p}$  of  $k$  and each prime  $\mathfrak{P}$  of  $K$  lying over  $\mathfrak{p}$ , let  $D_{\mathfrak{P}} = \text{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ , where  $K_{\mathfrak{P}}$  and  $k_{\mathfrak{p}}$  are the completions of  $K$  and  $k$  at  $\mathfrak{P}$  and  $\mathfrak{p}$ , respectively. Let  $F_{\mathfrak{P}}$  and  $F_{\mathfrak{p}}$  denote the residue fields of  $\mathfrak{P}$  and  $\mathfrak{p}$ . There is a map from  $D_{\mathfrak{P}}$  to  $\text{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$  that is surjective by Hensel's lemma. Define  $I_{\mathfrak{P}}$  to be the kernel of this map; we then have an exact sequence

$$1 \rightarrow I_{\mathfrak{P}} \rightarrow D_{\mathfrak{P}} \rightarrow \text{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}}) \rightarrow 1.$$

The group  $\text{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$  is cyclic with generator  $x \mapsto x^{N_{\mathfrak{p}}}$ . Choose  $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}$  whose image in  $\text{Gal}(F_{\mathfrak{P}}/F_{\mathfrak{p}})$  is this generator; it is only defined modulo  $I_{\mathfrak{P}}$ . We have  $I_{\mathfrak{P}} = 1$  for all unramified  $\mathfrak{p}$ , so for these  $\mathfrak{p}$ ,  $\sigma_{\mathfrak{P}}$  is well-defined. If we choose another prime  $\mathfrak{P}'$  above  $\mathfrak{p}$ , then  $I_{\mathfrak{P}'}$  and  $D_{\mathfrak{P}'}$

are conjugates of  $I_{\mathfrak{P}}$  and  $D_{\mathfrak{P}}$ . For  $\mathfrak{p}$  unramified, we denote by  $\sigma_{\mathfrak{p}}$  the conjugacy class of Frobenius automorphisms at primes  $\mathfrak{P}$  above  $\mathfrak{p}$ .

Let  $\rho: G \rightarrow \mathrm{GL}_n(\mathbb{C})$  be a complex representation of  $G$ , and let  $V$  be the underlying complex vector space on which  $\rho$  acts. We may restrict this action to the decomposition group  $D_{\mathfrak{P}}$  and see that the quotient  $D_{\mathfrak{P}}/I_{\mathfrak{P}}$  acts on the subspace  $V^{I_{\mathfrak{P}}}$  of  $V$  on which  $I_{\mathfrak{P}}$  acts trivially. Any  $\sigma_{\mathfrak{P}}$  will have the same characteristic polynomial on this subspace. For  $\mathrm{Re}(s) > 1$ , we define

$$L_{\mathfrak{p}}(s, \rho) = \det(1 - \rho(\sigma_{\mathfrak{P}})|V^{I_{\mathfrak{P}}}\mathbb{N}\mathfrak{p}^{-s})^{-1} = \prod_{j=1}^n (1 - \alpha_{j,\rho}(\mathfrak{p})\mathbb{N}\mathfrak{p}^{-s})^{-1}.$$

Note that the matrix  $\rho(\sigma_{\mathfrak{P}})|V^{I_{\mathfrak{P}}}$  remains the same if one changes the prime  $\mathfrak{P}$  lying above  $\mathfrak{p}$ ; indeed, if  $\mathfrak{p}$  is unramified, then  $\rho(\sigma_{\mathfrak{P}})|V^{I_{\mathfrak{P}}} = \rho(\sigma_{\mathfrak{p}})$ . We then define

$$(4.1) \quad L(s, \rho) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \rho) = \sum_{\mathfrak{n}} \frac{\lambda_{\rho}(\mathfrak{n})}{\mathbb{N}\mathfrak{n}^s}.$$

We have that  $|\alpha_{j,\rho}(\mathfrak{p})| \leq 1$  for all  $j$  and  $\mathfrak{p}$ , so  $L(s, \rho)$  has an absolutely convergent Dirichlet series and Euler product for  $\mathrm{Re}(s) > 1$ .

Let  $\Gamma_{\mathbb{R}}(s) := \pi^{-s/2}\Gamma(s/2)$ . For each archimedean place  $v$  of  $k$ , we define

$$L_v(s, \rho) = \begin{cases} \Gamma_{\mathbb{R}}(s)^n \Gamma_{\mathbb{R}}(s+1)^n & \text{if } k_v = \mathbb{C}, \\ \Gamma_{\mathbb{R}}(s)^a \Gamma_{\mathbb{R}}(s+1)^{n-a} & \text{if } k_v = \mathbb{R}, \end{cases}$$

where  $a = a(\rho)$  is the dimension of the  $+1$  eigenspace of complex conjugation. We define the numbers  $\mu_{\rho}(j)$  by the identity

$$L_{\infty}(s, \rho) = \prod_{v \text{ archim.}} L_v(s, \rho) = \prod_{j=1}^{n[k:\mathbb{Q}]} \Gamma_{\mathbb{R}}(s + \mu_{\rho}(j)).$$

Let the integral ideal  $\mathfrak{q}_{\rho} \subseteq \mathcal{O}_k$  denote the conductor of  $\rho$  over  $k$ . The completed  $L$ -function is defined by

$$(4.2) \quad \Lambda(s, \rho) := (D_k^n \mathbb{N}_{k/\mathbb{Q}} \mathfrak{q}_{\rho})^{s/2} L(s, \rho) L_{\infty}(s, \rho).$$

There exists  $W(\rho) \in \mathbb{C}$  of modulus one such that

$$\Lambda(s, \rho) = W(\rho) \Lambda(1-s, \bar{\rho})$$

for all  $s \in \mathbb{C}$  at which  $\Lambda(s, \rho)$  is holomorphic, where  $\bar{\rho}$  is the complex conjugate of  $\rho$ . We define the analytic conductor of  $\rho$  by

$$(4.3) \quad C(\rho, t) := D_k^n \mathbb{N}_{k/\mathbb{Q}} \mathfrak{q}_{\rho} \prod_{j=1}^{n[k:\mathbb{Q}]} (3 + |\mu_{\rho}(j) + it|), \quad C(\rho) := C(\rho, 0).$$

We observe that

$$(4.4) \quad C(\rho, t) \ll_{n, [k:\mathbb{Q}]} D_k^n \mathbb{N}_{k/\mathbb{Q}} \mathfrak{q}_{\rho} (3 + |t|)^{n[k:\mathbb{Q}]}.$$

**Lemma 4.1.** *If  $\rho$  is an  $n$ -dimensional Artin representation over  $k$  whose  $L$ -function  $L(s, \rho)$  is entire, then for  $\mathrm{Re}(s) \geq 1/2$ , then*

$$|L(s, \rho)| \ll_{n, [k:\mathbb{Q}]} C(\rho, t)^{\max\{\frac{1-\sigma}{2}, 0\}} (\log C(\rho, t))^{d[k:\mathbb{Q}](2\sigma-1)}.$$

*Proof.* The bound  $|L(1+it, \rho)| \ll_{n, [k:\mathbb{Q}]} (\log C(\rho, t))^{n[k:\mathbb{Q}]}$  follows by proceeding as in the proof of [9, Theorem 2]. The bound  $|L(\frac{1}{2}+it, \rho)| \ll_{n, [k:\mathbb{Q}]} C(\rho, t)^{n[k:\mathbb{Q}]/4}$  follows from the convexity bound due to Heath-Brown [28].  $\square$



If  $\rho$  is 1-dimensional, then Artin reciprocity shows that  $L(s, \rho)$  is a Hecke  $L$ -function and is thus entire if  $\rho$  is nontrivial. The Artin conjecture asserts that  $L(s, \rho)$  is entire for every nontrivial irreducible representation of  $G = \text{Gal}(K/k)$ , but this is unknown in general. The best general result is due to Brauer, and is a consequence of his induction theorem.

**Lemma 4.2** (Brauer induction). *For any complex representation  $\rho$  of  $\text{Gal}(K/k)$ , the Artin  $L$ -function  $L(s, \rho)$  has a meromorphic continuation to  $\mathbb{C}$ .*

We shall speak interchangeably about the Artin  $L$ -function associated to  $\rho$  and to its character  $\chi_\rho$  (i.e., its trace). For example, if  $\mathbf{1}_G$  denotes the character of the trivial representation of  $G$ , then  $L(s, \mathbf{1}_G) = \zeta_k(s)$ . Also, for any  $\rho$ , if there are rational coefficients  $c_i$  such that

$$\chi_\rho = \sum_{i=1}^k c_i \chi_{\rho_i},$$

where for each  $i \leq k$ ,  $\rho_i$  is complex representation of  $G$ , then Artin showed

$$L(s, \rho) = L(s, \chi_\rho) = \prod_{i=1}^k L(s, \chi_{\rho_i})^{c_i} = \prod_{i=1}^k L(s, \rho_i)^{c_i}.$$

Finally, if  $\chi$  is a character of a subgroup  $H \subset G$ , let  $\chi^* = \text{Ind}_H^G \chi$  denote the character of  $G$  induced by  $\chi$ . Then there is an equality of the associated  $L$ -functions,

$$L(s, \chi) = L(s, \chi^*),$$

where  $L(s, \chi)$  is an Artin  $L$ -function associated to  $K/K^H$  and  $K^H$  denotes the subfield fixed by  $H$ .

## 5. TRANSFER OF ZERO-FREE REGIONS

The goal of this section is to prove Theorems 3.3 and 3.4, whose setup we briefly recall. Let  $K/k$  be a normal extension of number fields with Galois group  $G$ . Let  $N \trianglelefteq G$  be a normal subgroup and let  $K^N$  denote the fixed field of  $N$ . We wish to show that if  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-zero in a region  $\Omega \subseteq \mathbb{C}$ , then  $L(s, \rho)$  is holomorphic and non-vanishing on  $\Omega$  for every irreducible Artin representation  $\rho$  of  $K/k$  whose kernel does not contain  $N$ . We shall make this more precise shortly, but in loose terms, the idea is to first show that a zero-free region for  $\zeta_K(s)/\zeta_{K^N}(s)$  transfers to  $L$ -functions attached to certain 1-dimensional characters of subgroups  $H \subseteq G$ . We do so in Lemma 5.5 for the largest possible set of characters for which this conclusion could reasonably hold, namely those whose kernel does not contain  $H \cap N$ . The next step is to show that this transfer of zero-free region to  $L$ -functions associated to 1-dimensional characters suffices. This transfer is equivalent to showing that the inductions of these 1-dimensional characters generate all characters of  $G$  whose kernel does not contain  $N$ . This is Hypothesis  $T(G, N)$ , which we restate in an equivalent manner below. Conjecture 3.2 asserts that Hypothesis  $T(G, N)$  holds for all finite groups  $G$  and normal subgroups  $N \trianglelefteq G$ . If Hypothesis  $T(G, N)$  holds, then Theorem 3.3 readily follows. The verification of Hypothesis  $T(G, N)$  is the most subtle piece of the argument. We are unable to prove Hypothesis  $T(G, N)$  holds in general; however, we do show in Theorem 5.6 that it holds in many natural cases, most notably when either the index  $[G : N]$  is a prime power or  $N$  is solvable. We then provide the proof of Theorem 3.6 that reduces the general Conjecture 3.2 to proving Hypothesis  $T(G, N)$  for a concrete set of groups. We close this section by illuminating the ideas of this paper with the example  $G = S_5$  and  $N = A_5$ .

Our approach is inspired by Brauer's approach to the Aramata–Brauer theorem that the quotient  $\zeta_K(s)/\zeta_k(s)$  is entire. The ideas of Brauer's proof quickly establish the theorem in the special case  $N = G$ , and thus with  $K^N = k$ . In fact, as Brauer's work is also an ingredient in our proof of the general case, we find it useful to briefly summarize his ideas.

**5.1. The Aramata–Brauer theorem and Theorem 3.3 when  $N = G$ .** We first introduce some notation. Given a subgroup  $H \subseteq G$ , we let  $\mathbf{1}_H$  denote the trivial character of  $H$ . Given any character  $\chi$  of  $H$  and any subgroup  $H' \supseteq H$ , we let  $\text{Ind}_H^{H'} \chi$  denote the character of  $H'$  induced by  $\chi$ . We begin with the following lemma of Brauer [7].

**Lemma 5.1** (Brauer). *Let  $N$  be a finite group. For each nontrivial character  $\chi$  of a cyclic subgroup of  $N$ , there is a positive rational constant  $c_\chi$  such that*

$$\text{Ind}_1^N \mathbf{1} - \mathbf{1}_N = \sum_{\substack{g \in N \\ g \neq \text{id}}} \sum_{\chi \in \widehat{\langle g \rangle}}' c_\chi \text{Ind}_{\langle g \rangle}^N \chi,$$

where  $\chi$  runs over the nontrivial characters of the cyclic group  $\langle g \rangle$ .

*Proof.* Brauer shows that if  $\chi$  is a nontrivial character of the cyclic subgroup  $\langle g \rangle$ , one may take

$$c_\chi = \frac{1}{|N|} \sum_{\substack{h \in \langle g \rangle \\ \langle h \rangle = \langle g \rangle}} (1 - \bar{\chi}(h)).$$

This is rational (it is invariant under the action of Galois) and positive (because  $\chi$  is nontrivial).  $\square$

From Lemma 5.1, it is straightforward to deduce the Aramata–Brauer theorem and a first consequence toward non-vanishing.

**Lemma 5.2.** *The quotient  $\zeta_K(s)/\zeta_{K^N}(s)$  is entire. Moreover, let  $H \subseteq N$  be a cyclic subgroup and let  $\chi$  be a nontrivial irreducible character of  $H$ . If  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-zero in a region  $\Omega \subseteq \mathbb{C}$ , then  $L(s, \chi)$  is holomorphic and non-vanishing in  $\Omega$ .*

*Proof.* By Lemma 5.1, it follows for  $\text{Re}(s) > 1$  that

$$\frac{\zeta_K(s)}{\zeta_{K^N}(s)} = \prod_{\substack{g \in N \\ g \neq \text{id}}} \prod_{\chi \in \widehat{\langle g \rangle}}' L(s, \chi)^{c_\chi}.$$

Each character  $\chi$  is abelian, hence each  $L(s, \chi)$  is entire. Since  $\zeta_K(s)/\zeta_{K^N}(s)$  is meromorphic and since each  $c_\chi$  is positive, it follows that  $\zeta_K(s)/\zeta_{K^N}(s)$  is entire. The statement on non-vanishing similarly follows from the positivity of each  $c_\chi$  and the fact that each  $L(s, \chi)$  is entire.  $\square$

For the next lemma, we introduce some additional notation. For any finite group  $G$ , let  $\mathcal{R}_{\mathbb{Z}}(G)$  denote the ring of virtual characters of  $G$ , i.e. integral linear combinations of the irreducible characters of  $G$ , and let  $\mathcal{R}_{\mathbb{Q}}(G) = \mathcal{R}_{\mathbb{Z}}(G) \otimes \mathbb{Q}$  and  $\mathcal{R}_{\mathbb{C}}(G) = \mathcal{R}_{\mathbb{Z}}(G) \otimes \mathbb{C}$ . The space  $\mathcal{R}_{\mathbb{C}}(G)$  is the space of class functions on  $G$ , on which there is an inner product

$$\langle f_1, f_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

The irreducible characters of  $G$  form an orthonormal basis for  $\mathcal{R}_{\mathbb{C}}(G)$  with respect to this inner product. The orthogonal complement of the trivial character is the space of class functions with mean 0 on  $G$ . By Frobenius reciprocity, this condition is invariant under induction. We also note that this inner product is defined on  $\mathcal{R}_{\mathbb{Q}}(G)$  as well.

Our next lemma is essentially the Artin induction theorem.

**Lemma 5.3** (Artin induction). *The orthogonal complement of the trivial character in  $\mathcal{R}_{\mathbb{Q}}(G)$  is spanned by the induction of nontrivial characters of cyclic subgroups of  $G$ .*

*Proof.* It suffices to prove the analogous statement over  $\mathbb{C}$ . Given  $g \neq \text{id}$ , let  $f_g$  be the class function on the cyclic group  $H = \langle g \rangle$  defined by

$$f_g(h) = \begin{cases} 1, & \text{if } h = g, \\ -1 & \text{if } h = \text{id}, \\ 0 & \text{if } h \notin \{g, \text{id}\}. \end{cases}$$

As  $f_g$  has mean 0 on  $H$ , it may be expressed as a linear combination of the non-trivial characters of  $H$ . Its induction  $\text{Ind}_H^G f_g$  thus also has mean 0, and is supported on the identity and the conjugacy class of  $g$ . Varying over all  $g \neq \text{id}$ , such functions naturally span the orthogonal complement of the trivial character.  $\square$

Combining Lemmas 5.2 and 5.3, we obtain:

**Lemma 5.4.** *Suppose that  $\zeta_K(s)/\zeta_{KN}(s)$  is non-zero in a region  $\Omega \subseteq \mathbb{C}$ . Let  $\psi \in \mathcal{R}_{\mathbb{Q}}(N)$  lie in the orthogonal complement of the trivial character of  $N$ . Then the Artin  $L$ -function  $L(s, \psi)$  is holomorphic and non-vanishing in  $\Omega$ .*

*Proof.* Applying Lemma 5.3 to  $N$ , there are rational numbers  $c_{\chi, \psi}$  such that

$$\psi = \sum_{\substack{g \in N \\ g \neq \text{id}}} \sum_{\substack{\chi \in \widehat{\langle g \rangle} \\ \chi \neq 1}} c_{\chi, \psi} \text{Ind}_{\langle g \rangle}^N \chi,$$

where the sum runs over the nontrivial characters of  $\langle g \rangle$ . Consequently, we find the factorization

$$L(s, \psi) = \prod_{\substack{g \in N \\ g \neq \text{id}}} \prod_{\substack{\chi \in \widehat{\langle g \rangle} \\ \chi \neq 1}} L(s, \chi)^{c_{\chi, \psi}}.$$

By Lemma 5.2, each  $L(s, \chi)$  is holomorphic and non-vanishing in  $\Omega$ , so the same must hold for  $L(s, \psi)$  as well.  $\square$

Lemma 5.4 yields Theorem 3.3 in the case  $N = G$ . The general case is apparently more subtle, however.

**5.2. Inductions of characters with restricted components.** Recall that there is a natural injection  $\mathcal{R}_{\mathbb{Q}}(G/N) \hookrightarrow \mathcal{R}_{\mathbb{Q}}(G)$  given by pullback, so we may regard  $\mathcal{R}_{\mathbb{Q}}(G/N)$  as a subgroup of  $\mathcal{R}_{\mathbb{Q}}(G)$ . Exploiting the inner product on  $\mathcal{R}_{\mathbb{Q}}(G)$ , we may thus consider an orthogonal decomposition

$$(5.1) \quad \mathcal{R}_{\mathbb{Q}}(G) = \mathcal{R}_{\mathbb{Q}}(G/N) \oplus \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp},$$

where  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  denotes the orthogonal complement of  $\mathcal{R}_{\mathbb{Q}}(G/N)$ . So doing,  $\mathcal{R}_{\mathbb{Q}}(G/N)$  is spanned by the irreducible constituents of the character  $\text{Ind}_N^G \mathbf{1}_N$ . Consequently,  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  is most naturally spanned by the irreducible characters whose kernel does not contain  $N$ . These are exactly the characters of the type considered in Theorem 3.3. However, as in the previous subsection, the analytic properties of the  $L$ -functions attached to such characters are not easily accessed directly and are only understood by comparison to  $L$ -functions attached to 1-dimensional characters.

Hypothesis  $\text{T}(G, N)$  asserts a refinement of the Artin induction theorem that respects the orthogonal decomposition (5.1). It follows from Lemma 5.3 that  $\mathcal{R}_{\mathbb{Q}}(G/N)$  is spanned by the induction of one-dimensional characters whose induction itself lies in  $\mathcal{R}_{\mathbb{Q}}(G/N)$ ; in fact, characters of cyclic subgroups suffice. In other words, it follows that

$$\mathcal{R}_{\mathbb{Q}}(G/N) = \text{span}_{\mathbb{Q}} \bigcup_{H \subseteq G} \{ \text{Ind}_H^G \chi : \chi \in \text{Irr}(H), \dim \chi = 1, \text{ and } \text{Ind}_H^G \chi \in \mathcal{R}_{\mathbb{Q}}(G/N) \},$$

where  $\text{Irr}(H)$  denotes the set of irreducible complex representations of a subgroup  $H \subseteq G$ .

Hypothesis  $\text{T}(G, N)$  is equivalent to the corresponding statement for  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$ .

**Hypothesis** (Equivalent formulation of Hypothesis  $T(G, N)$ ). *The space  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  is spanned by the induction of one-dimensional characters whose induction lies in  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$ . In other words, we have that*

$$\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp} = \text{span}_{\mathbb{Q}} \bigcup_{H \subseteq G} \{ \text{Ind}_H^G \chi : \chi \in \text{Irr}(H), \dim \chi = 1, \text{ and } \text{Ind}_H^G \chi \in \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp} \}.$$

The main result of this section, Theorem 5.6 below, establishes Hypothesis  $T(G, N)$  when  $N$  is solvable or the index  $[G : N]$  is a prime power. Its proof concludes that of Theorem 3.4.

The subtlety of Hypothesis  $T(G, N)$  is revealed upon noting that the orthogonal decomposition (5.1) is preserved neither upon restriction to subgroups  $H \subseteq G$  nor upon induction from subgroups. For example, the trivial character of  $H$  always lies in  $\mathcal{R}_{\mathbb{Q}}(H/H \cap N)$ , but its induction to  $G$  need not lie in  $\mathcal{R}_{\mathbb{Q}}(G/N)$ . Thus, typical elementary approaches exploiting the adjointness of induction and restriction do not obviously apply. Moreover, it is not the case that the induction of characters of cyclic, or even abelian, subgroups suffice to span  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  in general.

We first prove a non-vanishing result for  $L$ -functions attached to the characters we shall use. For this, we note that if  $\chi$  is a 1-dimensional character of a subgroup  $H \subseteq G$ , then  $\text{Ind}_H^G \chi \in \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  if and only if the kernel of  $\chi$  does not contain  $H \cap N$ .

