Algebra & Number Theory

Volume 19
2025
No. 3

Moments in the Chebotarev density theorem: general class functions

Régis de la Bretèche, Daniel Fiorilli and Florent Jouve

msp

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.481

Moments in the Chebotarev density theorem: general class functions

Régis de la Bretèche, Daniel Fiorilli and Florent Jouve

À la mémoire de Joël Bellaïche

We find lower bounds on higher moments of the error term in the Chebotarev density theorem. Inspired by the work of Bellaïche, we consider general class functions and prove bounds which depend on norms associated to these functions. Our bounds also involve the ramification and Galois theoretical information of the underlying extension L/K. Under a natural condition on class functions (which appeared in earlier work), we obtain that those moments are at least Gaussian. The key tools in our approach are the application of positivity in the explicit formula followed by combinatorics on zeros of Artin L-functions (which generalize previous work), as well as precise bounds on Artin conductors.

1. Introduction

The study of the error term in the Chebotarev density theorem has a long history and is critical in many applications. If L/K is a Galois extension of number fields, $G = \mathrm{Gal}(L/K)$ and $C \subset G$ is a conjugacy class, then this theorem states that as $x \to \infty$

$$\pi_C(x; L/K) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \mathcal{N}\mathfrak{p} \le x \\ \varphi_\mathfrak{p} = C}} 1 \sim \frac{|C|}{|G|} \mathrm{Li}(x),$$

where $\mathrm{Li}(x) := \int_2^x \mathrm{d}u/\log u$, and the sum extends to maximal ideals $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K with associated Frobenius (resp. norm) denoted $\varphi_\mathfrak{p}$ (resp. $\mathcal{N}\mathfrak{p}$); see, e.g., [Martinet 1977, Section 4] for the general definition of the Frobenius substitution. Equivalently, if $t\colon G \to \mathbb{R}$ is a real-valued class function, then

$$\pi(x; L/K, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \mathcal{N}\mathfrak{p} \le x}} t(\varphi_\mathfrak{p}) \sim \hat{t}(1) \mathrm{Li}(x),$$

where $\hat{t}(1) = (1/|G|) \sum_{g \in G} t(g)$. Note that if $\mathbf{1}_C$ denotes the indicator function of a given conjugacy class C of G, then $\pi(x; L/K, \mathbf{1}_C) = \pi_C(x; L/K)$. As for the error term, which was first bounded effectively by Lagarias and Odlyzko [1977], Bellaïche [2016] has shown under GRH and Artin's conjecture

MSC2020: primary 11R42, 11R44, 11R45; secondary 11N64.
Keywords: Chebotarev density theorem, distribution of primes, moments computation.

(denoted by AC throughout the paper; see Section 4 for recollections on Artin L-functions), that in the case $K = \mathbb{Q}$ and for $x \geq 3$,

$$\pi(x; L/K, t) - \hat{t}(1)\,\mathrm{Li}(x) \ll \lambda_{1,1}(t)\sqrt{x}\log(xM|G|),$$

where M is the product of all primes ramified in L and $\lambda_{1,1}(t) := \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)|\hat{t}(\chi)|$, with $\mathrm{Irr}(G)$ being the set of irreducible characters of G and

$$\hat{t}(\chi) := \langle t, \chi \rangle_G = \frac{1}{|G|}\sum_{g \in G} \overline{\chi(g)}\,t(g).$$

As an example, if $t = \mathbf{1}_C$ for some conjugacy class $C \subset G$, then $\hat{t}(\chi) = (|C|/|G|)\overline{\chi(C)}$.

Bellaïche's bound has been generalized and improved in the recent work [Fiorilli and Jouve 2024]. Moreover, [loc. cit.] studies the generic behavior of the error term, in particular its limiting distribution as $x \to \infty$. Using probabilistic tools, a sufficient condition is obtained for this error term to be Gaussian [loc. cit., Proposition 5.8]. This generalizes previous work on primes in arithmetic progressions [Hooley 1977; Rubinstein and Sarnak 1994; Fiorilli and Martin 2013]. For example, Hooley has shown that for $(a, q) = 1$, the error term

$$E(x; q, a) := \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n) - \frac{1}{\phi(q)}\sum_{n \leq x} \Lambda(n)$$

is such that for any fixed $r \in \mathbb{N}$,

$$\lim_{q \to \infty} \lim_{X \to \infty} \frac{\phi(q)^{r/2}}{(\log q)^{r/2}} \frac{1}{\log X} \int_2^X \frac{(E(x; q, a))^r}{x^{r/2}} \frac{\mathrm{d}x}{x} = \mu_r,$$

where

$$\mu_r := \begin{cases} (2n-1)\cdot(2n-3)\cdots 1 & \text{if } r = 2n, \\ 0 & \text{otherwise} \end{cases}$$

is the r-th moment of the Gaussian. Hooley's theorem is conditional on GRH, as well as the assumption that the multiset of nonnegative nontrivial zeros of Dirichlet L-functions modulo q is linearly independent over the rationals.

The results which we just described (including a number of results in [Fiorilli and Jouve 2024]) apply to limiting distributions as $x \to \infty$, and thus do not give information on the behavior of the error term uniformly when q varies with x. In fact, to obtain such explicit information one would need to significantly strengthen the linear independence hypothesis, that is one would need to assume that integer linear combinations of L-function zeros are bounded away from zero as a function of q (in the spirit of [Montgomery and Vaughan 2007, Section 15.3]).

In [de la Bretèche and Fiorilli 2023], a lower bound is established on higher moments of primes in progressions in a certain range of q in terms of x, assuming only GRH. More precisely, the results of [loc. cit.] manage to circumvent the linear independence assumption by considering a weighted version of $E(x; q, 1)$ and applying positivity in the explicit formula.

The goal of the present paper is to generalize these results in the context of the Chebotarev density theorem, that is to obtain lower bounds on moments of a weighted version of the error term $\pi(x; L/K, t) - \hat{t}(1)\,\mathrm{Li}(x)$ in certain ranges of x depending on the class function t and on invariants of the extension L/K such as the size of its Galois group and of the root discriminant of L. We stress that our