**Lemma 5.5.** *Let  $H \subseteq G$  be a subgroup and suppose that  $\chi$  is a 1-dimensional character of  $H$  whose kernel does not contain  $H \cap N$ . If  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in a region  $\Omega \subseteq \mathbb{C}$ , then  $L(s, \chi)$  is holomorphic and non-vanishing in  $\Omega$ .*

*Proof.* Since  $\chi$  is 1-dimensional, it follows from Artin reciprocity that  $L(s, \chi)$  is a Hecke  $L$ -function, and since  $\chi$  is nontrivial, it is thus entire. To show that  $L(s, \chi)$  is non-vanishing in  $\Omega$ , let  $\chi^* = \text{Ind}_H^G \chi$ , and consider the character  $\theta_N = \text{Ind}_N^G \mathbf{1}_N - \mathbf{1}_G$  of  $G$ . Then  $\chi^* + \theta_N \chi^* = \chi^* \text{Ind}_N^G \mathbf{1}_N = \text{Ind}_N^G \chi_N^*$ , where  $\chi_N^* := \chi^*|_N$  denotes the restriction of  $\chi^*$  to  $N$ . It follows that

$$L(s, \chi)L(s, \chi^* \otimes \theta_N) = L(s, \chi_N^*).$$

By our assumption on  $\chi$ , the character  $\chi_N^*$  of  $N$  is orthogonal to the trivial character. Thus, by Lemma 5.4,  $L(s, \chi_N^*)$  is holomorphic and non-vanishing on  $\Omega$ . Consequently, the lemma will follow provided we show that  $L(s, \chi^* \otimes \theta_N)$  is entire.

By Lemma 5.1 applied to  $G/N$ , we may express  $\theta_N$  as a positive rational linear combination of the induction  $\psi^*$  of characters  $\psi$  of cyclic subgroups of  $G/N$ . Since  $L(s, \chi^* \otimes \theta_N)$  is meromorphic by Lemma 4.2, it suffices to show that each  $L(s, \chi^* \otimes \psi^*)$  is entire. Let  $K^{\psi} \subseteq K^N$  be the cyclic subextension from which  $\psi$  is induced and let  $F'/F$  be the cyclic extension corresponding to  $\chi$ . Let  $\psi_F$  denote the restriction of  $\psi$  to the subgroup  $\text{Gal}(FK^N/FK^{\psi}) \subseteq \text{Gal}(K^N/K^{\psi})$ .

If  $F'$  is linearly disjoint from  $FK^{\psi}$  over  $F$ , then we may regard both  $\chi$  and  $\psi_F$  as characters of the abelian Galois group  $\text{Gal}(F'K^N/FK^{\psi})$ . Thus, the product  $\chi\psi_F$  is well-defined, and we have  $L(s, \chi^* \otimes \psi^*) = L(s, \chi\psi_F)$ . Our assumption on  $\chi$  ensures that  $F'$  is not contained in  $FK^N$ , so the character  $\chi\psi_F$  is non-trivial, and hence  $L(s, \chi^* \otimes \psi^*)$  is entire in this case.

If  $F'$  is not linearly disjoint from  $FK^{\psi}$  over  $F$ , the character  $\chi\psi_F$  need not be defined. However, we may regard  $\chi$  as a character of  $G_F = \text{Gal}(K^N F'/F)$  and  $\psi_F$  as a character of its subgroup  $G_{\psi} = \text{Gal}(K^N F'/FK^{\psi})$ . So doing, we find  $\chi \text{Ind}_{G_{\psi}}^{G_F} \psi_F = \text{Ind}_{G_{\psi}}^{G_F} (\psi_F \chi_{\psi})$ , where  $\chi_{\psi} := \chi|_{G_{\psi}}$  denotes the restriction of  $\chi$  to  $G_{\psi}$ . Then  $L(s, \chi^* \otimes \psi^*) = L(s, \psi_F \chi_{\psi})$ . As above, by our assumption on  $\chi$ , the (abelian) character  $\psi_F \chi_{\psi}$  is non-trivial, and we again conclude that  $L(s, \chi^* \otimes \psi^*)$  is entire. This completes the proof of the lemma.  $\square$

**Theorem 5.6.** *Let  $G$  be a finite group and  $N \trianglelefteq G$  a normal subgroup. If  $N$  is solvable or the index  $[G : N]$  is a prime power, then Hypothesis  $T(G, N)$  holds.*

*Proof.* Notice that the induction of a character  $\chi$  from a subgroup  $H$  is in the orthogonal complement of  $\mathcal{R}_{\mathbb{Q}}(G/N)$  if and only if its kernel does not contain  $H \cap N$ . Thus, the conclusion of the

theorem holds if every irreducible character of  $G$  is the induction of a 1-dimensional character of a subgroup of  $G$ , i.e. if  $G$  is monomial. Consequently, the theorem holds whenever  $G$  is abelian or, more generally, whenever  $G$  is nilpotent [47, Chapter 8]. In fact, all monomial groups are solvable, so this fact is subsumed by the statement of the theorem. We find it convenient to note also that all  $p$ -groups are nilpotent, so the statement is known in this case. It also holds when  $N = G$  by Lemma 5.3. Finally, we note that it is also known when  $N$  is abelian by work of Deligne and Henniart [13, Proposition 2.2].

We first consider the case that  $N$  is solvable. We proceed by induction on the order of  $G$ , taking as a base case the statement for abelian  $G$ . If  $N$  is trivial, then the conclusion is vacuous, so we may assume that  $N$  is nontrivial. Let  $N'$  be a nontrivial minimal normal subgroup of  $G$  contained in  $N$ . Since  $N$  is solvable,  $N'$  must be solvable as well. Additionally, since  $N'$  must be characteristically simple, it is isomorphic to a group of the form  $T^d$  for a simple group  $T$ . Since  $N'$  is solvable,  $T$  must be cyclic of prime order, so  $N'$  is abelian. Consequently, by [13, Proposition 2.2], it follows that  $T(G, N')$  holds.

If  $N' = N$ , then this establishes the result. If  $N' \subsetneq N$ , then  $\mathcal{R}_{\mathbb{Q}}(G/N)$  is a proper subspace of  $\mathcal{R}_{\mathbb{Q}}(G/N')$  and  $\mathcal{R}_{\mathbb{Q}}(G/N')^{\perp}$  is a subspace of  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$ , where all spaces are viewed as subspaces of  $\mathcal{R}_{\mathbb{Q}}(G)$ . Moreover,

$$\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp} = \mathcal{R}_{\mathbb{Q}}(G/N')^{\perp} \oplus (\mathcal{R}_{\mathbb{Q}}(G/N') \cap \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}).$$

Since  $T(G, N')$  holds,  $\mathcal{R}_{\mathbb{Q}}(G/N')^{\perp}$  is spanned by the induction of 1-dimensional characters whose inductions lie in  $\mathcal{R}_{\mathbb{Q}}(G/N')^{\perp}$ , which must also lie in  $\mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$ . It remains to show that  $\mathcal{R}_{\mathbb{Q}}(G/N') \cap \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  is spanned by such characters. However, since  $N' \subset N$ ,  $G/N \simeq (G/N')/(N/N')$ , and the elements of  $\mathcal{R}_{\mathbb{Q}}(G/N') \cap \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  are obtained by pullback from  $\mathcal{R}_{\mathbb{Q}}((G/N')/(N/N'))^{\perp} \subseteq \mathcal{R}_{\mathbb{Q}}(G/N')$ , where we regard  $\mathcal{R}_{\mathbb{Q}}(G/N')$  in this final statement as its own space and not as a subspace of  $\mathcal{R}_{\mathbb{Q}}(G)$ . Since  $N'$  is nontrivial,  $T(G/N', N/N')$  must hold by the inductive hypothesis, and we conclude that  $\mathcal{R}_{\mathbb{Q}}((G/N')/(N/N'))^{\perp}$  is spanned by the induction of 1-dimensional characters whose kernel does not contain  $N/N'$ . Pulling back a basis of such characters, we deduce that  $\mathcal{R}_{\mathbb{Q}}(G/N') \cap \mathcal{R}_{\mathbb{Q}}(G/N)^{\perp}$  is spanned by the induction of 1-dimensional characters whose kernel does not contain  $N$ . This yields the result in the case  $N$  is solvable.

We now consider the case that  $[G : N]$  is a prime power. We once again induct on the order of  $G$ , exploiting the subgroups of  $G$ . It suffices to work with complex coefficients, that is, to show the orthogonal complement of  $\mathcal{R}_{\mathbb{C}}(G/N)$  inside  $\mathcal{R}_{\mathbb{C}}(G)$  is spanned by the induction of such characters. We therefore consider a class function  $f$  of  $G$  that is orthogonal to the induction of all such characters, with the goal of showing that it lies in  $\mathcal{R}_{\mathbb{C}}(G/N)$ . Equivalently, we wish to show that  $f$  is constant on cosets of  $N$ , that is, that  $f(a) = f(b)$  whenever  $ab^{-1} \in N$ . Consider two such elements  $a, b \in G$ .

By Frobenius reciprocity and the inductive hypothesis, it follows that if  $a$  and  $b$  lie in the same proper subgroup  $H$ , then  $f(a) = f(b)$ . In particular, if  $a$  and  $b$  do not generate  $G$ , then we may take  $H$  to be the subgroup generated by  $a$  and  $b$ . Thus, we may assume that  $a$  and  $b$  generate  $G$ . This implies that  $G/N$  is cyclic, since we have assumed that  $aN = bN$ .

Next, since the index of  $N$  in  $G$  is a power of a prime, we may write  $[G : N] = p^k$ . By our inductive hypothesis applied to the cyclic subgroup generated by  $a$ , or noting that such a group is abelian, we see that  $f(a) = f(a^m)$  whenever  $m \equiv 1 \pmod{p^k}$ . Thus, replacing  $a$  by a suitable power if necessary, we may assume that the order of  $a$  is a power of  $p$ . Similarly, we assume that the order of  $b$  is a power of  $p$ . Let  $H$  be a Sylow  $p$ -subgroup of  $G$  containing  $a$ , possibly equal to  $G$  itself. Since  $f$  is a class function, we may conjugate  $b$  if necessary to assume that  $b \in H$  as well. But  $H$  is a  $p$ -group, so the theorem holds for  $H$ . As we have  $ab^{-1} \in H \cap N$ , it follows that  $f(a) = f(b)$ . This establishes the theorem in the case  $[G : N]$  is a prime power.  $\square$

*Proof of Theorem 3.3.* With these facts in hand, the proof of Theorem 3.3 is now straightforward. Any irreducible representation  $\rho$  of  $G$  whose kernel does not contain  $N$  lies in the orthogonal complement of  $\mathcal{R}_{\mathbb{Q}}(G/N)$ . If Hypothesis  $T(G, N)$  holds, and in particular under the assumptions of Theorem 5.6, there are rational constants  $c_{\chi}(\rho)$  such that

$$L(s, \rho) = \prod_{\chi} L(s, \chi)^{c_{\chi}(\rho)},$$

where the product runs over 1-dimensional characters  $\chi$  of subgroups  $H$  of  $G$  whose kernel does not contain  $N$ . By Lemma 5.5, if  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in the region  $\Omega \subseteq \mathbb{C}$ , then each  $L(s, \chi)$  is holomorphic and non-vanishing in  $\Omega$ . Thus, the same must be true for  $L(s, \rho)$ . This completes the proof.  $\square$

*Proof of Theorem 3.6.* The proof of Theorem 5.6 given above shows it is sufficient to understand Hypothesis  $T(G, N)$  for finite groups  $G$  with nonabelian minimal normal subgroups  $N$  such that  $G/N$  is cyclic of non-prime power order. We begin by showing it is further possible to reduce to the case that  $G$  is a subgroup of  $\text{Aut}(N)$ .

Let  $K$  be the kernel of the map  $G \rightarrow \text{Aut}(N)$  given by conjugation. Since  $N$  is nonabelian and minimal,  $K \cap N$  is trivial, and this realizes  $G$  as the fiber product  $G/N \times_{G/NK} G/K$ . The quotient  $G/K$  is naturally a subgroup of  $\text{Aut}(N)$  containing  $N$ , and we suppose that Hypothesis  $T(G/K, N)$  is true. Since  $G/N$  is abelian, any irreducible character of  $G$  may be decomposed as a product  $(\chi_1, \chi_2)$ , where  $\chi_1$  is a character of  $G/N$  and  $\chi_2$  is a character of  $G/K$ , with two such products being the same if they differ by a factor  $(\psi, \bar{\psi})$  for a character  $\psi$  of the common quotient,  $G/NK$ . Let  $(\chi_1, \chi_2)$  be an irreducible character of  $G$  not contained in  $\mathcal{R}_{\mathbb{Q}}(G/N)$ , so in particular  $\chi_2$  is an irreducible character of  $G/K$  lying in  $\mathcal{R}_{\mathbb{Q}}(G/KN)^{\perp}$ . Since we have assumed  $T(G/K, N)$  holds, there are constants  $c_{\chi} \in \mathbb{Q}$  such that

$$\chi_2 = \sum_{H \subseteq G/K} \sum_{\substack{\chi \in \text{Irr}(H) \\ \chi(1)=1 \\ \ker \chi \not\supseteq H \cap N}} c_{\chi} \text{Ind}_H^{G/K} \chi.$$

For a subgroup  $H \subseteq G/K$ , let  $H_G$  denote the corresponding subgroup of  $G$ , i.e.  $H_G = \{(a, h) \in G/N \times_{G/NK} G/K : h \in H\}$ . Then any 1-dimensional character  $\chi$  of  $H$  is also a character of  $H_G$  and the character  $\chi_1$  restricts to a character on  $H_G$ . Moreover, if  $N \cap H \not\subseteq \ker \chi$ , then  $N \cap H_G \not\subseteq \ker(\chi \cdot \chi_1|_{H_G})$  as well. Additionally, we have

$$(\chi_1, \chi_2) = \sum_{H \subseteq G/K} \sum_{\substack{\chi \in \text{Irr}(H) \\ \chi(1)=1 \\ \ker \chi \not\supseteq H \cap N}} c_{\chi} \text{Ind}_{H_G}^G (\chi \cdot \chi_1|_{H_G}),$$

which shows that  $T(G, N)$  holds provided  $T(G/K, N)$  does. This reduces Conjecture 3.2 to the case that  $G$  is a subgroup of  $\text{Aut}(N)$ , where  $N$  is a nonabelian minimal normal subgroup of  $G$ .

Since  $N$  is minimal, it is characteristically simple, and hence of the form  $T^d$  for some nonabelian simple group  $T$ , in which case  $G$  is a subgroup of the wreath product  $\text{Aut}(T) \wr S_d$ . Applying the reductions in the proof of Theorem 5.6, we may assume  $G/N$  is cyclic. This implies that  $d$  must be prime, since otherwise the degree  $d$  permutation action of  $G$  would have nontrivial blocks, violating the assumption that  $N$  is minimal. This yields the theorem.  $\square$

**5.3. An example: The symmetric group  $S_5$ .** We illustrate the proof of Theorem 3.3, in particular Lemma 5.5 and Theorem 5.6, with one of the simplest interesting examples. Let  $G = S_5$  and  $N = A_5$ , let  $K/k$  be a normal extension with Galois group  $S_5$ , and assume that  $\zeta_K(s)/\zeta_{K^{A_5}}(s)$  is non-vanishing in some region  $\Omega \subseteq \mathbb{C}$ . Apart from the trivial character,  $S_5$  also admits the sign character, which we denote  $\chi_{\text{sgn}}$ , whose kernel is equal to  $A_5$ . Every other irreducible complex

representation of  $S_5$  is faithful. We denote these  $\rho_4$ ,  $\rho_4 \otimes \chi_{\text{sgn}}$ ,  $\rho_5$ ,  $\rho_5 \otimes \chi_{\text{sgn}}$ , and  $\rho_6$ , where the subscript indicates the dimension of the representation; for the purposes of this discussion, the choice of which 4-dimensional representation we denote  $\rho_4$  and which we denote  $\rho_4 \otimes \chi_{\text{sgn}}$  is neither important nor illuminating, nor is the choice of  $\rho_5$  and  $\rho_5 \otimes \chi_{\text{sgn}}$ . Theorem 3.3 asserts that the  $L$ -functions attached to these five faithful representations should be holomorphic and non-vanishing in  $\Omega$ .

For  $L(s, \rho_6)$ , this follows from Lemma 5.4 since  $\rho_6$  is its own twist by  $\chi_{\text{sgn}}$  and is therefore induced from an irreducible representation of  $A_5$ . In general, a representation is induced from  $A_5$  if and only if it is its own twist by  $\chi_{\text{sgn}}$ , and the  $A_5$ -representation is orthogonal to the trivial character if and only if the associated  $L$ -function is holomorphic at  $s = 1$ . Thus, for the other faithful representations, it only follows from Lemma 5.4 that the products  $L(s, \rho_4)L(s, \rho_4 \otimes \chi_{\text{sgn}})$  and  $L(s, \rho_5)L(s, \rho_5 \otimes \chi_{\text{sgn}})$  are holomorphic and non-vanishing in  $\Omega$ .

Let now  $\chi_{C_6}$  be either primitive character of the cyclic subgroup  $C_6 := \langle (123)(45) \rangle \subseteq S_5$ . The kernel of  $\chi_{C_6}$  is trivial, but  $C_6 \cap A_5$  is not, so  $L(s, \chi_{C_6})$  is subject to Lemma 5.5. Indeed, the proof of Lemma 5.5 in this case amounts to observing that the character  $\chi_{C_6} \otimes \chi_{\text{sgn}} = \chi_{C_6}^4$  is another non-trivial character of  $C_6$  whose kernel does not contain  $C_6 \cap A_5$ . The product  $L(s, \chi_{C_6})L(s, \chi_{C_6} \otimes \chi_{\text{sgn}})$  is then induced from a representation of  $A_5$  that must be orthogonal to the trivial representation of  $A_5$  since the  $L$ -function does not have a pole at  $s = 1$ . It follows from Lemma 5.4 that this product is holomorphic and non-vanishing in  $\Omega$ , and since each factor is entire, the same holds for both  $L(s, \chi_{C_6})$  and  $L(s, \chi_{C_6} \otimes \chi_{\text{sgn}})$ .

By expressing the induction of  $\chi_{C_6}$  in terms of the irreducible representations of  $S_5$ , we now compute that

$$L(s, \chi_{C_6}) = L(s, \rho_4)L(s, \rho_5)L(s, \rho_5 \otimes \chi_{\text{sgn}})L(s, \rho_6).$$

Observe that  $L(s, \rho_4)$  may therefore be expressed as a quotient of functions that are holomorphic and non-vanishing in  $\Omega$ , so it must be holomorphic and non-vanishing as well. By instead considering  $L(s, \chi_{C_6} \otimes \chi_{\text{sgn}})$ , we similarly find that  $L(s, \rho_4 \otimes \chi_{\text{sgn}})$  is holomorphic and non-vanishing in  $\Omega$ .

To show that  $L(s, \rho_5)$  and  $L(s, \rho_5 \otimes \chi_{\text{sgn}})$  are holomorphic and non-vanishing in  $\Omega$ , it is necessary to work with non-abelian subgroups of  $S_5$ , since a computation reveals that the induction of characters from other abelian subgroups gives at most the same information as  $\chi_{C_6}$  above. Thus, we consider the 2-Sylow subgroup  $D_4 \subseteq S_5$ . The sign character restricts to a non-trivial character of  $D_4$ , but there are two other quadratic characters of  $D_4$  that are twists of each other by  $\chi_{\text{sgn}}$ , thus witnessing again the proof of Lemma 5.5. Let  $\chi_{D_4}$  denote one of these characters. Then  $L(s, \chi_{D_4})$  is holomorphic and non-vanishing in  $\Omega$ , and we compute

$$L(s, \chi_{D_4}) = L(s, \rho_4)L(s, \rho_5)L(s, \rho_6).$$

From the above discussion, both  $L(s, \rho_4)$  and  $L(s, \rho_6)$  are holomorphic and non-vanishing in  $\Omega$ , so it follows that  $L(s, \rho_5)$  must be too. Finally, working instead with  $L(s, \chi_{D_4} \otimes \chi_{\text{sgn}})$ , we conclude that  $L(s, \rho_5 \otimes \chi_{\text{sgn}})$  is holomorphic and non-vanishing in  $\Omega$  as well.

In general, an analysis of the proof of Theorem 5.6 shows that it always suffices to consider characters of abelian subgroups and of subgroups of  $p$ -Sylow subgroups for  $p \mid [G : N]$ . Unlike the above example, however, the proof of Theorem 5.6 proceeds indirectly via class functions to avoid needing a careful understanding of the character theory of  $G$  and its subgroups. We leave open the questions of whether there is a more direct proof of Theorem 5.6, whether Hypothesis T( $G, N$ ) holds in general, and whether there is an explicit description of a sufficient set of characters.

## 6. THE ZERO DENSITY ESTIMATE

We now turn to establishing the main zero density estimate, from which Theorem 3.1 will ultimately follow. Let  $k$  be a number field, let  $G$  be a finite group, and let  $N \trianglelefteq G$  be a normal subgroup. Recall the definitions of  $\mathfrak{F}_k^G$  and  $\mathfrak{F}_k^G(Q)$ .

Given  $K \in \mathfrak{F}_k^G$ , define

$$N_{K/K^N}(\sigma, T) := \#\left\{\beta + i\gamma : \beta \geq \sigma, |\gamma| \leq T, \frac{\zeta_K(\beta + i\gamma)}{\zeta_{K^N}(\beta + i\gamma)} = 0\right\}.$$

Recall that

$$\mathfrak{m}_k^{G,N}(Q) = \max_{K_1 \in \mathfrak{F}_k^G(Q)} \#\{K_2 \in \mathfrak{F}_k^G(Q) : K_1 \cap K_2 \neq K_1^N \cap K_2^N\}.$$

We will prove the following zero density estimate.

**Theorem 6.1.** *Let  $0 \leq \sigma \leq 1$ ,  $Q \geq 1$ ,  $T \geq 2$ , and  $\varepsilon > 0$ . There exists a constant  $C_G > 0$ , depending at most on  $G$ , such that*

$$\sum_{K \in \mathfrak{F}_k^G(Q)} N_{K/K^N}(\sigma, T) \ll_{|G|, [k:\mathbb{Q}], \varepsilon} \mathfrak{m}_k^{G,N}(Q) (QT)^{|G|[k:\mathbb{Q}]} (8+\varepsilon)^{|G|(1-\sigma)} (\log QT)^{C_G [k:\mathbb{Q}]}.$$

**6.1. Tensor products of certain Artin representations.** For future convenience, given  $K \in \mathfrak{F}_k^G$ , let  $\psi_K$  denote the character of  $G$  given by  $\psi_K := \text{Reg}_G - \text{Ind}_N^G \mathbf{1}_N$ , where  $\text{Reg}_G$  denotes the character of the regular representation of  $G$ . Thus,

$$L(s, \psi_K) = \zeta_K(s) / \zeta_{K^N}(s)$$

for any  $K \in \mathfrak{F}_k^G$ .

**Lemma 6.2.** *Let  $G_1$  and  $G_2$  be finite groups. Suppose that  $\psi_1$  and  $\psi_2$  are characters of  $G_1$  and  $G_2$ , respectively, that are positive rational linear combinations of characters induced from non-trivial one-dimensional representations of cyclic subgroups of  $G_1$  and  $G_2$ .*

*Then the character  $\psi_1\psi_2$  of the direct product  $G_1 \times G_2$  is a positive rational linear combination of characters induced from non-trivial one-dimensional representations of subgroups of  $G_1 \times G_2$ .*

*Proof.* If  $\chi_1$  and  $\chi_2$  are non-trivial characters of subgroups  $H_1 \subseteq G_1$  and  $H_2 \subseteq G_2$ , then  $\chi_1\chi_2$  is a character of  $H_1 \times H_2$ , and  $(\text{Ind}_{H_1}^{G_1} \chi_1)(\text{Ind}_{H_2}^{G_2} \chi_2) = \text{Ind}_{H_1 \times H_2}^{G_1 \times G_2} \chi_1\chi_2$ , where the equality is taken as characters of  $G_1 \times G_2$ . The result follows.  $\square$

**Lemma 6.3.** *Let  $K_1$  and  $K_2$  be distinct normal extensions of  $k$  with Galois group  $G$ . If  $K_1 \cap K_2 = K_1^N \cap K_2^N$  then the Artin  $L$ -function*

$$L(s, \psi_{K_1} \otimes \psi_{K_2})$$

*is entire,  $\mathfrak{q}_{\psi_{K_1} \otimes \psi_{K_2}}$  divides  $\mathfrak{D}_{K_1/k}^{[K_2:k]} \mathfrak{D}_{K_2/k}^{[K_1:k]}$ , and  $N_{k/\mathbb{Q}} \mathfrak{q}_{\psi_{K_1} \otimes \psi_{K_2}}$  divides  $D_{K_1}^{[K_2:k]} D_{K_2}^{[K_1:k]} D_k^{-[K_1:k][K_2:k]}$ .*

*Proof.* Let  $F = K_1 \cap K_2$ . By assumption, both  $K_1^N$  and  $K_2^N$  contain  $F$ , and we may regard the quotients  $\zeta_{K_1}(s) / \zeta_{K_1^N}(s)$  and  $\zeta_{K_2}(s) / \zeta_{K_2^N}(s)$  as  $L$ -functions over  $F$ , say

$$\frac{\zeta_{K_1}(s)}{\zeta_{K_1^N}(s)} =: L(s, \psi_{K_1/F}) \quad \text{and} \quad \frac{\zeta_{K_2}(s)}{\zeta_{K_2^N}(s)} =: L(s, \psi_{K_2/F}).$$

By Lemma 5.1, the characters  $\psi_{K_1/F}$  and  $\psi_{K_2/F}$  are non-negative linear combinations of characters induced from nontrivial one-dimensional representations. Moreover, we have  $\text{Gal}(K_1 K_2 / F) \simeq \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$ , so it follows from Lemma 6.2 that the same holds for the character  $\psi_{K_1/F} \psi_{K_2/F}$ . In particular, the  $L$ -function

$$(6.1) \quad L(s, \psi_{K_1/F} \otimes \psi_{K_2/F}) = \frac{\zeta_{K_1 K_2}(s) \zeta_{K_1^N K_2^N}(s)}{\zeta_{K_1 K_2^N}(s) \zeta_{K_1^N K_2}(s)}$$



is entire. Next, if we set  $G_F = \text{Gal}(K_1K_2/F)$  and  $G_k = \text{Gal}(K_1K_2/k)$ , then the characters  $\psi_{K_1}$  and  $\psi_{K_2}$  of  $G_k$  are induced by the characters  $\psi_{K_1/F}$  and  $\psi_{K_2/F}$  of  $G_F$ . It follows that

$$\begin{aligned} \psi_{K_1}\psi_{K_2} &= \left(\text{Ind}_{G_F}^{G_k}\psi_{K_1/F}\right)\left(\text{Ind}_{G_F}^{G_k}\psi_{K_2/F}\right) \\ &= \text{Ind}_{G_F}^{G_k}\left(\psi_{K_1/F} \cdot \text{Res}_{G_F}^{G_k}\text{Ind}_{G_F}^{G_k}\psi_{K_2/F}\right) = \sum_{\sigma \in G_k/G_F} \text{Ind}_{G_F}^{G_k}\psi_{K_1/F}\psi_{K_2/F}^\sigma, \end{aligned}$$

where  $\psi_{K_2/F}^\sigma$  is the character conjugate to  $\psi_{K_2/F}$  via  $\sigma$ . However, since  $K_2/k$  is Galois and the character  $\psi_{K_2/F}$  is valued in  $\mathbb{Z}$ ,  $\psi_{K_2/F}^\sigma = \psi_{K_2/F}$  for every  $\sigma \in G_k/G_F$ . Thus, we conclude that  $\psi_{K_1}\psi_{K_2} = [F:k]\text{Ind}_{G_F}^{G_k}\psi_{K_1/F}\psi_{K_2/F}$  and  $L(s, \psi_{K_1} \otimes \psi_{K_2}) = L(s, \psi_{K_1/F} \otimes \psi_{K_2/F})^{[F:k]}$ . This shows that it is entire.

To bound the conductor, we rewrite

$$L(s, \psi_{K_1/F} \otimes \psi_{K_2/F}) = \frac{\zeta_{K_1K_2}(s)/\zeta_{K_1K_2^N}(s)}{\zeta_{K_1^N K_2}(s)/\zeta_{K_1^N K_2^N}(s)}.$$

Both the numerator and denominator are entire, by the Artin–Brauer theorem. Since  $\psi_{K_1/F}\psi_{K_2/F}$  is a character of  $G_F$ , it follows that the conductor of  $L(s, \psi_{K_1/F}\psi_{K_2/F})$  divides that of the numerator, which in turn divides  $\mathfrak{D}_{K_1K_2/F}$ , the relative discriminant of the compositum  $K_1K_2/F$ . We have  $\mathfrak{D}_{K_1K_2/F} \mid \mathfrak{D}_{K_1/F}^{[K_2:F]}\mathfrak{D}_{K_2/F}^{[K_1:F]}$ , so the result follows by the conductor-discriminant formula and taking norms to  $k$ . Additionally taking norms to  $\mathbb{Q}$  gives the result on the absolute discriminants.  $\square$

**6.2. Dirichlet series for completely multiplicative functions.** Given an  $n$ -dimensional Artin  $L$ -function  $L(s, \rho)$  over  $k$  and a parameter  $z$  depending at most on  $n$ , we introduce the *completely multiplicative Artin  $L$ -function*

$$(6.2) \quad L_z(s, \rho) := \prod_{N\mathfrak{p} > z} (1 - \lambda_\rho(\mathfrak{p})N\mathfrak{p}^{-s})^{-1} = \sum_{\mathfrak{n}} \frac{a_\rho(\mathfrak{n})}{N\mathfrak{n}^s},$$

where  $z > 0$  is a parameter that we will choose to depend at most on  $n$ . By construction,  $a_\rho(\mathfrak{n})$  is completely multiplicative and satisfies  $a_\rho(\mathfrak{p}) = \lambda_\rho(\mathfrak{p})$  for  $N\mathfrak{p} > z$  while  $a_\rho(\mathfrak{p}) = 0$  for  $N\mathfrak{p} \leq z$ .

**Lemma 6.4.** *Let  $\rho$  be an  $n$ -dimensional Artin representation over  $k$  whose  $L$ -function  $L(s, \rho)$  is entire, and let  $L_z(s, \rho)$  be as in (6.2). If  $z$  is sufficiently large with respect to  $n$ , then there exists an Euler product*

$$H_z(s, \rho) = \prod_{\mathfrak{p}} H_{\mathfrak{p}}(s, \rho)$$

such that if  $\text{Re}(s) > \frac{1}{2}$ , then:

- (1)  $H_z(s, \rho)$  converges uniformly and absolutely,
- (2)  $L_z(s, \rho) = H_z(s, \rho)L(s, \rho)$ ,
- (3)  $H_z(s, \rho)$  is non-vanishing, and
- (4) there exists a constant  $B = B(n) > 0$  such that  $H_z(s, \rho) \ll_n (\text{Re}(s) - \frac{1}{2})^{-Bn}$ .

*Proof.* The claimed identity for  $L_z(s, \rho)$  holds for  $\text{Re}(s) > 1$  once we define

$$H_{\mathfrak{p}}(s, \rho) = \begin{cases} \frac{L_{\mathfrak{p}}(s, \rho)^{-1}}{1 - \lambda_\rho(\mathfrak{p})N\mathfrak{p}^{-s}} & \text{if } N\mathfrak{p} > z, \\ L_{\mathfrak{p}}(s, \rho)^{-1} & \text{otherwise.} \end{cases}$$

Because  $L(s, \rho)$  is assumed to be an entire Artin  $L$ -function and  $z$  depends at most on  $n$ , it follows that

$$\prod_{N\mathfrak{p} \leq z} |H_{\mathfrak{p}}(s, \rho)| \ll_n 1$$

for  $\operatorname{Re}(s) > \frac{1}{2}$ . Since each  $\alpha_{j,\rho}(\mathfrak{p})$  has modulus at most 1, it follows that if  $N\mathfrak{p} \leq z$ , then  $H_{\mathfrak{p}}(s, \rho)$  has no zero in the region  $\operatorname{Re}(s) > \frac{1}{2}$ .

When  $N\mathfrak{p} > z$ , a tedious calculation similar to that in the proof of [19, Proposition 2] shows that there exists a degree  $n - 2$  polynomial  $f$  whose coefficients depend only on the  $\alpha_{j,\rho}(\mathfrak{p})$  such that

$$H_{\mathfrak{p}}(s, \rho) = 1 + \frac{N\mathfrak{p}^{-2s} f(N\mathfrak{p}^{-s})}{1 - \lambda_{\rho}(\mathfrak{p})N\mathfrak{p}^{-s}}.$$

If  $z \geq 4n^2$ , then for  $N\mathfrak{p} > z$  and  $\operatorname{Re}(s) > \frac{1}{2}$ , we have  $|1 - \lambda_{\rho}(\mathfrak{p})N\mathfrak{p}^{-s}| \geq \frac{1}{2}$ . Since each  $\alpha_{j,\rho}(\mathfrak{p})$  has modulus at most one, it follows that  $|f(N\mathfrak{p}^{-s})| \ll_n 1$  when  $\operatorname{Re}(s) > \frac{1}{2}$ . Therefore,

$$H_{\mathfrak{p}}(s, \rho) = 1 + O_n(N\mathfrak{p}^{-2\operatorname{Re}(s)}).$$

If  $z$  is sufficiently large with respect to  $n$ , then we ensure that  $H_{\mathfrak{p}}(s, \rho) \neq 0$  for  $\operatorname{Re}(s) > \frac{1}{2}$ . Furthermore, in this region, there exists a constant  $A(n) > 0$  depending at most on  $n$  such that

$$|H_{\mathfrak{p}}(s, \rho)| \leq (1 + N\mathfrak{p}^{-2\operatorname{Re}(s)})^{A(n)}.$$

The desired result now follows from the bound

$$\prod_{N\mathfrak{p} > z} |H_{\mathfrak{p}}(s, \rho)| \ll_n \zeta(2\operatorname{Re}(s))^{A(n)}, \quad \operatorname{Re}(s) > \frac{1}{2}.$$

□

Let  $K_1, K_2 \in \mathfrak{F}_k^G$ , and let  $N$  be a normal subgroup of  $G$ . We write

$$(6.3) \quad L_{\mathfrak{p}}(s, \psi_K) = \prod_{j=1}^d \left(1 - \frac{\alpha_{j, \psi_K}(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{-1} =: 1 + \sum_{j=1}^{\infty} \frac{\lambda_{\psi_K}(\mathfrak{p}^j)}{N\mathfrak{p}^{js}},$$

where

$$d := |G| - |G|/|N|.$$

We define  $\lambda_{\psi_K}(\mathfrak{n})$  by

$$L(s, \psi_K) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \psi_K) =: \sum_{\mathfrak{n}} \frac{\lambda_{\psi_K}(\mathfrak{n})}{N\mathfrak{n}^s}.$$

In particular,  $\lambda_{\psi_K}(\mathfrak{n})$  is a multiplicative function.

Suppose that  $K_1 \cap K_2 = K_1^N \cap K_2^N$ . Since  $\psi_{K_1} \otimes \psi_{K_2}$  is an Artin representation, there exist complex numbers  $\alpha_{j_1, j_2, K_1 \times K_2}(\mathfrak{p})$  with modulus at most 1 such that

$$L_{\mathfrak{p}}(s, \psi_{K_1} \otimes \psi_{K_2}) = \prod_{j_1=1}^d \prod_{j_2=1}^d \left(1 - \frac{\alpha_{j_1, j_2, K_1 \times K_2}(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{-1} =: 1 + \sum_{j=1}^{\infty} \frac{\lambda_{\psi_{K_1} \otimes \psi_{K_2}}(\mathfrak{p}^j)}{N\mathfrak{p}^{js}}.$$

It follows from our proof of Lemma 6.3 that if  $\mathfrak{p} \nmid \mathfrak{D}_{K_1/k} \mathfrak{D}_{K_2/k}$ , then

$$(6.4) \quad \{\alpha_{j_1, j_2, K_1 \times K_2}(\mathfrak{p}) : 1 \leq j_1, j_2 \leq d\} = \{\alpha_{j_1, K_1}(\mathfrak{p}) \alpha_{j_2, K_2}(\mathfrak{p}) : 1 \leq j_1, j_2 \leq d\}.$$

As with  $L(s, \psi_K)$ , we write

$$(6.5) \quad L(s, \psi_{K_1} \otimes \psi_{K_2}) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \psi_{K_1} \otimes \psi_{K_2}) =: \sum_{\mathfrak{n}} \frac{\lambda_{\psi_{K_1} \otimes \psi_{K_2}}(\mathfrak{n})}{N\mathfrak{n}^s}.$$

Parallel with Lemma 6.4, we provide a convenient factorization of  $L(s, \psi_{K_1} \otimes \psi_{K_2})$  when  $K_1 \cap K_2 = K_1^N \cap K_2^N$ . We define

$$(6.6) \quad L_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) := \sum_{\mathfrak{n}} \frac{a_{\psi_{K_1}}(\mathfrak{n}) a_{\psi_{K_2}}(\mathfrak{n})}{N\mathfrak{n}^s}.$$

Recall that the definitions of the completely multiplicative functions  $a_{\psi_{K_j}}(\mathfrak{n})$  depend on the choice of  $z$  in Lemma 6.4, which we assume is sufficiently large and depending at most on  $d$ .

**Lemma 6.5.** *Suppose that  $K_1 \cap K_2 = K_1^N \cap K_2^N$ . Let  $z$  in Lemma 6.4 be sufficiently large (depending at most on  $d$ ). There exists an Euler product*

$$H_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) = \prod_{\mathfrak{p}} H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})$$

such that if  $\operatorname{Re}(s) > \frac{1}{2}$ , then:

- (1)  $H_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})$  converges uniformly and absolutely,
- (2)  $L_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) = H_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})L(s, \psi_{K_1} \otimes \psi_{K_2})$ , and
- (3) there exists a constant  $B'_d > 0$ , depending at most on  $d$ , such that

$$|H_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})| \ll_d (D_{K_1} D_{K_2})^{\varepsilon/2} (\operatorname{Re}(s) - \frac{1}{2})^{-B'_d}.$$

*Proof.* This is similar to Lemma 6.4. Observe by complete multiplicativity that

$$L_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) = \prod_{\mathfrak{Np} > z} (1 - \lambda_{\psi_{K_1}}(\mathfrak{p})\lambda_{\psi_{K_2}}(\mathfrak{p})\mathfrak{Np}^{-s})^{-1}.$$

We thus compute

$$H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) = \begin{cases} \frac{L_{\mathfrak{p}}(s, \psi_{K_1} \otimes \psi_{K_2})^{-1}}{1 - \lambda_{\psi_{K_1}}(\mathfrak{p})\lambda_{\psi_{K_2}}(\mathfrak{p})\mathfrak{Np}^{-s}} & \text{if } \mathfrak{Np} > z, \\ L_{\mathfrak{p}}(s, \psi_{K_1} \otimes \psi_{K_2})^{-1} & \text{otherwise.} \end{cases}$$

Because  $K_1 \cap K_2 = K_1^N \cap K_2^N$  by hypothesis,  $L(s, \psi_{K_1} \otimes \psi_{K_2})$  is an entire Artin  $L$ -function. Since  $z$  depends at most on  $d$ , it follows that

$$\prod_{\mathfrak{Np} \leq z} |H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})| \ll_d 1, \quad \operatorname{Re}(s) > \frac{1}{2}.$$

We proceed as in [19, Proposition 2] using Lemma 6.3. For all  $\varepsilon > 0$ , we have

$$\left| \prod_{\substack{\mathfrak{Np} > z \\ \mathfrak{p} \text{ ramified}}} H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) \right| \ll_{d, \varepsilon} (D_{K_1} D_{K_2})^{\varepsilon/2}, \quad \operatorname{Re}(s) > \frac{1}{2}.$$

For the other Euler factors, there exists a degree  $d^2 - 2$  polynomial  $f$  whose coefficients depend only on the  $\alpha_{j_1, j_2, \psi_{K_1} \otimes \psi_{K_2}}(\mathfrak{p})$  such that

$$H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) = 1 + \frac{\mathfrak{Np}^{-2s} f(\mathfrak{Np}^{-s})}{1 - \lambda_{\rho}(\mathfrak{p})\mathfrak{Np}^{-s}}.$$

If  $z \geq 4n^4$ , then  $|1 - \lambda_{\rho}(\mathfrak{p})\mathfrak{Np}^{-s}| \geq \frac{1}{2}$  for  $\mathfrak{Np} > z$  and  $\operatorname{Re}(s) > \frac{1}{2}$ . Since  $\alpha_{j_1, j_2, \psi_{K_1} \otimes \psi_{K_2}}(\mathfrak{p})$  has modulus at most one, it follows that  $|f(\mathfrak{Np}^{-s})| \ll_d 1$  when  $\operatorname{Re}(s) > \frac{1}{2}$ . Therefore,

$$H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) = 1 + O_d(\mathfrak{Np}^{-2\operatorname{Re}(s)}), \quad \operatorname{Re}(s) > \frac{1}{2}.$$

Thus, there exists a constant  $B'_d > 0$  depending at most on  $d$  such that

$$|H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})| \leq (1 + \mathfrak{Np}^{-2\operatorname{Re}(s)})^{B'_d}.$$

The desired result now follows from the bound

$$\prod_{\mathfrak{Np} > z} |H_{\mathfrak{p}}^{RS}(s, \psi_{K_1} \otimes \psi_{K_2})| \leq \zeta(2\operatorname{Re}(s))^{B'_d}.$$

for  $\operatorname{Re}(s) > \frac{1}{2}$ . □

**6.3. Partial sums.** Let  $\phi(t)$  be a smooth test function supported in a compact subset of  $[-2, 2]$ , and suppose that  $\phi(t) = 1$  for  $t \in [0, 1]$  and  $\phi(t) \in [0, 1)$  otherwise. The Laplace transform of  $\phi$  is

$$(6.7) \quad \widehat{\phi}(s) = \int_{\mathbb{R}} \phi(y) e^{sy} dy.$$

By construction,  $\widehat{\phi}(s)$  is an entire function of  $s$ , and upon integrating by parts, we find for any integer  $m \geq 0$  that

$$(6.8) \quad \widehat{\phi}(s) \ll_{\phi, m} e^{2|\operatorname{Re}(s)|} |s|^{-m}.$$

Let  $T \geq 1$ . By Fourier inversion, for any  $x > 0$  and any  $c \in \mathbb{R}$ , we have the identity

$$\phi(T \log x) = \frac{1}{2\pi iT} \int_{c-i\infty}^{c+i\infty} \widehat{\phi}(s/T) x^{-s} ds.$$

**Lemma 6.6.** *Let  $T, x \geq 1$  and  $\varepsilon > 0$ . If  $D_{K_1}, D_{K_2} \leq Q$ , then*

$$\left| \sum_{\mathfrak{n}} a_{\psi_{K_1}}(\mathfrak{n}) a_{\psi_{K_2}}(\mathfrak{n}) \phi\left(T \log \frac{N\mathfrak{n}}{x}\right) \right| \ll_{|G|, [k:\mathbb{Q}], \phi, \varepsilon} \begin{cases} \sqrt{x}(\log x)^{B'_d Q^{|G|/2+\varepsilon}} T^{d^2[k:\mathbb{Q}]} & \text{if } K_1 \cap K_2 = K_1^N \cap K_2^N, \\ \frac{1}{T} x(\log x)^{d^2[k:\mathbb{Q}]-1} + \sqrt{x} T^{d^2[k:\mathbb{Q}]} & \text{if } K_1 \cap K_2 \neq K_1^N \cap K_2^N. \end{cases}$$

*Proof.* Let  $\tau_m(n)$  be the  $n$ -th Dirichlet coefficient of  $\zeta(s)^m$ . By the definition of  $a_{\psi_K}(\mathfrak{n})$  and the fact that  $|\alpha_{j, \psi_K}(\mathfrak{p})| \leq 1$ , the sum we want to estimate is bounded in modulus by

$$\begin{aligned} \sum_n \tau_{d^2[k:\mathbb{Q}]}(n) \phi\left(T \log \frac{n}{x}\right) &= \frac{1}{2\pi iT} \int_{3-i\infty}^{3+i\infty} \zeta(s)^{d^2[k:\mathbb{Q}]} \widehat{\phi}(s/T) x^s ds \\ &= \frac{1}{T} \operatorname{Res}_{s=1} \zeta(s)^{d^2[k:\mathbb{Q}]} \widehat{\phi}(s/T) x^s + \frac{1}{2\pi iT} \int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty} \zeta(s)^{d^2[k:\mathbb{Q}]} \widehat{\phi}(s/T) x^s ds \\ &= \frac{x}{T} P_{d^2[k:\mathbb{Q}]}(\log x) + O_{d, [k:\mathbb{Q}]}(\sqrt{x} T^{d^2[k:\mathbb{Q}]}). \end{aligned}$$

Here,  $P_{d^2[k:\mathbb{Q}]}$  is a polynomial of degree  $d^2[k:\mathbb{Q}] - 1$  whose coefficients depend the Laurent series expansion of  $\zeta(s)$  centered at  $s = 1$  and  $\phi^{(j)}(1/T)$  for  $0 \leq j \leq d^2[k:\mathbb{Q}] - 1$ . Since  $T \geq 1$ , it follows from (6.8) that  $P_{d^2[k:\mathbb{Q}]}(\log x) \ll_{d, [k:\mathbb{Q}]} (\log x)^{d^2[k:\mathbb{Q}]-1}$ . This result holds for all  $K_1, K_2 \in \mathfrak{F}_k^G(Q)$ ; in particular, the result when  $K_1 \cap K_2 \neq K_1^N \cap K_2^N$  follows.

Now, assume that  $K_1 \cap K_2 = K_1^N \cap K_2^N$ . Note that in view of the preceding analysis, our proposed bound is trivial if  $x \leq Q^{|G|/2+\varepsilon} T^{d^2[k:\mathbb{Q}]}$ . Thus, we may assume that  $x > Q^{|G|/2+\varepsilon} T^{d^2[k:\mathbb{Q}]}$ . By (6.6) and Lemma 6.5, the sum we want to estimate equals

$$\left| \frac{1}{2\pi iT} \int_{1/2+\frac{1}{\log x}-i\infty}^{1/2+\frac{1}{\log x}+i\infty} H_z^{RS}(s, \psi_{K_1} \otimes \psi_{K_2}) L(s, \psi_{K_1} \otimes \psi_{K_2}) \widehat{\phi}(s/T) x^s ds \right|.$$

Thus, by Lemma 4.1 and (6.8), the integral is

$$\begin{aligned} &\ll_{d, [k:\mathbb{Q}], \phi} \frac{\sqrt{x}}{T} (\log x)^{B'_d Q^{|G|/2+\varepsilon}} \int_{-\infty}^{\infty} (2 + |t|)^{\frac{d^2[k:\mathbb{Q}]}{4}} \left| \widehat{\phi}\left(\frac{1}{T} \left(\frac{1}{2} + \frac{1}{\log x} + it\right)\right) \right| dt \\ &\ll_{d, [k:\mathbb{Q}], \phi} \frac{\sqrt{x}}{T} (\log x)^{B'_d Q^{|G|/2+\varepsilon}} \int_{-\infty}^{\infty} (2 + |t|)^{\frac{d^2[k:\mathbb{Q}]}{4}} \min\left\{1, \frac{T^{d^2[k:\mathbb{Q}]+2}}{(2 + |t|)^{d^2[k:\mathbb{Q}]+2}}\right\} dt, \end{aligned}$$

which is bounded as claimed.  $\square$

**6.4. A large sieve inequality for Artin representations.** We use the results from the preceding subsections to prove a large sieve inequality for the coefficients  $a_{\psi_K}(\mathbf{n})$  of  $L_z(s, \psi_K)$ . We then apply our large sieve to bound the mean value of a certain Dirichlet polynomial which naturally arises in Montgomery's method of detecting zeros of  $L$ -functions [39].

Recall that  $\mathfrak{F}_k^G$  is a set of distinct number fields  $K$  which are Galois extensions of  $k$ , each with Galois group isomorphic to a fixed group  $G$ ,  $\mathfrak{F}_k^G(Q) = \{K \in \mathfrak{F} : D_K \leq Q\}$ , and

$$\mathfrak{m}_k^{G,N}(Q) := \max_{K_1 \in \mathfrak{F}_k^G(Q)} \#\{K_2 \in \mathfrak{F}_k^G(Q) : K_1 \cap K_2 \neq K_1^N \cap K_2^N\}.$$

Let  $b : \mathcal{O}_k \rightarrow \mathbb{C}$  and  $\beta : \mathfrak{F}_k^G(Q) \rightarrow \mathbb{C}$  be functions with  $\ell^2$  norms  $\|b\|_2$  and  $\|\beta\|_2$  defined by

$$\|b\|_2^2 = \sum_{x < \mathbf{Nn} \leq xe^{1/T}} |b(\mathbf{n})|^2, \quad \|\beta\|_2^2 = \sum_{K \in \mathfrak{F}_k^G(Q)} |\beta(K)|^2.$$

**Theorem 6.7.** *Let  $Q, T, x \geq 1$  and  $\varepsilon > 0$ . Define*

$$C(Q, T, x) := \sup_b \sum_{\|b\|_2 \neq 0} \left| \sum_{K \in \mathfrak{F}_k^G(Q)} \sum_{\mathbf{Nn} \in (x, xe^{1/T}]} a_{\psi_K}(\mathbf{n}) b(\mathbf{n}) \right|^2 \bigg/ \sum_{\mathbf{Nn} \in (x, xe^{1/T}]} |b(\mathbf{n})|^2$$

There exists a constant  $B_G'' > 0$ , depending at most on  $|G|$ , such that

$$C(Q, T, x) \ll_{|G|, [k:\mathbb{Q}]} (\log x)^{B_G'' [k:\mathbb{Q}]} \left( \mathfrak{m}_k^{G,N}(Q) \frac{x}{T} + \sqrt{x} Q^{|G|+\varepsilon} T^{|G|^2 [k:\mathbb{Q}]} \right).$$

*Proof.* By the duality principle of finite-dimensional Hilbert spaces,  $C(Q, T, x)$  equals the supremum over all functions  $\beta : \mathfrak{F}_k^G(Q) \rightarrow \mathbb{C}$  such that  $\|\beta\|_2 = 1$  of

$$(6.9) \quad \sum_{\mathbf{Nn} \in (x, xe^{1/T}]} \left| \sum_{K \in \mathfrak{F}_k^G(Q)} a_{\psi_K}(\mathbf{n}) \beta(K) \right|^2.$$

Fix a smooth function  $\phi$  supported on a compact subset of  $[-2, 2]$ , such that  $\phi(T \log \frac{t}{x})$  is a pointwise upper bound for the indicator function of the interval  $(x, xe^{1/T}]$ . Then (6.9) is

$$(6.10) \quad \leq \sum_{\mathbf{n}} \left| \sum_{K \in \mathfrak{F}_k^G(Q)} a_{\psi_K}(\mathbf{n}) \beta(K) \right|^2 \phi\left(T \log \frac{\mathbf{Nn}}{x}\right).$$

Expanding the square and swapping the order of summation, we find that (6.10) equals

$$\sum_{K_1, K_2 \in \mathfrak{F}_k^G(Q)} \beta(K_1) \overline{\beta(K_2)} \sum_{\mathbf{n}} a_{\psi_{K_1}}(\mathbf{n}) \overline{a_{\psi_{K_2}}(\mathbf{n})} \phi\left(T \log \frac{\mathbf{Nn}}{x}\right)$$

Since  $\psi_K$  is real-valued, we have  $a_{\psi_K}(\mathbf{n}) \in \mathbb{R}$ . Since  $|\beta(K_1) \overline{\beta(K_2)}| \leq \frac{1}{2}(|\beta(K_1)|^2 + |\beta(K_2)|^2)$  by the inequality of arithmetic and geometric means and  $\|\beta\|_2 = 1$ , the above display is

$$\leq \max_{K_1 \in \mathfrak{F}_k^G(Q)} \sum_{K_2 \in \mathfrak{F}_k^G(Q)} \left| \sum_{\mathbf{n}} a_{\psi_{K_1}}(\mathbf{n}) a_{\psi_{K_2}}(\mathbf{n}) \phi\left(T \log \frac{\mathbf{Nn}}{x}\right) \right|.$$

By Lemma 6.6, the definition of  $\mathfrak{m}_k^{G,N}(Q)$ , and the fact that  $d \leq |G| - 1$ , there exists a constant  $B_G'' > 0$  (depending at most on  $|G|$ ) such that

$$\ll_{|G|, [k:\mathbb{Q}], \phi, \varepsilon} (\log x)^{B_G'' [k:\mathbb{Q}]} \left( \mathfrak{m}_k^{G,N}(Q) \frac{x}{T} \widehat{\phi}(1/T) + \sqrt{x} Q^{|G|/2+\varepsilon} T^{|G|^2 [k:\mathbb{Q}]} \#\mathfrak{F}_k^G(Q) \right).$$

Once we fix  $\phi$ , we have that  $\widehat{\phi}(1/T) \ll 1$  by (6.7). Since Schmidt [46] proved that

$$\#\mathfrak{F}_k^G(Q) \ll_{|G|, [k:\mathbb{Q}]} (Q/D_k)^{(|G|+2)/4}$$

and  $|G| \geq 2$ , the theorem follows.  $\square$

Let  $\mu_k(\mathbf{n})$  be the  $\mathbf{n}$ -th Dirichlet coefficient of  $\zeta_k(s)^{-1}$ . Then  $\mu_k(\mathbf{n}) = 0$  unless  $\mathbf{n}$  is squarefree, in which case  $\mu_k(\mathbf{n}) = (-1)^{\#\{p|\mathbf{n}\}}$ .

**Corollary 6.8.** *Let  $Q, T \geq 1$ . There exists a constant  $B_G'' > 0$ , depending at most on  $|G|$ , such that if  $X := Q^{2(|G|+\varepsilon)}T^{2|G|^2[k:\mathbb{Q}]}$  and  $\log Y \asymp_{|G|, [k:\mathbb{Q}]} \log X$ , then*

$$\begin{aligned} \sum_{K \in \mathfrak{F}_k^G(Q)} \int_{-T}^T \left| \sum_{X < \mathbf{Nn} \leq X^{\log Y}} \frac{a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})}{\mathbf{Nn}^{1+\frac{1}{\log Y}+iv}} \right|^2 dv &\ll_{|G|, [k:\mathbb{Q}], \varepsilon} \mathbf{m}_k^{G, N}(Q) (\log X)^{B_G''[k:\mathbb{Q}]}, \\ \sum_{K \in \mathfrak{F}_k^G(Q)} \int_{-T}^T \left| \sum_{\mathbf{Nn} \leq X} \frac{a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})}{\mathbf{Nn}^{\frac{1}{2}+\frac{1}{\log Y}+iv}} \right|^2 dv &\ll_{|G|, [k:\mathbb{Q}], \varepsilon} \mathbf{m}_k^{G, N}(Q) X (\log X)^{B_G''[k:\mathbb{Q}]}. \end{aligned}$$

*Proof.* We prove the first bound; the second is proved identically. A formal generalization of a result of Gallagher [27, Theorem 1] to number fields tells us that if  $c(\mathbf{n})$  is a complex-valued function supported on the integral ideals of  $F$  such that  $\sum_{\mathbf{n}} |c(\mathbf{n})| < \infty$ , then

$$\int_{-T}^T \left| \sum_{\mathbf{n}} c(\mathbf{n}) \mathbf{Nn}^{-it} \right|^2 dt \ll T^2 \int_0^\infty \left| \sum_{\mathbf{Nn} \in (x, xe^{1/T}]} c(\mathbf{n}) \right|^2 \frac{dx}{x}.$$

Let  $X = Q^{2|G|}T^{2|G|^2[k:\mathbb{Q}]}$ ,  $\log Y \asymp_{|G|, [k:\mathbb{Q}]} \log X$ , and

$$b(\mathbf{n}) = \begin{cases} \mu_k(\mathbf{n}) \mathbf{Nn}^{-1-\frac{1}{\log Y}} & \text{if } \mathbf{Nn} \in [X, X^{\log Y}], \\ 0 & \text{otherwise.} \end{cases}$$

If  $c(\mathbf{n}) = a_{\psi_K}(\mathbf{n})b(\mathbf{n})$ , then

$$(6.11) \quad \sum_{K \in \mathfrak{F}_k^G(Q)} \int_{-T}^T \left| \sum_{\mathbf{Nn} \in (X, X^{\log Y}]} \frac{a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})}{\mathbf{Nn}^{1+\frac{1}{\log Y}+iv}} \right|^2 dv \ll T^2 \int_0^\infty \sum_{K \in \mathfrak{F}_k^G(Q)} \left| \sum_{\mathbf{Nn} \in (x, xe^{1/T}]} a_{\psi_K}(\mathbf{n})b(\mathbf{n}) \right|^2 \frac{dx}{x}.$$

We apply Theorem 6.7 and bound the above display by

$$\ll_{|G|, [k:\mathbb{Q}], \varepsilon} \mathbf{m}_k^{G, N}(Q) \sum_{\mathbf{n}} |b(\mathbf{n})|^2 \mathbf{Nn} \left( (\log \mathbf{Nn})^{B_G''[k:\mathbb{Q}]} + \frac{X}{\mathbf{Nn}^{1/2}} \right).$$

Since  $\log Y \asymp \log X$ , Lemma 2.4 of [56] implies that (6.11) is bounded by  $\mathbf{m}_k^{G, N}(Q)$  times

$$(\log X)^{B_G''[k:\mathbb{Q}]} \sum_{\mathbf{Nn} \in [X, X^{\log Y}]} \frac{1}{\mathbf{Nn}} \ll_{|G|, [k:\mathbb{Q}]} (\log X)^{B_G''[k:\mathbb{Q}]+1} \operatorname{Res}_{s=1} \zeta_k(s).$$

The residue is  $\ll_{[k:\mathbb{Q}]} (\log D_k)^{[k:\mathbb{Q}]-1}$  [35, Theorem 1], and the result follows.  $\square$

**6.5. Proof of Theorem 6.1.** Let  $K \in \mathfrak{F}_k^G(Q)$ . The bound

$$\#\{\beta + i\gamma: \beta \geq 0, |\gamma - t| \leq 1, L(\beta + i\gamma, \psi_K) = 0\} \ll_{|G|, [k:\mathbb{Q}]} \log Q + \log(|t| + 2)$$

holds for all  $t \in \mathbb{R}$  by proceeding as in [30, Proposition 5.7]. Given  $\sigma \in (\frac{1}{2}, 1)$ , we decompose the rectangle  $[\sigma, 1] \times [-T, T]$  into disjoint boxes of the shape  $[\sigma, 1] \times [u, u + 2(\log X)^2]$ , where  $X$  is as in Corollary 6.8. Each of these boxes contains  $\ll_{|G|, [k:\mathbb{Q}]} (\log QT)^3$  zeros. Writing  $\eta_{\psi_K}$  for the number of smaller boxes which contain at least one zero of  $L(s, \psi_K)$ , then

$$N_{K/K^N}(\sigma, T) \ll_{|G|, [k:\mathbb{Q}]} (\log QT)^3 \eta_{\psi_K}.$$

Since  $L(s, \psi_K)$  is entire, it follows from Lemma 6.4 if  $\gamma \in \mathbb{R}$  and  $\beta > \frac{1}{2}$ , then  $\beta + i\gamma$  is a zero of  $L(s, \psi_K)$  if and only if it is a zero of  $L_z(s, \psi_K)$ . Thus, we will detect the zeros of  $L_z(s, \psi_K)$ . Since

the coefficients  $a_{\psi_K}(\mathbf{n})$  are completely multiplicative, the  $\mathbf{n}$ -th Dirichlet coefficient of  $L_z(s, \psi_K)^{-1}$  is  $a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})$ . With  $X$  as in Corollary 6.8, we define

$$Y := X^{\frac{2}{3-2\sigma}}, \quad M_X(s, \psi_K) := \sum_{\mathbf{Nn} \leq X} \frac{a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})}{\mathbf{Nn}^s}.$$

A straightforward computation shows that if  $\beta + i\gamma$  is a nontrivial zero of  $L(s, \psi_K)$  with  $\beta \geq \sigma \geq \frac{1}{2} + (\log Y)^{-1}$ , then

$$\begin{aligned} e^{-1/Y} &= \frac{1}{2\pi i} \int_{1-\beta+\frac{1}{\log Y}-i\infty}^{1-\beta+\frac{1}{\log Y}+i\infty} (1 - L_z(\beta + i\gamma + w, \psi_K)M_X(\beta + i\gamma + w, \psi_K))\Gamma(w)Y^w dw \\ &\quad + \frac{1}{2\pi i} \int_{\frac{1}{2}-\beta+\frac{1}{\log Y}-i\infty}^{\frac{1}{2}-\beta+\frac{1}{\log Y}+i\infty} L_z(\beta + i\gamma + w, \psi_K)M_X(\beta + i\gamma + w, \psi_K)\Gamma(w)Y^w dw. \end{aligned}$$

If such a zero exists, then at least one of the two integrals above must be large since  $e^{-1/Y} = 1 + O(Y^{-1})$ . As in Montgomery's method [39] for Dirichlet characters, one uses Stirling's formula to show that

$$\begin{aligned} \eta_{\psi_K} &\ll_{|G|, [k; \mathbb{Q}]} Y^{2(1-\sigma)}(\log Y)^2 \int_{-T}^T |1 - L_z(1 + \frac{1}{\log Y} + iv, \psi_K)M_X(1 + \frac{1}{\log Y} + iv, \psi_K)|^2 dv \\ &\quad + Y^{\frac{1}{2}-\sigma} \int_{-T}^T |L_z(\frac{1}{2} + \frac{1}{\log Y} + iv, \psi_K)M_X(\frac{1}{2} + \frac{1}{\log Y} + iv, \psi_K)| dv \\ &\ll_{|G|, [k; \mathbb{Q}]} Y^{2(1-\sigma)}(\log Y)^2 \int_{-T}^T |1 - L_z(1 + \frac{1}{\log Y} + iv, \psi_K)M_X(1 + \frac{1}{\log Y} + iv, \psi_K)|^2 dv \\ &\quad + Y^{\frac{1}{2}-\sigma} \int_{-T}^T |L_z(\frac{1}{2} + \frac{1}{\log Y} + iv, \psi_K)|^2 dv + Y^{\frac{1}{2}-\sigma} \int_{-T}^T |M_X(\frac{1}{2} + \frac{1}{\log Y} + iv, \psi_K)|^2 dv. \end{aligned}$$

The second bound follows from the inequality of arithmetic and geometric means.

Lemmas 4.1 and 6.4 imply that

$$\int_{-T}^T |L_z(\frac{1}{2} + \frac{1}{\log Y} + iv, \psi_K)|^2 dv \ll_{|G|, [k; \mathbb{Q}]} Q^{1/2} T^{1+d[k; \mathbb{Q}]/2} (\log Y)^{2A_d}.$$

Furthermore, by Lemmas 4.1 and 6.4 again, if we temporarily write  $L = L_z(1 + \frac{1}{\log Y} + iv, \psi_K)$  and  $M_X = M_X(1 + \frac{1}{\log Y} + iv, \psi_K)$ , then we have

$$\begin{aligned} |1 - LM_X|^2 &= |L|^2 |L^{-1} - M_X|^2 \\ &\leq |L|^2 (|L^{-1} - M_{X^{\log Y}}| + |M_{X^{\log Y}} - M_X|)^2 \\ &\ll_{|G|, [k; \mathbb{Q}]} (\log QT)^{d[k; \mathbb{Q}]} (|L^{-1} - M_{X^{\log Y}}|^2 + |M_{X^{\log Y}} - M_X|^2). \end{aligned}$$

A straightforward partial summation shows that  $|L^{-1} - M_{X^{\log Y}}|^2 \ll_{|G|, [k; \mathbb{Q}]} 1$ , and thus

$$\begin{aligned} N_{K/K^N}(\sigma, T) &\ll_{|G|, [k; \mathbb{Q}]} \left( Y^{\frac{1}{2}-\sigma} \left[ Q^{1/2} T^{1+|G|[k; \mathbb{Q}]/2} (\log QT)^{2A_d} + \int_{-T}^T \left| \sum_{\mathbf{Nn} \leq X} \frac{a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})}{\mathbf{Nn}^{\frac{1}{2} + \frac{1}{\log Y} + iv}} \right|^2 dv \right] \right. \\ &\quad \left. + Y^{2(1-\sigma)} (\log QT)^{|G|[k; \mathbb{Q}]+2} \left[ 1 + \int_{-T}^T \left| \sum_{X < \mathbf{Nn} \leq X^{\log Y}} \frac{a_{\psi_K}(\mathbf{n})\mu_k(\mathbf{n})}{\mathbf{Nn}^{1 + \frac{1}{\log Y} + iv}} \right|^2 \right] \right) (\log QT)^3. \end{aligned}$$

Finally, we sum over  $K \in \mathfrak{F}_k^G(Q)$  and apply Corollary 6.8. By the Schmidt bound  $\#\mathfrak{F}_k^G(Q) \ll_{|G|, [k; \mathbb{Q}]} Q^{(|G|+2)/4}$  and our choices of  $X$  and  $Y$ , we find that there exists a constant  $C_G > 0$ , depending at

most on  $G$ , such that

$$\sum_{K \in \mathfrak{F}_k^G(Q)} N_{K/K^N}(\sigma, T) \ll_{[k:\mathbb{Q}], |G|, \varepsilon} \mathfrak{m}_k^{G,N}(Q) (\log QT)^{C_G [k:\mathbb{Q}]} (Y^{\frac{1}{2}-\sigma} X + Y^{2(1-\sigma)}).$$

which is bounded as desired when  $\sigma > \frac{1}{2}$ . For  $\sigma < \frac{1}{2}$ , our results are trivial in view of the generalized Riemann–von Mangoldt asymptotic for the count of all zeros up to height  $T$  (see [30, Theorem 5.8]).

## 7. PROOFS OF THEOREMS 3.1 AND 3.7

We begin by recalling the zero-free region of Lagarias and Odlyzko [33, Section 8]:  $\zeta_K(s)$  does not vanish in the region

$$(7.1) \quad \operatorname{Re}(s) \geq 1 - \frac{c_8}{\log(D_K(|\operatorname{Im}(s)| + 3)^{[k:\mathbb{Q}]})},$$

apart from the possibility of a single real simple zero. Since  $\zeta_K(s)/\zeta_{K^N}(s)$  is entire, it follows that  $\zeta_K(s)/\zeta_{K^N}(s) \neq 0$  in the region (7.1), apart from the possibility of a single real simple zero.

We will use Theorem 6.1 to prove Theorem 3.1, showing that for all  $K \in \mathfrak{F}_k^G(Q)$  apart from a small exceptional subset, the ratio of Dedekind zeta functions  $\zeta_K(s)/\zeta_{K^N}(s)$  has a much stronger zero-free region than (7.1). In particular, since we may assume that  $C_G \geq 6$  in Theorem 6.1, we may choose  $\varepsilon = \frac{1}{3} - \frac{5}{3C_G [k:\mathbb{Q}]}$  in Theorem 6.1, which leads to

$$(7.2) \quad \sum_{K \in \mathfrak{F}_k^G(Q)} N_{K/K^N}(\sigma, T) \ll_{|G|, [k:\mathbb{Q}]} \mathfrak{m}_k^{G,N}(Q) (QT^{|G|[k:\mathbb{Q}]})^{\left(\frac{25}{3} - \frac{5}{3C_G [k:\mathbb{Q}]}\right)|G|(1-\sigma)} (\log QT)^{C_G [k:\mathbb{Q}]}$$

*Proof of Theorem 3.1.* Let  $0 < \varepsilon < 1$ , and define  $\delta := \varepsilon/(20|G|)$ . For each integer  $2 \leq j \leq Q^{\varepsilon/(6C_G [k:\mathbb{Q}])} + 1$ , we iteratively apply (7.2) with

$$T = T_j = e^j - 3, \quad \sigma = \sigma_j := 1 - \frac{2\delta \log Q}{\log Q + |G|[k:\mathbb{Q}] \log(T_j + 3)},$$

discarding  $O_{|G|, [k:\mathbb{Q}], \varepsilon}(\mathfrak{m}_k^{G,N}(Q) Q^{2\left(\frac{25}{3} - \frac{5}{3C_G [k:\mathbb{Q}]}\right)\delta|G| + \frac{\varepsilon}{6}})$  exceptions at most  $Q^{\frac{\varepsilon}{6C_G [k:\mathbb{Q}]}}$  times. This dyadically builds a zero-free region for all except  $O_{|G|, [k:\mathbb{Q}], \varepsilon}(\mathfrak{m}_k^{G,N}(Q) Q^\varepsilon)$  of the fields  $K \in \mathfrak{F}_k^G(Q)$ . Thus, for all except  $O_{|G|, [k:\mathbb{Q}], \varepsilon}(\mathfrak{m}_k^{G,N}(Q) Q^\varepsilon)$  fields  $K \in \mathfrak{F}_k^G(Q)$ , the ratio  $\zeta_K(s)/\zeta_{K^N}(s)$  is holomorphic and non-vanishing in the region

$$\operatorname{Re}(s) \geq 1 - \frac{2\delta \log Q}{\log Q + |G|[k:\mathbb{Q}] \log(|\operatorname{Im}(s)| + 3)}, \quad |\operatorname{Im}(s)| \leq \exp(Q^{\varepsilon/(6C_G [k:\mathbb{Q}])}).$$

Since  $D_K \leq Q$ , we may replace the above region with the more restrictive region

$$(7.3) \quad \operatorname{Re}(s) \geq 1 - \frac{2\delta \log D_K}{\log D_K + |G|[k:\mathbb{Q}] \log(|\operatorname{Im}(s)| + 3)}, \quad |\operatorname{Im}(s)| \leq \exp(D_K^{\varepsilon/(6C_G [k:\mathbb{Q}])}).$$

For  $|\operatorname{Im}(s)| > \exp(D_K^{\varepsilon/(6C_G [k:\mathbb{Q}])})$ , we have the zero-free region (7.1). The theorem follows once we combine (7.3) with (7.1).  $\square$

**Proposition 7.1.** *Let  $K/k$  be a Galois extension of number fields. Assume  $\chi$  is a character of  $G = \operatorname{Gal}(K/k)$  which is the induction of a non-trivial 1-dimensional cyclic character of a subgroup of  $G$ . Let  $0 < \varepsilon < 1$ , and let the region  $\Omega_K(\varepsilon)$  be given by (3.5). If  $D_K$  is sufficiently large with respect to  $[k:\mathbb{Q}]$ ,  $|G|$ , and  $\varepsilon$ , and  $L(s, \chi)$  does not vanish in the region  $\Omega_K(\varepsilon)$ , then there exists an effectively computable constant  $c_1 = c_1(|G|, [k:\mathbb{Q}], \varepsilon) > 0$  such that*

$$\left| \sum_{N\mathfrak{p} \leq x} \chi(\mathfrak{p}) \right| \ll_{|G|, [k:\mathbb{Q}], \varepsilon} x \exp(-c_1 \sqrt{\log x}), \quad x \geq (\log D_K)^{81|G|/\varepsilon}.$$



*Proof of Theorem 3.7 assuming Proposition 7.1.* Since we have proved Theorems 3.1 and 3.3, it suffices for us to prove (3.10) using Proposition 7.1. Suppose that  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in the region  $\Omega_K(\varepsilon)$  and that  $\rho$  is an irreducible Artin representation of  $K/k$  whose kernel does not contain  $N$ . Assuming Conjecture 3.2, there exist rational constants  $c_\chi(\rho)$  such that

$$L(s, \rho) = \prod_{H \subseteq G} \prod_{\substack{\chi \in \text{Irr}(H) \\ \dim \chi = 1 \\ \ker \chi \not\supseteq H \cap N}} L(s, \text{Ind}_H^G \chi)^{c_\chi(\rho)},$$

the inner summation running over 1-dimensional characters of subgroups  $H$  whose kernel does not contain  $H \cap N$ . Note that  $c_\chi(\rho) \ll_G 1$  for each  $\chi$ . Taking logarithmic derivatives, it follows for all  $x \geq 3$  that

$$(7.4) \quad \sum_{\mathbf{Nn} \leq x} \chi_\rho(\mathbf{n}) \Lambda_k(\mathbf{n}) = \sum_{H \subseteq G} \sum_{\substack{\chi \in \text{Irr}(H) \\ \dim \chi = 1 \\ \ker \chi \not\supseteq H \cap N}} c_\chi(\rho) \sum_{\mathbf{Nn} \leq x} (\text{Ind}_H^G \chi)(\mathbf{n}) \Lambda_k(\mathbf{n}),$$

where  $\Lambda_k(\mathbf{p}^j) = \log \mathbf{Np}$  and  $\Lambda_k(\mathbf{n}) = 0$  otherwise. For each  $\chi$  in the righthand sum, Lemma 5.5 implies that  $L(s, \text{Ind}_H^G \chi)$  is non-vanishing in  $\Omega_K(\varepsilon)$ . The desired result now follows by Proposition 7.1, partial summation, and (7.4).  $\square$

To prove Proposition 7.1, we use the following smooth function to count prime ideals  $\mathbf{p}$  with  $\mathbf{Np} \leq x$ .

**Lemma 7.2.** *For all  $x \geq 3$  and  $\Delta \in (0, 1/4)$ , there exists a continuous real-variable function  $f(t) = f_{x, \Delta}(t)$  such that:*

- (1)  $0 \leq f(t) \leq 1$  for all  $t \in \mathbb{R}$ , and  $f(t) \equiv 1$  for  $\frac{1}{2} \leq t \leq 1$ .
- (2) The support of  $f$  is contained in the interval  $[\frac{1}{2} - \frac{\Delta}{\log x}, 1 + \frac{\Delta}{\log x}]$ .
- (3) Its Laplace transform  $F(z) = \int_{\mathbb{R}} f(t) e^{-zt} dt$  is entire and is given by

$$F(z) = e^{-(1 + \frac{\Delta}{\log x})z} \cdot \left( \frac{1 - e^{(\frac{1}{2} + \frac{\Delta}{\log x})z}}{-z} \right) \left( \frac{1 - e^{\frac{\Delta z}{2 \log x}}}{-\frac{\Delta z}{2 \log x}} \right)^2.$$

- (4) Let  $s = \sigma + it$ ,  $\sigma > 0$ , and  $t \in \mathbb{R}$ . Then

$$|F(-s \log x)| \leq e^{\sigma \Delta} x^\sigma \min \left\{ 1, \frac{1 + x^{-\sigma/2}}{|s| \log x} \left( \frac{4}{\Delta |s|} \right)^2 \right\}.$$

Moreover,  $1/2 < F(0) < 3/4$  and

$$(7.5) \quad F(-\log x) = \frac{x}{\log x} + O\left(\frac{\Delta x + x^{1/2}}{\log x}\right).$$

- (5) Let  $s = -\frac{1}{2} + it$  with  $t \in \mathbb{R}$ . Then

$$|F(-s \log x)| \leq \frac{5x^{-1/4}}{\log x} \left( \frac{4}{\Delta} \right)^2 (1/4 + t^2)^{-1}.$$

*Proof.* This lemma and its proof can be found by taking  $\ell = 2$  in [53, Lemma 2.2].  $\square$

Our next lemma uses the weight function constructed in Lemma 7.2 to establish a preliminary form of the prime number theorem for  $L(s, \chi)$ . Define  $\delta = \varepsilon/(20|G|)$ . For convenience, we rewrite the zero-free region (3.5) as

$$\Omega_K(\varepsilon) := \{s \in \mathbb{C} : \text{Re}(s) \geq 1 - \omega_K(|\text{Im}(s)| + 3)\},$$

where for  $t \geq 3$  we define

$$(7.6) \quad \omega_K(t) = \omega_K(t; \varepsilon) = \begin{cases} \frac{2\delta \log D_K}{\log D_K + [k:\mathbb{Q}] \log t} & \text{if } \log 3 \leq t \leq D_K^{\varepsilon/(6C_G[k:\mathbb{Q}])}, \\ \frac{c_8}{\log D_K + [G][k:\mathbb{Q}] \log t} & \text{if } \log t > D_K^{\varepsilon/(6C_G[k:\mathbb{Q}])} \end{cases}$$

**Lemma 7.3.** *Recall the notation and hypotheses of Proposition 7.1. Let  $\omega_K(t) = \omega_K(t; \varepsilon)$  be as in (7.6), and define*

$$\eta_K(x) = \inf_{t \geq 3} (\omega_K(t) \log x + \log t).$$

If  $L(s, \chi)$  does not vanish in the region  $\Omega_K(\varepsilon)$ , then

$$\left| \sum_{\mathfrak{N}\mathfrak{p} \leq x} \chi(\mathfrak{p}) \right| \ll_{[K:\mathbb{Q}]} \frac{x}{\log x} e^{-\eta_K(x)/8} \log(eD_K) + \frac{x^{3/4}}{\log x}, \quad x \geq \max\{3, (\log D_K)^4\}.$$

*Proof.* To start, we record a basic observation that will be often used:

$$(7.7) \quad [K : \mathbb{Q}] \ll \log D_K \leq x^{1/4}.$$

The first bound is Minkowski's inequality; the second bound holds by assumption.

Select the weight function  $f(\cdot) = f_{x, \Delta}(\cdot)$  from Lemma 7.2 for any  $x \geq 3$  and with

$$\Delta = x^{-1/4} + \min\{\frac{1}{8}, 8e^{-\eta_K(x)/4}\}.$$

A calculation identical to that in [53, Lemma 2.3] shows that

$$\sum_{\mathfrak{N}\mathfrak{n} \leq x} \Lambda_k(\mathfrak{n}) \chi(\mathfrak{n}) = \sum_{\mathfrak{n}} \Lambda_k(\mathfrak{n}) \chi(\mathfrak{n}) f\left(\frac{\log \mathfrak{N}\mathfrak{n}}{\log x}\right) + O_{[K:\mathbb{Q}]}(\sqrt{x} + \Delta x).$$

Since  $\chi$  is the induction of a non-trivial 1-dimensional character,  $L(s, \chi)$  is a Hecke  $L$ -function and hence entire. Thus, by Mellin inversion, we have

$$\begin{aligned} & \sum_{\mathfrak{N}\mathfrak{n} \leq x} \Lambda_k(\mathfrak{n}) \chi(\mathfrak{n}) \\ &= \frac{\log x}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{L'}{L}(s, \chi) F(-s \log x) ds + O_{[K:\mathbb{Q}]}(\sqrt{x} + \Delta x) \\ &= \log x \sum_{\rho} F(-\rho \log x) + \frac{\log x}{2\pi i} \int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} -\frac{L'}{L}(s, \chi) F(-s \log x) ds + O_{[K:\mathbb{Q}]}(\sqrt{x} + \Delta x), \end{aligned}$$

where  $\rho$  ranges over the nontrivial zeros of  $L(s, \chi)$ . The standard bound

$$-\frac{L'}{L}(s, \chi) \ll_{[K:\mathbb{Q}]} \log(D_K(|\operatorname{Im}(s)| + 3)), \quad \operatorname{Re}(s) = -\frac{1}{2}$$

and the lower bound  $\Delta \geq x^{-1/4}$  imply via Lemma 7.2(5) that

$$\sum_{\mathfrak{n}} \Lambda_k(\mathfrak{n}) \chi(\mathfrak{n}) = \log x \sum_{\rho} F(-\rho \log x) + O_{[K:\mathbb{Q}]}(\sqrt{x} + \Delta x).$$

By Lemma 7.2(4), we have

$$\log x \sum_{|\rho| \leq 1/4} F(-\rho \log x) \ll \log x \sum_{|\rho| \leq 1/4} x^{1/4} \ll_{[K:\mathbb{Q}]} x^{1/4} (\log x) \log D_K \ll_{[K:\mathbb{Q}]} \sqrt{x} \log x$$

by (7.7). For the zeros  $\rho = \beta + i\gamma$  of  $L(s, \chi)$  with  $|\rho| \geq 1/4$ , observe that our assumed zero-free region for  $L(s, \chi)$  implies that

$$\frac{x^{-(1-\beta)}}{(|\gamma| + 3)} = e^{-((1-\beta) \log x + \log(|\gamma| + 3))} \leq e^{-\eta_K(x)}.$$

by definition of  $\eta_K$ . Hence Lemma 7.2(4) and our choice of  $\Delta$  yields the estimate

$$(\log x)|F(-\rho \log x)| \ll \frac{x^\beta}{(|\gamma| + 3)} \cdot \frac{\Delta^{-2}}{(|\gamma| + 3)^2} \ll xe^{-\eta_K(x)} \cdot \frac{e^{\eta_K(x)/2}}{(|\gamma| + 3)^2}$$

for  $|\rho| \geq 1/4$ . Thus, summing over all zeros  $\rho$  of  $L(s, \chi)$ , it follows that

$$\log x \sum_{\rho} |F(-\rho \log x)| \ll_{[K:\mathbb{Q}]} xe^{-\eta_K(x)/2} \sum_{\rho} \frac{1}{(|\gamma| + 3)^2} + \sqrt{x} \log x.$$

Since  $L(s, \chi)$  is a Hecke  $L$ -function with  $C(\chi) \ll_{[K:\mathbb{Q}]} D_K$ , it follows by standard estimates for it zeros [53, Lemma 2.5] and (7.7) that the above expression is

$$\begin{aligned} &\ll_{[K:\mathbb{Q}]} xe^{-\eta_K(x)/2} \sum_{T=1}^{\infty} \sum_{T-1 \leq |\operatorname{Im}(\rho)| \leq T} \frac{\log D_K + \log(T+3)}{T^2} + \sqrt{x} \log x \\ &\ll_{[K:\mathbb{Q}]} xe^{-\eta_K(x)/2} \log(eD_K) + \sqrt{x} \log x. \end{aligned}$$

By our choice of  $\Delta$  and (7.7), this implies that

$$(7.8) \quad \left| \sum_{\mathbf{Nn} \leq x} \Lambda_k(\mathbf{n}) \chi(\mathbf{n}) \right| \ll_{[K:\mathbb{Q}]} xe^{-\eta_K(x)/4} \log(eD_K) + x^{3/4}.$$

The contribution from the prime powers and ramified primes is  $O(\sqrt{x} + \log(eD_K))$ , so by partial summation [53, Lemma 2.1 and Equation 5.3], it follows that

$$\left| \sum_{\mathbf{Np} \leq x} \chi(\mathbf{p}) \right| \ll_{[K:\mathbb{Q}]} \frac{x}{\log x} \sup_{\sqrt{x} \leq y \leq x} (e^{-\eta_K(y)/4}) \log(eD_K) + \frac{x^{3/4}}{\log x} + \log(eD_K).$$

From the definition of  $\eta_K$ , one can see that  $\eta_K(y)$  is an increasing function of  $y$  and also  $\eta_K(x^{1/2}) \geq \frac{1}{2}\eta_K(x)$ . Hence, as  $\log D_K \leq x^{1/4}$ , we conclude the desired result.  $\square$

**Lemma 7.4.** *Recall the notation and hypotheses of Proposition 7.1. There exist effectively computable constants  $c_1 = c_1(|G|, [k:\mathbb{Q}], \varepsilon) > 0$  and  $c_{12} = c_{12}(|G|, [k:\mathbb{Q}], \varepsilon) > 0$  such that if  $D_K \geq c_{12}$  is sufficiently large with respect to  $|G|$ ,  $[k:\mathbb{Q}]$ , and  $\varepsilon$ , and  $x \geq (\log D_K)^{81|G|/\varepsilon}$ , then*

$$\frac{\log(eD_K)}{\log x} e^{-\eta_K(x)/8} \ll_{|G|, [k:\mathbb{Q}], \varepsilon} \exp(-c_1 \sqrt{\log x}).$$

*Proof.* For notational compactness, we introduce  $\varepsilon_0 = \varepsilon/(6C_G[k:\mathbb{Q}])$ . By the definition of  $\eta_K(x)$  and (7.6), we have that

$$\eta_K(x) \geq \min \left\{ \inf_{0 \leq u \leq D_K^{\varepsilon_0}} \left( \frac{\varepsilon(\log D_K) \log x}{10|G|(\log D_K + [k:\mathbb{Q}]u)} + u \right), \inf_{u \geq D_K^{\varepsilon_0}} \left( \frac{c_8 \log x}{\log D_K + |G|[k:\mathbb{Q}]u} + u \right) \right\}.$$

Define

$$\phi_1(u, x) := \frac{\varepsilon(\log D_K) \log x}{10|G|(\log D_K + [k:\mathbb{Q}]u)} + u, \quad \phi_2(u, x) := \frac{c_8 \log x}{\log D_K + |G|[k:\mathbb{Q}]u} + u.$$

Notice that the global infimum of  $\phi_1(u, x)$  over  $u \in (-\log D_K)/[k:\mathbb{Q}], \infty)$  is at

$$u = u_1 := \sqrt{\frac{\varepsilon \log D_K}{10|G|[k:\mathbb{Q}]} \log x} - \frac{\log D_K}{[k:\mathbb{Q}]}.$$

Thus, the value of  $u \in [0, D_K^{\varepsilon_0}]$  at which  $\phi_1(u, x)$  attains its infimum lies in  $\{0, u_1, D_K^{\varepsilon_0}\} \cap [0, D_K^{\varepsilon_0}]$ . Observe that  $u_1 \geq 0$  if and only if  $x \geq D_K^{(10|G|)/(\varepsilon[k:\mathbb{Q}])}$ , in which case  $\phi_1(u_1, x) \leq \phi_1(D_K^{\varepsilon_0}, x)$  because

$u_1$  is the global minimum. For this range of  $x$ , we compute

$$\phi_1(u_1, x) = \sqrt{\frac{2\varepsilon \log D_K}{5|G|[k:\mathbb{Q}]} \log x - \frac{\log D_K}{[k:\mathbb{Q}]}} \geq \sqrt{\frac{\varepsilon \log D_K}{10|G|[k:\mathbb{Q}]} \log x}.$$

We also compute that  $\phi_1(0, x) \geq \phi_1(D^{\varepsilon_0}, x)$  if and only if

$$x \geq D_K^{\frac{10|G|}{\varepsilon[k:\mathbb{Q}]}} e^{\frac{10|G|D_K^{\varepsilon_0}}{\varepsilon}},$$

a range in which we already established that  $u_1 \geq 0$ . Therefore, since  $\phi_1(0, x) = \frac{\varepsilon}{10|G|} \log x$ , we conclude that

$$\inf_{0 \leq u \leq D_K^{\varepsilon_0}} \phi_1(u, x) \geq \min \left\{ \frac{\varepsilon}{10|G|} \log x, \sqrt{\frac{\varepsilon \log D_K}{10|G|[k:\mathbb{Q}]} \log x} \right\}.$$

Next, notice that the global minimum of  $\phi_2(u, x)$  over  $u \in (-(\log D_K)/[k:\mathbb{Q}], \infty)$  is at

$$u_2 = \sqrt{\frac{c_8 \log x}{|G|[k:\mathbb{Q}]} - \frac{\log D_K}{|G|[k:\mathbb{Q}]}}.$$

Thus,  $\phi_2(u, x)$  attains its infimum over  $u \geq D_K^{\varepsilon_0}$  at  $u = \max\{D_K^{\varepsilon_0}, u_2\}$ . It follows from a straightforward calculation that

$$\inf_{u \geq D_K^{\varepsilon_0}} \phi_2(u, x) \geq \sqrt{\frac{c_8 \log x}{|G|[k:\mathbb{Q}]} + D_K^{\varepsilon_0}}.$$

We conclude from the analysis for  $u \leq D_K^{\varepsilon_0}$  and  $u \geq D_K^{\varepsilon_0}$  that if  $D_K \geq c_{12}$ , then

$$\begin{aligned} & \frac{\log(eD_K)}{\log x} e^{-\eta_K(x)/8} \\ & \leq \frac{\log(eD_K)}{\log x} \exp \left( -\frac{1}{8} \min \left\{ \frac{\varepsilon \log x}{10|G|}, \sqrt{\frac{\varepsilon \log D_K}{10|G|[k:\mathbb{Q}]} \log x}, \sqrt{\frac{c_8 \log x}{|G|[k:\mathbb{Q}]} + D_K^{\varepsilon_0}} \right\} \right). \end{aligned}$$

The desired result follows once we ensure that  $x \geq (\log D_K)^{8|G|/\varepsilon}$ .  $\square$

*Proof of Proposition 7.1.* This follows from Lemmas 7.3 and 7.4 with the same constant  $c_1$ .  $\square$

## 8. APPLICATION TO PRIME DEGREE EXTENSIONS

In this section, we show how our results apply to the family of prime degree  $p$  extensions of a number field  $k$ . The normal closures  $K/k$  of such fields have Galois groups  $G$  that are transitive subgroups of the symmetric group  $S_p$ . The properties of such groups are well understood. For example, they must be primitive permutation groups, and are thus subject to many of the results in Dixon and Mortimer [14]. More than this, such groups are *classified*; see Lemma 8.2 below. However, as the properties of such groups are of vital importance to many of our applications, we begin by providing a succinct but complete proof of the classical fact that such groups always have a unique minimal normal subgroup, and that the fixed field  $K^N$  of this normal subgroup is linearly disjoint from the degree  $p$  extension that we started with.

**Lemma 8.1.** *If  $G \subseteq S_p$  is a transitive subgroup, then  $G$  has a unique minimal nontrivial normal subgroup  $N$ . Also, if  $H \subseteq G$  is the stabilizer of a point, then  $[H : H \cap N] = [G : N]$ .*

*Proof.* Since  $G$  is a transitive group of prime degree, it is primitive. Consequently, any nontrivial normal subgroup acts transitively, and thus has an element of order  $p$ . If  $G$  had two minimal normal subgroups, say  $N_1$  and  $N_2$ , then  $N_1$  and  $N_2$  commute, since any commutator lies in the intersection  $N_1 \cap N_2$ , which is trivial since  $N_1$  and  $N_2$  are minimal. It follows that  $G$  would then have a subgroup isomorphic to  $N_1 \times N_2$ , which has order divisible by  $p^2$ . Since the order of  $G$  divides  $p!$ , which

is not divisible by  $p^2$ , this cannot happen, so  $G$  must have a unique minimal normal subgroup,  $N$ . Finally, since  $N$  is nontrivial, it acts transitively, so by the orbit-stabilizer theorem, we find  $[N : H \cap N] = p = [G : H]$ . We conclude that  $[H : H \cap N] = [G : H \cap N]/p = [G : N]$ , as desired.  $\square$

Let  $\mathrm{PSL}(n, q)$  and  $\mathrm{PGL}(n, q)$  denote the projective special linear and projective semilinear groups of rank  $n$  over the finite field  $\mathbb{F}_q$ , respectively, and write  $M_{11}$  and  $M_{23}$  for the Mathieu groups of rank 11 and rank 23. The transitive subgroups of  $S_p$  and their unique minimal normal nontrivial subgroups are classified as follows.

**Lemma 8.2.** *Let  $p$  be a prime, let  $G \subseteq S_p$  be transitive, and let  $N \trianglelefteq G$  denote its unique minimal normal subgroup. Then  $G$ ,  $N$ , and  $p$  satisfy one of the following:*

- (a)  $N = \mathbb{Z}/p\mathbb{Z}$ ,  $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes H$  for some  $H \subseteq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ ;
- (b)  $N = G = A_p$  or  $N = A_p$  and  $G = S_p$ ;
- (c)  $p = 11$ ,  $N = G = \mathrm{PSL}(2, 11)$  or  $N = G = M_{11}$ ;
- (d)  $p = 23$ ,  $N = G = M_{23}$ ; or
- (e) *there is some integer  $n \geq 2$  and prime power  $q$  for which  $N = \mathrm{PSL}(n, q)$ ,  $N \subseteq G \subseteq \mathrm{PGL}(n, q)$ , and  $p = (q^n - 1)/(q - 1)$ .*

*Proof.* This follows from the classification of finite simple groups. See [26, Corollary 4.2].  $\square$

As a consequence of Lemma 8.2, we obtain the following.

**Lemma 8.3.** *Let  $p$  be a prime, let  $G$  be a transitive subgroup of  $S_p$ , and let  $N \trianglelefteq G$  be its unique minimal normal subgroup. Then either  $G$  is solvable or the index of  $N$  in  $G$  is a prime power. In particular, Hypothesis  $T(G, N)$  holds.*

*Proof.* In the first case of Lemma 8.2, the group  $G$  is monomial since every irreducible representation is either 1-dimensional or induced from the normal subgroup  $\mathbb{Z}/p\mathbb{Z}$ . For cases (b)-(d), the index of  $N$  is either 1 or 2.

For case (e), write  $q = \ell^m$  for some prime  $\ell$  and integer  $m \geq 1$ . Then  $p = (\ell^{mn} - 1)/(\ell^m - 1)$ , an expression that may be factored in terms of cyclotomic polynomials. An elementary argument then shows that for  $(\ell^{mn} - 1)/(\ell^m - 1)$  to be prime,  $n$  must be prime and  $m$  must be a power of  $n$ . Next, since  $(q^n - 1)/(q - 1)$  is a prime, it must be the case that  $\gcd(n, q - 1) = 1$ . It follows that  $\mathrm{PSL}(n, q)$  and  $\mathrm{PGL}(n, q)$  coincide, and thus the quotient  $\mathrm{PGL}(n, q)/\mathrm{PSL}(n, q)$  is isomorphic to  $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_\ell) \simeq \mathbb{Z}/m\mathbb{Z}$ . Since  $m$  is a power of the prime  $n$ , we conclude that  $N$  must have prime power index in  $G$ .  $\square$

We next prove Corollary 3.8.

*Proof of Corollary 3.8.* Let  $G \subseteq S_p$  be transitive. It follows by Lemma 8.1 that  $G$  admits a unique minimal nontrivial subgroup  $N$ . Appealing to Theorem 3.1, we find that for all except  $O_{|G|, [k:\mathbb{Q}, \varepsilon]}(Q^\varepsilon)$  fields  $K \in \mathfrak{F}_k^G(Q)$  that  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in the region  $\Omega_K(\varepsilon)$ . For all  $K$  outside the exceptional set, by Lemma 8.3 and Theorem 3.3, it follows that  $L(s, \rho)$  is holomorphic and non-vanishing in  $\Omega_K(\varepsilon)$  for each nontrivial irreducible Artin representation of  $K/k$  whose kernel does not contain  $N$ . (Such representations are in fact precisely the faithful representations of  $G$ , since  $N$  is minimal, but we do not need this.)

Let now  $F/k$  be a degree  $p$  extension whose normal closure is  $K$ . Lemma 8.1 implies that  $F \cap K^N = k$ , since  $F$  corresponds to one of the conjugate stabilizer subgroups of  $G$ . This implies that  $\zeta_F(s)/\zeta_k(s)$  may be decomposed as a product of irreducible Artin  $L$ -functions whose kernels do not contain  $N$ , since for example  $\zeta_{K^N}(s)$  may be decomposed exactly as the product over the unfaithful representations of  $G$ . Thus,  $\zeta_F(s)/\zeta_k(s)$  is holomorphic and non-vanishing in  $\Omega_K(\varepsilon)$ .

We prove the corollary for the family  $\mathcal{F}_k^p$  by considering each of the finitely many transitive subgroups  $G \subseteq S_p$  in turn. For the family  $\mathcal{F}_k^{n, S_n}$  with  $n \geq 2$ , it follows as above from Theorem 3.1 by taking  $G = S_n$  and  $N$  to be the unique minimal nontrivial normal subgroup of  $G$ .  $\square$

## 9. AN EFFECTIVE CHEBOTAREV DENSITY THEOREM FOR FIBERS

In this section, we prove Theorem 3.10.

*Proof of Theorem 3.10.* We begin by outlining our strategy in broad terms since the ultimate proof will be almost immediate once set up. Let  $K/k$  be a normal extension with Galois group  $G$ . For any  $x$ , let  $\Pi_K(x)$  be the class function on  $G$  defined by

$$\Pi_K(x) = \sum_{\mathcal{C}} \frac{1}{|\mathcal{C}|} \pi_{\mathcal{C}}(x; K/k) \mathbf{1}_{\mathcal{C}},$$

where the summation runs over the conjugacy classes  $\mathcal{C}$  of  $G$  and  $\mathbf{1}_{\mathcal{C}}$  denotes the indicator function of the class  $\mathcal{C}$ . Because it is a class function,  $\Pi_K(x)$  may be decomposed in terms of the irreducible characters of  $G$ , namely

$$(9.1) \quad \Pi_K(x) = \sum_{\rho \in \text{Irr}(G)} \langle \Pi_K(x), \chi_{\rho} \rangle \chi_{\rho},$$

where  $\text{Irr}(G)$  denotes the set of irreducible complex representations of  $G$ . Since  $\langle \Pi_K(x), \mathbf{1}_G \rangle$  is the average value of  $\Pi_K(x)$  across  $G$ , we find

$$\langle \Pi_K(x), \mathbf{1}_G \rangle = \frac{1}{|G|} \pi_k^{ur}(x),$$

where  $\pi_k^{ur}(x)$  denotes the number of primes of  $k$  with bounded norm that are unramified in  $K/k$ . In particular, the usual Chebotarev density theorem follows if  $\langle \Pi_K(x), \chi_{\rho} \rangle$  is small for each nontrivial irreducible  $\rho$ , since then the difference between  $\Pi_K(x)$  and  $\langle \Pi_K(x), \mathbf{1}_G \rangle \mathbf{1}_G$  would be small by (9.1).

More generally, let  $N \trianglelefteq G$  be a normal subgroup. Then we may regard the analogous class function  $\Pi_{K^N}(x)$  of  $G/N$  as a class function on  $G$ , and we find

$$\text{Proj}_{\mathcal{R}_{\mathbb{C}}(G/N)} \Pi_K(x) = \frac{1}{|N|} \Pi_{K^N}(x),$$

where  $\text{Proj}_{\mathcal{R}_{\mathbb{C}}(G/N)} \Pi_K(x)$  denotes the orthogonal projection of  $\Pi_K(x)$  onto  $\mathcal{R}_{\mathbb{C}}(G/N)$ , the space of class functions on  $G/N$ . Theorem 3.10 is true if and only if  $\Pi_K(x)$  is “close” to  $\frac{1}{|N|} \Pi_{K^N}(x)$ . Since  $\mathcal{R}_{\mathbb{C}}(G/N)$  is spanned by the irreducible characters that factor through  $G/N$ , we find

$$\Pi_K(x) - \text{Proj}_{\mathcal{R}_{\mathbb{C}}(G/N)} \Pi_K(x) = \sum_{\substack{\rho \in \text{Irr}(G) \\ N \not\subseteq \ker \rho}} \langle \Pi_K(x), \chi_{\rho} \rangle \chi_{\rho}.$$

Thus, to prove Theorem 3.10, our goal is to show that  $\langle \Pi_K(x), \chi_{\rho} \rangle$  is small for each  $\rho$  whose kernel does not contain  $N$ . In fact, we find

$$\langle \Pi_K(x), \chi_{\rho} \rangle = \langle \Pi_K(x), \bar{\chi}_{\rho} \rangle = \frac{1}{|G|} \sum_{N\mathfrak{p} \leq x} \chi_{\rho}(\mathfrak{p}).$$

Thus, Theorem 3.9 may be used directly to control the inner product  $\langle \Pi_K(x), \chi_{\rho} \rangle$ . Theorem 3.10 follows.  $\square$

## 10. APPLICATIONS TO CLASS GROUPS

In this section, we prove Theorem 2.4 on the  $\ell$ -torsion subgroups of class groups, and we prove Theorem 2.1 on the extremal order of class numbers.

**10.1. Bounds on  $\ell$ -torsion subgroups.** We begin by recalling the key lemma of [25].

**Lemma 10.1** (Ellenberg–Venkatesh). *Suppose that  $F/k$  is a degree  $d$  extension of number fields, and let  $\ell \geq 2$ . Suppose that  $\mathfrak{P}_1, \dots, \mathfrak{P}_M$  are prime ideals of  $F$  with norm at most  $D_F^{1/(2\ell(d-1))-\delta}$  for some  $\delta > 0$  and that are not extensions of prime ideals from any proper subfield of  $F/k$ . Then*

$$|\text{Cl}(F)[\ell]| \ll_{k,\ell,\varepsilon} D_F^{1/2+\varepsilon}/M.$$

*Proof of Theorem 2.4.* Let  $n \geq 2$  be an integer,  $Q \geq 1$ , and  $F \in \mathcal{F}_k^{n,S_n}(Q)$ . For a number field  $L$ , let  $\pi_L(x)$  be the prime ideal counting function for  $L$ . Apart from at most  $O_{n,[k:\mathbb{Q}],\varepsilon}(Q^\varepsilon)$  such fields  $F$ , it follows from (3.11) in Corollary 3.8 that if  $x \geq (\log D_F)^{81(n!)^2/\varepsilon}$ , we have

$$\pi_F(x) = \pi_k(x) + \sum_{\mathbb{N}_{k/\mathbb{Q}}\mathfrak{p} \leq x} \chi_{\rho_F}(\mathfrak{p}) = \pi_k(x) + O_{n,[k:\mathbb{Q}],\varepsilon}(x \exp(-c_9 \sqrt{\log x})).$$

The contribution from the prime ideals of  $F$  of degree larger than two is  $\ll_n \sqrt{x}$ , so this is absorbed by the error term. Since there exist effectively computable constants  $c_{13} = c_{13}(k) > 0$  and  $c_{14} = c_{14}(k) > 0$  such that  $\pi_k(x) \geq c_{13}x/\log x$  for all  $x \geq c_{14}$ , it follows that for all fixed  $\delta > 0$ , there exists an effectively computable constant  $c_{15} = c_{15}(n, k, \delta, \varepsilon) > 0$  such that there are at least  $c_{15}D_F^{1/(2\ell(n-1))-\delta}/\log D_F$  degree one prime ideals with norm at most  $D_F^{1/(2\ell(n-1))-\delta}$ . The result then follows from Lemma 10.1, since degree 1 primes are necessarily not the extension of a prime ideal in a proper subfield of  $F$ . For a prime  $p$ , the same conclusion holds for all except  $O_{p,[k:\mathbb{Q}],\varepsilon}(Q^\varepsilon)$  fields  $F \in \mathcal{F}_k^p(Q)$  by appealing to (3.12) in Corollary 3.8.  $\square$

**10.2. The extremal order of class numbers.** We turn now to the proof of Theorem 2.1. Thus, let  $r_1$  and  $r_2$  be non-negative integers with  $n := r_1 + 2r_2$  at least 2. We wish to construct degree  $n$   $S_n$ -extensions  $F/\mathbb{Q}$  of signature  $(r_1, r_2)$  with large class number. Our approach is inspired by the conditional work of Duke [17] in the totally real case,  $r_2 = 0$ . In particular, Duke considered a slight modification of a family of polynomials first considered by Ankeny, Brauer, and Chowla [3] for which there is an explicit full-rank subgroup of the units of the resulting fields. Building on this, let  $a_1, \dots, a_{r_1}$  and  $b_{r_1+1}, \dots, b_{r_1+r_2}, c_{r_1+1}, \dots, c_{r_1+r_2}$  be integers with each  $b_j^2 - 4c_j < 0$  such that the polynomial

$$(10.1) \quad g(x) = \prod_{i=1}^{r_1} (x - a_i) \prod_{j=r_1+1}^{r_1+r_2} (x^2 + b_j x + c_j)$$

has only simple roots, the derivative  $g'(x)$  also only has simple roots  $\beta_1, \dots, \beta_{n-1}$ , and  $g(\beta_i) \neq g(\beta_j)$  for  $i \neq j$ . That such integers exist follows, for example, by noting that these conditions are generic for real coefficients, that they may therefore be satisfied for rational coefficients by continuity, and then for integral coefficients by rescaling. Now, consider a polynomial  $f(t, x)$  over  $\mathbb{Q}(t)$  defined by

$$(10.2) \quad f(t, x) := t^n g(x/t) - t = \prod_{i=1}^{r_1} (x - a_i t) \prod_{j=r_1+1}^{r_1+r_2} (x^2 + b_j t x + c_j t^2) - t.$$

The key properties of the polynomial  $f(t, x)$  we shall need are the following.

**Lemma 10.2.** *Let  $g(x)$  and  $f(t, x)$  be as defined above. Then:*

- (i) *The polynomial  $f(t, x)$  is irreducible and has Galois group  $S_n$  over  $\mathbb{Q}(t)$ .*
- (ii) *When  $\tau \in \mathbb{Z}$  is squarefree and sufficiently large, the polynomial  $f(\tau, x)$  is irreducible and the field  $F = \mathbb{Q}(x)/f(\tau, x)$  has signature  $(r_1, r_2)$ , is totally ramified at primes  $p \mid \tau$ , and has regulator satisfying  $\text{Reg}_F \asymp_n (\log D_F)^{r_1+r_2-1}$  if  $\text{Gal}(\tilde{F}/\mathbb{Q}) \simeq S_n$  and  $\text{Reg}_F \ll_n (\log D_F)^{r_1+r_2-1}$  in general.*

*Proof.* We provide a complete proof since our family is slightly more general than his, but all of the essential ideas are due to Duke [17].

When  $\tau \neq \pm 1$  is squarefree, the polynomial  $f(\tau, x)$  is Eisenstein and thus irreducible. Thus,  $f(t, x)$  must be irreducible over  $\mathbb{Q}(t)$ . To compute its Galois group, we follow Duke [17] and note that the splitting field of  $f(t, x)$  over  $\mathbb{Q}(t)$  is the same as that of  $t^n f(1/t, x/t) = g(x) - t^{n-1}$ . By the monodromy computation of [17, Lemma 1], it follows that the Galois group is generated by transpositions and is thus equal to  $S_n$ .

For (ii), the claim about irreducibility and ramification follows from the previous observation that  $f(\tau, x)$  is Eisenstein. For the claim about the signature of  $F$ , we note that as  $\tau \rightarrow \infty$ , the roots of  $f(\tau, x\tau)$  approach those of  $g(x)$ , which was constructed to have signature  $(r_1, r_2)$ . The polynomial  $g(x)$  has simple roots, and as complex roots come in conjugate pairs, it follows that for sufficiently large  $\tau$ ,  $f(\tau, x)$ , and therefore  $F$ , must have signature  $(r_1, r_2)$  as well. It also follows that to each root of  $g(x)$  we may associate an embedding of  $F$ . Explicitly, if we write  $F = \mathbb{Q}(\xi)$  with  $\xi$  an arbitrary root of  $f(\tau, x)$ , then for  $j \leq r_1$ , we associate the embedding  $\sigma_j: F \rightarrow \mathbb{R}$  given by assigning  $\xi$  the value of the root approximating  $\tau a_j$ , and for  $r_1 + 1 \leq j \leq r_1 + r_2$ , we associate the embedding  $\sigma_j: F \rightarrow \mathbb{C}$  such that  $\sigma_j(\xi)/\tau$  approximates a root of  $x^2 + b_j x + c_j$ . For each  $\sigma_j$ , let  $\gamma_j$  denote the associated root of  $g(x)$ . Additionally, to each  $\sigma_j$ , we attach the usual absolute value  $|\cdot|_j: F \rightarrow \mathbb{R}_{\geq 0}$  given by  $|\alpha|_j = |\sigma_j(\alpha)|$  if  $\sigma_j$  is real and  $|\alpha|_j = |\sigma_j(\alpha)|^2$  if  $\sigma_j$  is complex.

We now construct units  $\varepsilon_1, \dots, \varepsilon_{r_1+r_2}$  in  $F$  as follows. For  $i \leq r_1$ , define  $\varepsilon_i = \tau(\xi - a_i\tau)^{-n}$ , and for  $r_1 + 1 \leq i \leq r_1 + r_2$ , define  $\varepsilon_i = \tau^2(\xi^2 + b_i\tau\xi + c_i\tau^2)^{-n}$ . Then

$$\prod_{i=1}^{r_1+r_2} \varepsilon_i = \tau^n (f(\tau, \xi) + \tau)^{-n} = 1.$$

We also find that, in the ring  $\mathcal{O}_F/(\tau)$ , we have

$$(\xi - a_i\tau)^n = \xi^n = f(\tau, \xi) = 0$$

and, using this, that  $(\xi^2 + b_i\tau\xi + c_i\tau^2)^n \equiv 0 \pmod{\tau^2}$ . It follows that each  $\varepsilon_i^{-1}$  is integral and a unit, so each  $\varepsilon_i \in \mathcal{O}_F^\times$ . We next find if  $i \leq r_1$  and  $j \neq i$  that as  $\tau \rightarrow \infty$ , then

$$|\varepsilon_i|_j \sim \begin{cases} \tau^{1-n} |\gamma_j - \gamma_i|^{-n}, & \text{if } j \leq r_1 \\ \tau^{2-2n} |\gamma_j - \gamma_i|^{-2n}, & \text{if } r_1 + 1 \leq j \leq r_1 + r_2, \end{cases}$$

while if  $r_1 + 1 \leq i \leq r_1 + r_2$  and  $j \neq i$ , then

$$|\varepsilon_i|_j \sim \begin{cases} \tau^{2-2n} |(\gamma_j - \gamma_i)(\gamma_j - \bar{\gamma}_i)|^{-n}, & \text{if } j \leq r_1, \\ \tau^{4-4n} |(\gamma_j - \gamma_i)(\gamma_j - \bar{\gamma}_i)|^{-2n}, & \text{if } r_1 + 1 \leq j \leq r_1 + r_2. \end{cases}$$

It then follows, using either the product formula or the relation  $\varepsilon_1 \dots \varepsilon_{r_1+r_2} = 1$ , that

$$|\sigma_i(\varepsilon_i)| \sim \begin{cases} \tau^{(n-1)^2} \left| \text{Res}\left(x - a_i, \frac{g(x)}{x - a_i}\right) \right|^n, & \text{if } i \leq r_1, \\ \tau^{2(n-1)(n-2)} \left| \text{Res}\left(x^2 + b_i x + c_i, \frac{g(x)}{x^2 + b_i x + c_i}\right) \right|^n, & \text{if } r_1 + 1 \leq i \leq r_1 + r_2, \end{cases}$$

where  $\text{Res}(\cdot, \cdot)$  denotes the polynomial resultant. It follows that for  $\tau$  sufficiently large, the  $(r_1 + r_2) \times (r_1 + r_2)$  matrix

$$\begin{pmatrix} \log |\varepsilon_1|_1 & \dots & \log |\varepsilon_1|_{r_1+r_2} \\ \vdots & & \vdots \\ \log |\varepsilon_{r_1+r_2}|_1 & \dots & \log |\varepsilon_{r_1+r_2}|_{r_1+r_2} \end{pmatrix}$$

has positive diagonal entries, negative off-diagonal entries, and rows that sum to 0. It then follows by a lemma of Minkowski [38] that any principal  $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$  minor has positive determinant. Thus, any  $r_1 + r_2 - 1$  of the units  $\varepsilon_1, \dots, \varepsilon_{r_1+r_2}$  are multiplicatively independent, thus



forming a full-rank subgroup of  $\mathcal{O}_F^\times$ , and it follows from the above that  $\text{Reg}_F \ll_n (\log \tau)^{r_1+r_2-1} \ll_n (\log D_F)^{r_1+r_2-1}$ , the latter inequality holding because  $F$  is totally ramified at each prime dividing  $\tau$ . The corresponding asymptotic lower bound follows from work of Remak [45] (see also [49]).  $\square$

By comparison with the cited work of Remak [45], Lemma 10.2 constructs fields whose regulators are essentially as small as possible. To show that such fields often have class number as large as possible, we will show that the residue of the associated Dedekind zeta function  $\text{Res}_{s=1} \zeta_F(s)$  can be as large as conjecturally possible. The key is to show that in many cases this residue may be approximated by a short Euler product. We will do so in more generality. Recall that the family  $\mathfrak{F}_k^G$  is the set of normal extensions  $K/k$  with Galois group isomorphic to  $G$ . We show for the Artin representations  $\rho$  of  $K \in \mathfrak{F}_k^G$  considered in Theorem 3.7 that the value  $L(1, \rho)$  may be approximated by a short Euler product.

**Proposition 10.3.** *Suppose for some  $K \in \mathfrak{F}_k^G$ , with  $D_K$  sufficiently large with respect to  $|G|$ ,  $[k : \mathbb{Q}]$ , and  $\varepsilon$ , that  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in the region  $\Omega_K(\varepsilon)$  for some normal subgroup  $N \trianglelefteq G$  for which Hypothesis  $\mathbb{T}(G, N)$  holds. Let  $\varepsilon > 0$ . For any Artin  $L$ -function  $L(s, \rho)$  that does not factor through  $K^N$ , there holds for any  $x \geq (\log D_K)^{81|G|/\varepsilon}$ ,*

$$L(1, \rho) = \left(1 + O_{|G|, [k:\mathbb{Q}], \varepsilon}(\exp(-c_1 \sqrt{\log x}))\right) \prod_{\mathbf{Np} \leq x} L_{\mathbf{p}}(1, \rho),$$

where  $L_{\mathbf{p}}(s, \rho)$  denotes the Euler factor of  $L(s, \rho)$  at the prime  $\mathbf{p}$ . In particular, if  $A > 0$ , then

$$L(1, \rho) \asymp_{|G|, [k:\mathbb{Q}], A, \varepsilon} \prod_{\mathbf{Np} \leq (\log D_K)^A} L_{\mathbf{p}}(1, \rho).$$

*Proof.* Write

$$\log L(s, \rho) =: \sum_{\mathbf{n}} \frac{A_{\rho}(\mathbf{n})}{\mathbf{Nn}^s},$$

where  $A_{\rho}(\mathbf{n})$  is supported on prime powers and  $A_{\rho}(\mathbf{p}) = \chi_{\rho}(\mathbf{p})$ .

We first claim that this series converges at  $s = 1$ . Indeed, by (3.10) in Theorem 3.7 and partial summation, we have

$$\sum_{\mathbf{Np} \geq x} \frac{\chi_{\rho}(\mathbf{p})}{\mathbf{Np}} \ll_{|G|, [k:\mathbb{Q}], \varepsilon} \exp(-c_1 \sqrt{\log x})$$

for any  $x \geq (\log D_K)^{81|G|/\varepsilon}$ , and we trivially bound the contribution from prime powers by

$$\sum_{\substack{\mathbf{Np}^j \geq x \\ j \geq 2}} \frac{A_{\rho}(\mathbf{p}^j)}{\mathbf{Np}^j} \ll_{[K:k]} \sum_{\substack{\mathbf{Np}^j \geq x \\ j \geq 2}} \frac{1}{j \mathbf{Np}^j} \ll_{[K:\mathbb{Q}]} x^{-1/2}.$$

Thus, the series defining  $\log L(s, \rho)$  converges at  $s = 1$ . It follows that it converges uniformly in sectors to the right of  $s = 1$ , and that it converges to  $\log L(1, \rho)$ , where  $L(1, \rho)$  is defined via the standard Dirichlet series. Moreover, the above argument also shows that

$$\log L(1, \rho) = \sum_{\mathbf{Np} \leq x} \log L_{\mathbf{p}}(1, \rho) + O(\exp(-c_1 \sqrt{\log x})).$$

The first claim follows upon exponentiating. For the second claim, we apply Mertens's theorem to trivially bound the contribution from the range  $(\log D_K)^A \leq \mathbf{Np} \leq (\log D_K)^{81|G|/\varepsilon}$ .  $\square$

We next show for families of fields obtained by specializing extensions of  $\mathbb{Q}(t)$  that it is possible to choose the values of  $L_{\mathbf{p}}(1, \rho)$  at small primes to be as large as possible. See also [17, Proposition 3] and [48].

**Lemma 10.4.** *Let  $f(t, x) \in \mathbb{Q}[x, t]$  be irreducible over  $\mathbb{Q}(t)$ . There exists a constant  $c_{16} = c_{16}(f) > 0$  such that for every prime  $p > c_{16}$ , there exists  $t_p \in \mathbb{Z}$  such that the polynomial  $f(t_p, x) \pmod{p}$  splits completely.*

*Proof.* As the polynomial  $f(t, x)$  is irreducible over  $\mathbb{Q}(t)$ , it defines a separable extension of  $\mathbb{Q}(t)$ . The normal closure of this extension must also be separable, and is hence cut out by an irreducible polynomial  $g(t, x)$ . As  $g(t, x)$  is irreducible, the curve  $g(t, x) \equiv 0 \pmod{p}$  over  $\mathbb{F}_p$  is non-singular for all but finitely many primes  $p$ . Moreover, the Weil bound implies that there is a point  $(t_p, x_p)$  on this curve for every sufficiently large  $p$ . As  $g(t, x)$  defines a normal extension of  $\mathbb{Q}(t)$ , it follows that  $g(t_p, x)$  splits completely modulo  $p$ , and hence that  $f(t_p, x)$  splits completely as well.  $\square$

We are now ready to prove Theorem 2.1. We do so in the following slightly stronger form. For any possible signature  $(r_1, r_2)$ , we set  $n = r_1 + 2r_2$  and let

$$\mathcal{F}_{\mathbb{Q}}^{r_1, r_2}(Q) := \{F \in \mathcal{F}_{\mathbb{Q}}^{n, S_n}(Q) : \text{sgn}(F) = (r_1, r_2)\},$$

where  $\tilde{F}/\mathbb{Q}$  denotes the normal closure of  $F/\mathbb{Q}$ .

**Theorem 10.5.** *Let  $r_1, r_2 \geq 0$  be integers with  $n = r_1 + 2r_2 \geq 2$ . Let  $0 < \varepsilon < 1/(n!(n^2 - n))$  and let  $0 < \eta < 1/(n^2 - n)$ . There exists a constant  $c_{n, \eta, \varepsilon} > 0$  such that if  $Q$  is sufficiently large in terms of  $n, \eta$ , and  $\varepsilon$ , then for at least  $c_{n, \eta, \varepsilon} Q^{\frac{1}{n^2 - n} - \eta}$  fields  $F \in \mathcal{F}_{\mathbb{Q}}^{r_1, r_2}(Q)$ , we have*

$$|\text{Cl}(F)| \lesssim_{n, \varepsilon} \frac{D_F^{1/2} (\log \log D_F)^{n-1}}{(\log D_F)^{r_1 + r_2 - 1}}$$

and  $\zeta_{\tilde{F}}(s)/\zeta_{\tilde{F}^N}(s)$  is non-vanishing in  $\Omega_{\tilde{F}}(\varepsilon)$ , where  $N$  is the unique minimal nontrivial normal subgroup of  $S_n$ .

*Proof.* Let  $(r_1, r_2)$  be a possible signature and consider the polynomial  $f(t, x)$  defined by (10.2). Let  $T$  be sufficiently large in terms of  $n$ . By Lemma 10.4, there is a constant  $c$  such that for every prime  $p$  between  $c$  and  $(\log T)^{1/2}$ , there is a congruence class  $t_p \pmod{p}$  for which  $f(t_p, x)$  splits completely  $\pmod{p}$ . Define a congruence class  $a \pmod{M}$  by

$$M = \prod_{c \leq p \leq (\log T)^{1/2}} p, \quad a \equiv t_p \pmod{p} \text{ for all } c \leq p \leq (\log T)^{1/2}.$$

Note that  $M = \exp(O(\sqrt{\log T}))$  by the prime number theorem.

Consider squarefree  $\tau \leq T$  for which  $\tau \equiv a \pmod{M}$ . A quantitative version of the Hilbert irreducibility theorem due to Cohen [11] shows that for at most  $O(T^{1/2} \log T)$  values  $\tau$  the polynomial  $f(\tau, x)$  does not cut out an  $S_n$ -extension of  $\mathbb{Q}$ . Additionally, by Lemma 10.2, if  $f(\tau, x)$  cuts out a field  $F$ , then necessarily  $\tau | D_F$ . Since  $D_F = O_n(T^{n^2 - n})$ , it follows for any  $\eta > 0$  that altogether there are  $\gg_{n, \eta} T^{1 - \eta}$  distinct degree  $n$   $S_n$ -extensions with signature  $(r_1, r_2)$  produced in this way.

Let  $F/\mathbb{Q}$  be such an extension and let  $\tilde{F}$  denote its normal closure over  $\mathbb{Q}$ . Since  $D_{\tilde{F}} \leq D_F^{n!} \ll_n T^{n!(n^2 - n)}$ , it follows from Theorem 3.1 that for any  $\varepsilon < 1/(n!(n^2 - n))$  all but  $O_{n, \varepsilon}(T^{\varepsilon n!(n^2 - n)})$  of the fields  $F$  are such that  $\zeta_{\tilde{F}}(s)/\zeta_{\tilde{F}^N}(s)$  is non-vanishing in the region  $\Omega_{\tilde{F}}(\varepsilon)$ . For any such  $F$ , we find by Proposition 10.3 that

$$\text{Res}_{s=1} \zeta_F(s) \lesssim_{n, \varepsilon} \prod_{p \leq (\log T)^{1/2}} L_p(1, \rho_F) \lesssim_{n, \varepsilon} (\log \log T)^{n-1} \lesssim_{n, \varepsilon} (\log \log D_F)^{n-1}$$

by our choice of the congruence class  $a \pmod{M}$ . Using the estimate for the regulator provided by Lemma 10.2, we conclude by the analytic class number formula that

$$|\text{Cl}(F)| \lesssim_{n, \varepsilon} \frac{D_F^{1/2} (\log \log D_F)^{n-1}}{(\log D_F)^{r_1 + r_2 - 1}}.$$

The result follows once we choose  $Q = cT^{n^2-n}$  for a suitable constant  $c$  depending on  $n$ .  $\square$

While the family of polynomials (10.2) provides a self-contained exposition, it is possible to obtain the conclusion of Theorem 10.5 for a larger set of fields by using different families while simultaneously imposing certain other constraints. For example, by working instead with a family of polynomials considered by Bilu and Luca [5], we obtain the following result for the family  $\mathcal{F}_{\mathbb{Q}}^{n,0}$ .

**Theorem 10.6.** *Let  $n \geq 2$  and  $\ell, \ell_0 \geq 2$  be integers. Let  $0 < \varepsilon < 1/(2\ell n!(n-1))$  and  $0 < \eta < 1/(2\ell_0(n-1))$ . There are positive constants  $c_{17}$  and  $c_{18}$  (depending at most on  $n, \ell, \ell_0, \varepsilon$ , and  $\eta$ ) such that if  $Q \geq c_{17}$ , then at least  $c_{18}Q^{\frac{1}{2\ell(n-1)}-\eta}$  fields  $F \in \mathcal{F}_{\mathbb{Q}}^{n,0}(Q)$  have the following properties:*

- (i)  $\zeta_{\tilde{F}}(s)/\zeta_{\tilde{F}^N}(s) \neq 0$  in  $\Omega_{\tilde{F}}(\varepsilon)$ , where  $N$  is the unique minimal normal subgroup of  $S_n$ ;
- (ii)  $|\text{Cl}(F)| \asymp_{n,\ell,\varepsilon} D_F^{1/2}(\log \log D_F)^{n-1}/(\log D_F)^{n-1}$ ;
- (iii)  $\text{Cl}(F)$  contains an element of exact order  $\ell$ ; and
- (iv)  $|\text{Cl}(F)[\ell_0]| \ll_{n,\ell,\ell_0,\varepsilon,\eta} D_F^{\frac{1}{2}-\frac{1}{2\ell_0(n-1)}+\eta}$ .

*Proof.* Bilu and Luca consider the family of polynomials

$$f_{\ell}(t, x) = (x - a_1) \dots (x - a_{n-1}) \left( x - (-1)^{n-1} \frac{t^{\ell} - 1}{a_1 \dots a_{n-1}} \right) - 1,$$

and show for any  $\ell$  that there exist integers  $a_1, \dots, a_{n-1}$  such that all but  $O_{n,\ell}(T^{1/2} \log T)$  integers  $|t| \leq T$  subject to a fixed congruence condition cut out an extension  $F \in \mathcal{F}_{n,0}(cT^{2n-2})$  with a point of order  $\ell$  in the associated class group, and that any given field arises for at most  $n(n-1)(n-2)$  values  $t$ . Additionally, they also show for such values of  $t$  that the regulator  $\text{Reg}_F$  of the associated field  $F$  satisfies  $\text{Reg}_F \ll_n (\log D_F)^{n-1}$ . Appealing to Theorem 3.1, Proposition 10.3, and Lemma 10.4 as in the proof of Theorem 10.5, along with Theorem 2.4 for (iv), the result follows.  $\square$

## 11. APPLICATIONS TO SUBCONVEXITY AND PERIODIC TORUS ORBITS

**11.1. Subconvexity.** We begin with an bound for  $L(\frac{1}{2} + it, \rho)$  depending only on  $C(\rho, t)$  (see (4.3)) and the number  $N_{\rho}(\sigma, T)$  of zeros  $\beta + i\gamma$  of  $L(s, \rho)$  such that  $\beta \geq \sigma$  and  $|\gamma| \leq T$ .

**Lemma 11.1.** *Let  $\rho$  be an  $n$ -dimensional Artin representation defined over a field  $k$ . Suppose that  $L(s, \rho)$  has a pole of order  $0 \leq r \leq n$  at  $s = 1$  and that  $(s-1)^r L(s, \rho)$  is entire. If  $0 \leq \Delta < \frac{1}{2}$  and  $t \in \mathbb{R}$ , then*

$$\begin{aligned} \log |L(\tfrac{1}{2} + it, \rho)| &\leq \left( \frac{1}{4} - \frac{\Delta}{10^9} \right) \log(C(\rho)(|t| + 1)^{n[k:\mathbb{Q}]}) \\ &\quad + \frac{\Delta}{10^7} \#\{\beta + i\gamma : \beta \geq 1 - \Delta, |\gamma - t| \leq 6, L(\beta + i\gamma, \rho) = 0\} + O_{n,[k:\mathbb{Q}]}(1) \\ &\leq \left( \frac{1}{4} - \frac{\Delta}{10^9} \right) \log(C(\rho)(|t| + 1)^{n[k:\mathbb{Q}]}) + \frac{\Delta}{10^7} N_{\rho}(1 - \Delta, |t| + 6) + O_{n,[k:\mathbb{Q}]}(1). \end{aligned}$$

*Proof.* Viewing  $L(s, \rho)$  as a degree  $n[k:\mathbb{Q}]$   $L$ -function over  $\mathbb{Q}$ , our hypotheses imply that  $L(s, \rho)$  is an  $L$ -function in the class  $\mathcal{S}(n[k:\mathbb{Q}])$  defined by Soundararajan and Thorner in [50, Section 1]. As such, it follows from [50, Theorem 1.1] that

$$\log |L(\tfrac{1}{2}, \rho)| \leq \left( \frac{1}{4} - \frac{\Delta}{10^9} \right) \log C(\rho) + \frac{\Delta}{10^7} N_{\rho}(1 - \Delta, 6) + 2 \log |L(\tfrac{3}{2}, \rho)| + O((n[k:\mathbb{Q}])^2),$$

where  $C(\rho)$  is defined in (4.3). Following an observation of Heath-Brown in [28], we have for any  $t \in \mathbb{R}$  the bound

$$\begin{aligned} \log |L(\tfrac{1}{2} + it, \rho)| &\leq \left( \frac{1}{4} - \frac{\Delta}{10^9} \right) \log C(\rho, t) + 2 \log |L(\tfrac{3}{2} + it, \rho)| + O((n[k:\mathbb{Q}])^2) \\ &\quad + \frac{\Delta}{10^7} \#\{\beta + i\gamma : \beta \geq 1 - \Delta, |\gamma - t| \leq 6, L(\beta + i\gamma, \rho) = 0\}, \end{aligned}$$

where  $C(\rho, t)$  is defined in (4.3). Since  $|\alpha_{j,\rho}(\mathfrak{p})| \leq 1$  uniformly, we have that

$$2 \log |L(\frac{3}{2} + it, \rho)| + O((n[k : \mathbb{Q}])^2) \ll_{n, [k : \mathbb{Q}]} 1.$$

Moreover, we have the crude bound  $\#\{\beta + i\gamma : \beta \geq 1 - \Delta, |\gamma - t| \leq 6, L(\beta + i\gamma, \rho) = 0\} \leq N_\rho(1 - \Delta, |t| + 6)$ . The result now follows from (4.4).  $\square$

*Proof of Theorem 2.2.* We will prove the result for  $F \in \mathcal{F}_k^p(Q)$ , where  $p$  is prime. For integers  $n \geq 2$ , the corresponding proof for  $F \in \mathcal{F}_k^{n, S_n}(Q)$  is essentially identical. In what follows, let  $G \subseteq S_p$  be a transitive subgroup, and let  $N \trianglelefteq G$  be its unique minimal nontrivial normal subgroup.

Let  $0 < \varepsilon < 1$ , and let  $\delta = \varepsilon/(20|G|)$ . Let  $K \in \mathfrak{F}_k^G$  with  $D_K$  sufficiently large with respect to  $|G|$ ,  $[k : \mathbb{Q}]$ , and  $\varepsilon$ . By Lemma 5.2, the Artin  $L$ -function  $\zeta_K(s)/\zeta_{K^N}(s)$  is holomorphic and the corresponding Artin representation  $\psi_K$  has dimension  $d = |G| - |G/N|$ . Assume that  $\zeta_K(s)/\zeta_{K^N}(s)$  is non-vanishing in the region  $\Omega_K(\varepsilon)$ . When  $D_K$  is sufficiently large with respect to  $|G|$ ,  $[k : \mathbb{Q}]$ , and  $\varepsilon$ , the region  $\Omega_K(\varepsilon)$  contains the rectangle

$$[1 - \delta, 1] \times [-D_K^{1/(|G|[k : \mathbb{Q}])} - 6, D_K^{1/(|G|[k : \mathbb{Q}])} + 6].$$

It follows that  $N_{K/K^N}(1 - \delta, D_K^{1/(|G|[k : \mathbb{Q}])} + 6) = 0$ . As the analytic conductor satisfies  $C(\psi_K) \ll_{|G|, [k : \mathbb{Q}]} D_K$ , Lemma 11.1 implies that if  $|t| \leq D_K^{1/(|G|[k : \mathbb{Q}])}$ , then

$$\log \left| \frac{\zeta_K(\frac{1}{2} + it)}{\zeta_{K^N}(\frac{1}{2} + it)} \right| \leq \left( \frac{1}{4} - \frac{\delta}{10^9} \right) \log \left( \frac{D_K}{D_{K^N}} (1 + |t|)^{d[k : \mathbb{Q}]} \right) + O_{|G|, [k : \mathbb{Q}]}(1).$$

For  $|t| > D_K^{1/(|G|[k : \mathbb{Q}])}$ , we appeal to the fact that neither  $\zeta_K(s)$  nor  $\zeta_{K^N}(s)$  vanishes on the line  $\text{Re}(s) = 1$ . The same must hold for  $\zeta_K(s)/\zeta_{K^N}(s)$ . We may therefore apply Lemma 11.1 with  $\Delta = 0$  so that if  $|t| > D_K^{1/(|G|[k : \mathbb{Q}])}$ , then

$$\begin{aligned} \log \left| \frac{\zeta_K(\frac{1}{2} + it)}{\zeta_{K^N}(\frac{1}{2} + it)} \right| &\leq \frac{1}{4} \log \left( \frac{D_K}{D_{K^N}} (1 + |t|)^{d[k : \mathbb{Q}]} \right) + O_{|G|, [k : \mathbb{Q}]}(1) \\ &\leq \left( \frac{1}{4} - \frac{\delta}{10^9} \right) \log \frac{D_K}{D_{K^N}} + d[k : \mathbb{Q}] \left( \frac{1}{4} + \frac{\delta}{10^9} \right) \log(1 + |t|) + O_{|G|, [k : \mathbb{Q}]}(1). \end{aligned}$$

Combining bounds for both ranges and noting  $d \leq |G| - 1$ , we conclude for all  $t \in \mathbb{R}$  that

$$\left| \frac{\zeta_K(\frac{1}{2} + it)}{\zeta_{K^N}(\frac{1}{2} + it)} \right| \ll_{|G|, [k : \mathbb{Q}]} \left( \frac{D_K}{D_{K^N}} \right)^{\frac{1}{4} - \frac{\varepsilon}{2 \cdot 10^{10}|G|}} (1 + |t|)^{(|G|+1)[k : \mathbb{Q}]}.$$

By Lemma 11.1 with  $\Delta = 0$ , we have  $|\zeta_{K^N}(\frac{1}{2} + it)| \ll_{|G|, [k : \mathbb{Q}]} D_{K^N}^{1/4} (1 + |t|)^{|G/N|[k : \mathbb{Q}]/4}$ . If  $\zeta_{K^N}(\frac{1}{2} + it) = 0$ , then so does  $\zeta_K(\frac{1}{2} + it)$ , so we may assume that  $\zeta_{K^N}(\frac{1}{2} + it) \neq 0$ . Since  $N$  is nontrivial and  $D_{K^N} \leq D_K^{1/|N|}$ , we conclude that

$$|\zeta_K(\frac{1}{2} + it)| \ll_{|G|, [k : \mathbb{Q}]} D_K^{\frac{1}{4} - \frac{\varepsilon}{2 \cdot 10^{10}|G|}} D_{K^N}^{\frac{\varepsilon}{2 \cdot 10^{10}|G|}} (1 + |t|)^{2|G|[k : \mathbb{Q}]} \ll_{|G|, [k : \mathbb{Q}]} D_K^{\frac{1}{4} - \frac{\varepsilon}{4 \cdot 10^{10}|G|}} (1 + |t|)^{2|G|[k : \mathbb{Q}]}.$$

The desired result now follows.

Let  $F \in \mathcal{F}_k^p(Q)$  be a subfield of  $K/k$ , in which case  $F \cap K^N = k$ . We have the factorization  $(s-1)\zeta_F(s) = \left(\frac{\zeta_F(s)}{\zeta_k(s)}\right)((s-1)\zeta_k(s))$ . The function  $(s-1)\zeta_k(s)$  is entire, and the ratio  $\zeta_F(s)/\zeta_k(s)$  is holomorphic in the region  $\Omega_K(\varepsilon)$  by Corollary 3.8. Consequently, the righthand side is a product of two functions which are holomorphic in  $\Omega_K(\varepsilon)$ , and we have the bound

$$\begin{aligned} &\#\{\beta + i\gamma : \beta \geq 1 - \delta, |\gamma - t| \leq 6, \zeta_F(\beta + i\gamma) = 0\} \\ &\leq \#\{\beta + i\gamma : \beta \geq 1 - \delta, |\gamma - t| \leq 6, \zeta_F(\beta + i\gamma)/\zeta_k(\beta + i\gamma) = 0\} \\ &+ \#\{\beta + i\gamma : \beta \geq 1 - \delta, |\gamma - t| \leq 6, \zeta_k(\beta + i\gamma) = 0\}. \end{aligned}$$

By Lemma 11.1 with  $\Delta = \delta$ , we deduce that if  $|t| \leq D_K^{1/(\lvert G \rvert^{[k:\mathbb{Q}]})}$ , then

$$\begin{aligned} \log |\zeta_F(\tfrac{1}{2} + it)| &\leq \left(\frac{1}{4} - \frac{\delta}{10^9}\right) \log(D_F(1 + |t|)^{[F:\mathbb{Q}]}) \\ &\quad + \frac{\delta}{10^7} \#\{\beta + i\gamma: \beta \geq 1 - \delta, |\gamma - t| \leq 6, \zeta_F(\beta + i\gamma) = 0\} + O_{[F:\mathbb{Q}]}(1) \\ &\leq \left(\frac{1}{4} - \frac{\delta}{10^9}\right) \log(D_F(1 + |t|)^{[F:\mathbb{Q}]}) \\ &\quad + \frac{\delta}{10^7} \#\{\beta + i\gamma: \beta \geq 1 - \delta, |\gamma - t| \leq 6, \zeta_k(\beta + i\gamma) = 0\} + O_{[F:\mathbb{Q}]}(1). \end{aligned}$$

By [30, Proposition 5.7], we find that

$$10^{-7} \delta \#\{\beta + i\gamma: \beta \geq 1 - \delta, |\gamma - t| \leq 6, \zeta_k(\beta + i\gamma) = 0\} \ll |G|^{-1} \varepsilon \log(D_k(1 + |t|)^{[k:\mathbb{Q}]}) ,$$

hence

$$|\zeta_F(\tfrac{1}{2} + it)| \ll_{|G|, [k:\mathbb{Q}]} D_k^{O(\frac{\varepsilon}{|G|})} D_F^{\frac{1}{4} - \frac{\varepsilon}{2 \cdot 10^{10} |G|}} (1 + |t|)^{O(1 + \frac{\varepsilon [k:\mathbb{Q}]}{|G|})}.$$

This proves the desired result for  $\zeta_F(\frac{1}{2} + it)$  when  $|t| \leq D_K^{1/[k:\mathbb{Q}]}$ . By arguing as we did for  $\zeta_K(\frac{1}{2} + it)$  when  $|t| > D_K^{1/[k:\mathbb{Q}]}$  using the convexity bound (which follows from Lemma 11.1 with  $\Delta = 0$ ), we arrive at the desired result for all  $t$ .  $\square$

**11.2. Equidistribution of periodic torus orbits.** As indicated in [22, Section 1.6.3], the equidistribution statement of Theorem 2.3 follows once a suitable subconvexity bound is known. We elaborate slightly on their general setup, with notation consistent with this paper rather than [22], before specializing to the case of interest to us.

Thus, let  $k$  be a number field and let  $S$  be a finite set of places of  $k$  containing all archimedean places and such that the finite primes in  $S$  generate the class group of  $k$ . Let  $k_S := \prod_{v \in S} k_v$  and let  $\mathcal{O}_{k,S}$  denote the  $S$ -integers of  $k$ , i.e. the elements of  $k$  that are integral away from primes in  $S$ . To show that torus orbits inside  $\mathrm{PGL}_p(\mathcal{O}_{k,S}) \backslash \mathrm{PGL}_p(k_S)$  associated to orders  $\mathcal{O}$  in degree  $p$  extensions  $F/k$  become equidistributed, Einsiedler, Lindenstrauss, Michel, and Venkatesh prove two key lemmas, namely [22, Lemmas 13.3 and 13.4], both relying on a subconvexity hypothesis stated formally as [22, Equation (71)]. This subconvexity hypothesis is that for any Hecke character  $\chi$  of  $k$  ramified only at primes in  $S$ , there are constants  $A$  and  $\delta > 0$  depending at most on  $k$  and  $p$  such that for any  $t$ ,

$$(11.1) \quad L(\tfrac{1}{2} + it, \mathrm{Ind}_{G_F}^{G_k} \mathbf{1} \otimes \chi) \ll_{[F:\mathbb{Q}]} (q_\chi \cdot (1 + |t|))^A D_F^{\frac{1}{4} - \delta},$$

where  $q_\chi$  is the conductor of the  $L$ -function  $L(s, \chi)$  and  $\mathrm{Ind}_{G_F}^{G_k} \mathbf{1}$  denotes the induction of the trivial character of the absolute Galois group  $G_F$  to the absolute Galois group  $G_k$  of  $k$ . In other words, the  $L$ -function  $L(s, \mathrm{Ind}_{G_F}^{G_k} \mathbf{1} \otimes \chi)$  is the twist of the Dedekind zeta function of  $F$  by the character  $\chi$ .

This general statement appears to be outside the scope of our methods, but in the special case that  $k = \mathbb{Q}$  and  $S$  consists only of the infinite place, (11.1) reduces to requiring

$$(11.2) \quad \zeta_F(\tfrac{1}{2} + it) \ll_{[F:\mathbb{Q}]} (1 + |t|)^A D_F^{\frac{1}{4} - \delta}.$$

This is provided by Theorem 2.2 and Lemma 8.1 by the assumptions of Theorem 2.3. Thus, for orders  $\mathcal{O}$  inside fields for which (11.2) holds, both Lemmas 13.3 and 13.4 of [22] hold. Lemma 13.4 is used to control the ‘‘escape of mass’’ of the measure  $\mu_{\mathcal{O}}$  associated to  $\mathcal{O}$ , and in particular it follows that any weak-\* limit of the measures  $\mu_{\mathcal{O}}$  for orders considered in Theorem 2.3 must be a probability measure. Lemma 13.3 is used to show that any weak-\* limit is such that almost every ergodic component has positive entropy with respect to the action of a regular element in  $H_p$ . (See also [21, Theorem 1.9] for a weaker but more general statement.) By a measure rigidity theorem of Einsiedler, Katok, and Lindenstrauss [20] (also restated as [22, Theorem 2.5]), any

ergodic  $H_p$ -invariant measure on  $\mathrm{PGL}_p(\mathbb{Z}) \backslash \mathrm{PGL}_p(\mathbb{R})$  with positive entropy must be Haar measure. Thus, any weak- $*$  limit of the  $\mu_{\mathcal{O}}$  has almost every ergodic component given by Haar measure on  $\mathrm{PGL}_p(\mathbb{Z}) \backslash \mathrm{PGL}_p(\mathbb{R})$ , and equidistribution follows.

## 12. HEURISTICS FOR THE INTERSECTION MULTIPLICITY

While our work is strongest for groups  $G$  that have a unique minimal normal subgroup, our results may apply in other situations as well, provided that there is sufficient control over the intersection multiplicity  $\mathfrak{m}_k^{G,N}(Q)$ . We therefore find it worthwhile to record a conjecture for how  $\mathfrak{m}_k^{G,N}(Q)$  should grow; by taking  $N = G$ , this will also describe how the intersection multiplicity  $\mathfrak{m}_k^G(Q)$  that was relevant in the previous works [44, 52] (either implicitly or explicitly) should grow. We work in somewhat more generality.

Fix a transitive and faithful permutation representation  $\pi: G \rightarrow S_n$  with  $n \geq 2$ . Given a field  $K \in \mathfrak{F}_k^G$ , such permutation representations correspond to subextensions of  $K$  whose normal closure over  $k$  is  $K$  by taking the fixed field of a stabilizer subgroup. Let  $K^\pi$  denote the associated subextension, so for example  $K^\pi = K$  when  $\pi$  is the regular representation. Define

$$\mathfrak{F}_k^{G,\pi}(Q) := \{K \in \mathfrak{F}_k^G : D_{K^\pi} \leq Q\}.$$

Malle's conjecture [36] predicts that

$$(12.1) \quad Q^{\frac{1}{a_\pi(G)}} \ll_{k,G} \#\mathfrak{F}_k^{G,\pi}(Q) \ll_{k,G,\varepsilon} Q^{\frac{1}{a_\pi(G)} + \varepsilon},$$

where  $a_\pi(G) := \min\{n - \#\mathrm{Orb}_\pi(g) : g \neq \mathrm{id}\}$  and  $\mathrm{Orb}_\pi(g)$  denotes the set of orbits of the action of  $\pi(g)$  on the set  $\{1, \dots, n\}$ .

Now, for a normal subgroup  $N \trianglelefteq G$ , generalizing (3.4), define

$$\mathfrak{m}_k^{G,N,\pi}(Q) := \max_{K_1 \in \mathfrak{F}_k^{G,\pi}(Q)} |\{K_2 \in \mathfrak{F}_k^{G,\pi}(Q) : K_1 \cap K_2 \neq K_1^N \cap K_2^N\}|,$$

Thus,  $\mathfrak{m}_k^{G,N,\pi}(Q)$  measures how often two fields  $K_1, K_2 \in \mathfrak{F}_k^{G,\pi}(Q)$  have an intersection outside their associated subfields fixed by  $N$ . In order for such an intersection to occur, there must exist normal subgroups  $N_1, N_2 \trianglelefteq G$  not containing  $N$ , possibly equal to each other, for which  $K_1^{N_1} = K_2^{N_2}$ . Thus,  $\mathfrak{m}_k^{G,N,\pi}(Q)$  will be bounded above by

$$\sum_{\substack{N' \trianglelefteq G \\ N \not\subseteq N'}} \max_F \#\{K \in \mathfrak{F}_k^{G,\pi}(Q) : K^{N'} = F\},$$

where the summation runs over the normal subgroups  $N' \trianglelefteq G$  not containing  $N$  and the maximum runs over all extensions  $F/k$  inside the fixed choice of  $\bar{k}$ . Notice that if  $\mathfrak{p}$  is a tamely ramified prime in  $K/k$ , then  $\mathfrak{p}$  is unramified in  $K^{N'}$  precisely when the inertia subgroup at  $\mathfrak{p}$  is contained in  $N'$ . Motivated by the heuristic reasoning behind Malle's conjecture, set

$$a_\pi(G, N') := \min\{n - \#\mathrm{Orb}_\pi(g) : g \in N', g \neq \mathrm{id}\}.$$

If  $F = K^{N'}$  for some  $K \in \mathfrak{F}_k^{G,\pi}(Q)$ , we then expect

$$Q^{\frac{1}{a_\pi(G, N')}} \ll_{F,G} \#\{K \in \mathfrak{F}_k^{G,\pi}(Q) : K^{N'} = F\} \ll_{F,G,\varepsilon} Q^{\frac{1}{a_\pi(G, N')} + \varepsilon}.$$

Consequently, define

$$m_\pi(G, N) := \max_{\substack{N' \trianglelefteq G \\ N \not\subseteq N'}} a_\pi(G, N')^{-1}$$

if there is at least one nontrivial such  $N'$ , and define  $m_\pi(G, N) = 0$  if there is no such  $N'$  (as is the case if either  $N$  is the unique minimal normal subgroup of  $G$ , or if  $N = G$  and  $G$  is simple). We then conjecture:

**Conjecture 12.1.** *With notation as above, as  $Q \rightarrow \infty$ ,*

$$Q^{m_\pi(G,N)} \ll_{k,G} \mathfrak{m}_k^{G,N,\pi}(Q) \ll_{k,G,\varepsilon} Q^{m_\pi(G,N)+\varepsilon}.$$

A few remarks are in order. First, taking  $\pi$  to be the (right) regular representation of  $G$ , so that  $\mathfrak{m}_k^{G,N,\pi}(Q) = \mathfrak{m}_k^{G,N}(Q)$ , the orbits of  $\pi(g)$  are exactly the (left) cosets of the cyclic subgroup  $\langle g \rangle$ . There are  $|G|/|\langle g \rangle|$  such orbits, and it follows that

$$m_{\text{reg}}(G, N) = \min_{\substack{N' \trianglelefteq G \\ N \not\subseteq N'}} \max_{1 \neq g \in N'} \frac{|\langle g \rangle|}{|G|(|\langle g \rangle| - 1)}.$$

Thus, for  $\mathfrak{m}_k^{G,N}(Q)$  defined in (3.4), Conjecture 12.1 implies

$$(12.2) \quad \mathfrak{m}_k^{G,N}(Q) \gg_{k,G} Q^{m_{\text{reg}}(G,N)}.$$

Specializing further by taking  $N = G$ , this implies

$$(12.3) \quad \mathfrak{m}_k^G(Q) \gg_{k,G} Q^{m(G)}, \quad \text{where } m(G) = \min_{\substack{N \trianglelefteq G \\ 1 \neq N \neq G}} \max_{1 \neq g \in N} \frac{|\langle g \rangle|}{|G|(|\langle g \rangle| - 1)}.$$

Second, we now consider when we should expect  $\mathfrak{m}_k^G(Q)$  to be  $\gg_{k,G,\varepsilon} Q^{-\varepsilon} \# \mathfrak{F}_k^G(Q)$  for every  $\varepsilon > 0$ , or more generally when  $\mathfrak{m}_k^{G,N,\pi}(Q) \gg_{k,G,\varepsilon} Q^{-\varepsilon} \# \mathfrak{F}_k^{G,\pi}(Q)$ . Comparing Conjecture 12.1 with Malle's conjecture (12.1), it is apparent we should expect this to hold whenever there is a normal subgroup  $N'$  not containing  $N$  for which  $a_\pi(G, N) = a_\pi(G)$ . Focusing again on the regular representation, this will occur whenever there is a non-identity element of minimal order in  $G$  contained in such an  $N'$ , and when  $N = G$ , whenever there is an element of minimal order contained in any nontrivial proper normal subgroup. This situation arises, for example, if  $G = S_n$  for some  $n \geq 4$ , as  $A_n$  contains elements of order 2, and this leads to our aforementioned speculation that  $\mathfrak{m}_k^{S_n}(Q) \gg_{k,n,\varepsilon} Q^{-\varepsilon} \# \mathfrak{F}_k^{S_n}(Q)$  for every  $\varepsilon > 0$ .

Though it does not follow directly from the above conjectures, we also remark that there are groups  $G$  for which one should even expect  $\mathfrak{m}_k^G(Q) \gg_{k,G} \# \mathfrak{F}_k^G(Q)$ . In particular, this is what one should expect if every non-identity element of minimal order in  $G$  is contained in the same proper normal subgroup; this is ensured, for example, if  $G$  is not a  $p$ -group and the Sylow  $p$ -subgroup of  $G$  is normal for the smallest prime divisor  $p$  of  $|G|$ .

Lastly, we comment on the role of the ramification restrictions imposed by Pierce, Turnage-Butterbaugh, and Wood. As described above, for certain groups  $G$ , they fix conjugacy invariant subsets  $\mathcal{R}_G \subseteq G$  and ask that all tamely ramified primes have inertia subgroups in  $\mathcal{R}_G$ . An analogous story to the above holds, but with the key quantity  $a_\pi(G, N')$  replaced by

$$a_\pi(G, N; \mathcal{R}_G) := \min\{n - \#\text{Orb}_\pi(g) : g \in N' \cap \mathcal{R}_G, g \neq \text{id}\}.$$

For the groups they consider ( $S_n$  for  $n \geq 3$ , the alternating group  $A_4$ , the dihedral group  $D_p$ , and the cyclic group  $C_n$  for any  $n$ ), the set  $\mathcal{R}_G$  is chosen specifically so that the intersection  $N' \cap \mathcal{R}_G$  is empty for every proper normal subgroup  $N' \trianglelefteq G$ . Thus, with the analogous definition, one should expect  $\mathfrak{m}_k^G(Q, \mathcal{R}_G) \ll_{k,G,\varepsilon} Q^\varepsilon$  for every  $\varepsilon > 0$ . We note, however, that apart from  $G = C_p$ , none of these groups are simple, so (12.3) implies that we should nonetheless expect for the full family without restrictions on inertia that  $\mathfrak{m}_k^G(Q) \gg_{k,G} Q^{m(G)}$ , where  $m(G) > 0$ .

As touched upon earlier, a key advantage of our work is that all of the non-abelian groups  $G$  considered in [44] have a unique minimal normal subgroup  $N$ , and thus unconditionally we have  $\mathfrak{m}_k^{G,N}(Q) = 1$  independently of any of the conjectural analysis above. This is the case for many other groups as well.

## REFERENCES

- [1] C. An.  $\ell$ -torsion in class groups of certain families of  $D_4$ -quartic fields. *J. Théor. Nombres Bordeaux*, 32(1):1–23, 2020.
- [2] C. An. Log-free zero density estimates for automorphic  $L$ -functions. *arXiv e-prints*, page arXiv:2004.14410, Apr. 2020.
- [3] N. C. Ankeny, R. Brauer, and S. Chowla. A note on the class-numbers of algebraic number fields. *Amer. J. Math.*, 78:51–61, 1956.
- [4] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *J. Amer. Math. Soc.*, 33(4):1087–1099, 2020.
- [5] Y. F. Bilu and F. Luca. Divisibility of class numbers: enumerative approach. *J. Reine Angew. Math.*, 578:79–91, 2005.
- [6] V. Blomer, G. Harcos, and P. Michel. Bounds for modular  $L$ -functions in the level aspect. *Ann. Sci. École Norm. Sup. (4)*, 40(5):697–740, 2007.
- [7] R. Brauer. A note on zeta-functions of algebraic number fields. *Acta Arith.*, 24:325–327, 1973.
- [8] D. A. Burgess. On character sums and  $L$ -series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.
- [9] E. Carletti, G. Monti Bragadin, and A. Perelli. On general  $L$ -functions. *Acta Arith.*, 66(2):147–179, 1994.
- [10] P. J. Cho. The strong Artin conjecture and large class numbers. *Q. J. Math.*, 65(1):101–111, 2014.
- [11] S. D. Cohen. The distribution of Galois groups and Hilbert’s irreducibility theorem. *Proc. London Math. Soc. (3)*, 43(2):227–250, 1981.
- [12] R. C. Daileda. Non-abelian number fields with very large class numbers. *Acta Arith.*, 125(3):215–255, 2006.
- [13] P. Deligne and G. Henniart. Sur la variation, par torsion, des constantes locales d’équations fonctionnelles de fonctions  $L$ . *Invent. Math.*, 64(1):89–118, 1981.
- [14] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
- [15] W. Duke. Hyperbolic distribution problems and half-integral weight Maass forms. *Invent. Math.*, 92(1):73–90, 1988.
- [16] W. Duke. Bounds for arithmetic multiplicities. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, number Extra Vol. II, pages 163–172, 1998.
- [17] W. Duke. Extreme values of Artin  $L$ -functions and class numbers. *Compositio Math.*, 136(1):103–115, 2003.
- [18] W. Duke, J. B. Friedlander, and H. Iwaniec. The subconvexity problem for Artin  $L$ -functions. *Invent. Math.*, 149(3):489–577, 2002.
- [19] W. Duke and E. Kowalski. A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations. *Invent. Math.*, 139(1):1–39, 2000. With an appendix by Dinakar Ramakrishnan.
- [20] M. Einsiedler, A. Katok, and E. Lindenstrauss. Invariant measures and the set of exceptions to Littlewood’s conjecture. *Ann. of Math. (2)*, 164(2):513–560, 2006.
- [21] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh. Distribution of periodic torus orbits on homogeneous spaces. *Duke Math. J.*, 148(1):119–174, 2009.
- [22] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh. Distribution of periodic torus orbits and Duke’s theorem for cubic fields. *Ann. of Math. (2)*, 173(2):815–885, 2011.
- [23] J. Ellenberg, L. B. Pierce, and M. M. Wood. On  $\ell$ -torsion in class groups of number fields. *Algebra Number Theory*, 11(8):1739–1778, 2017.
- [24] J. S. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.
- [25] J. S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN*, (1):Art. ID rnm002, 18, 2007.
- [26] W. Feit. Some consequences of the classification of finite simple groups. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 175–181. Amer. Math. Soc., Providence, R.I., 1980.
- [27] P. X. Gallagher. A large sieve density estimate near  $\sigma = 1$ . *Invent. Math.*, 11:329–339, 1970.
- [28] D. R. Heath-Brown. Convexity bounds for  $L$ -functions. *Acta Arith.*, 136(4):391–395, 2009.
- [29] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527–550, 2006.
- [30] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.
- [31] J. Klüners and J. Wang.  $\ell$ -torsion bounds for the class group of number fields with an  $\ell$ -group as Galois group. *arXiv e-prints*, page arXiv:2003.12161, Mar. 2020.
- [32] E. Kowalski and P. Michel. Zeros of families of automorphic  $L$ -functions close to 1. *Pacific J. Math.*, 207(2):411–431, 2002.



- [33] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.
- [34] A. Landesman, R. Lemke Oliver, and F. Thorne. Improved lower bounds for the number of fields with alternating Galois group. *Bull. Lond. Math. Soc.* accepted for publication.
- [35] S. Louboutin. Explicit bounds for residues of Dedekind zeta functions, values of  $L$ -functions at  $s = 1$ , and relative class numbers. *J. Number Theory*, 85(2):263–282, 2000.
- [36] G. Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.
- [37] P. Michel and A. Venkatesh. The subconvexity problem for  $GL_2$ . *Publ. Math. Inst. Hautes Études Sci.*, (111):171–271, 2010.
- [38] H. Minkowski. Zur Theorie der Einheiten in den algebraischen Zahlkörpern. *Nachr. Akad. Wiss. Göttingen*, pages 90–93, 1900.
- [39] H. L. Montgomery. Zeros of  $L$ -functions. *Invent. Math.*, 8:346–354, 1969.
- [40] H. L. Montgomery and P. J. Weinberger. Real quadratic fields with large class number. *Math. Ann.*, 225(2):173–176, 1977.
- [41] M. R. Murty and V. K. Murty. *Non-vanishing of L-functions and applications*. Modern Birkhäuser Classics. Birkhäuser/Springer Basel AG, Basel, 1997. [2011 reprint of the 1997 original] [MR1482805].
- [42] V. K. Murty. Modular forms and the Chebotarev density theorem. II. In *Analytic number theory (Kyoto, 1996)*, volume 247 of *London Math. Soc. Lecture Note Ser.*, pages 287–308. Cambridge Univ. Press, Cambridge, 1997.
- [43] L. B. Pierce. A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. *Forum Math.*, 18(4):677–698, 2006.
- [44] L. B. Pierce, C. L. Turnage-Butterbaugh, and M. M. Wood. An effective Chebotarev density theorem for families of number fields, with an application to  $\ell$ -torsion in class groups. *Invent. Math.*, 219(2):701–778, 2020.
- [45] R. Remak. Über Größenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers. *Compositio Math.*, 10:245–285, 1952.
- [46] W. M. Schmidt. Number fields of given degree and bounded discriminant. Number 228, pages 4, 189–195. 1995. Columbia University Number Theory Seminar (New York, 1992).
- [47] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
- [48] J.-P. Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.
- [49] J. H. Silverman. An inequality relating the regulator and the discriminant of a number field. *J. Number Theory*, 19(3):437–442, 1984.
- [50] K. Soundararajan and J. Thorner. Weak subconvexity without a Ramanujan hypothesis. *Duke Math. J.*, 168:1231–1268, 2019. With an appendix by Farrell Brumley.
- [51] H. M. Stark. Some effective cases of the Brauer–Siegel theorem. *Invent. Math.*, 23:135–152, 1974.
- [52] J. Thorner and A. Zaman. A zero density estimate for Dedekind zeta functions. *arXiv e-prints*, page arXiv:1909.01338, Sept. 2019.
- [53] J. Thorner and A. Zaman. A unified and improved Chebotarev density theorem. *Algebra Number Theory*, 13(5):1039–1068, 2019.
- [54] J. Wang. Pointwise Bound for  $\ell$ -torsion in Class Groups II: Nilpotent Extensions. *arXiv e-prints*, page arXiv:2006.10295, June 2020.
- [55] J. Wang. Pointwise bound for  $\ell$ -torsion in class groups: Elementary abelian extensions. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 2021(773):129–151, 2021.
- [56] A. Weiss. The least prime ideal. *J. Reine Angew. Math.*, 338:56–94, 1983.

DEPARTMENT OF MATHEMATICS, TUFTS UNIVERSITY, MEDFORD, MA 02155  
 Email address: robert.lemke.oliver@tufts.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, URBANA, IL 61801  
 Email address: jesse.thorner@gmail.com

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO, ONTARIO, CANADA M5S 2E4  
 Email address: zaman@math.toronto.edu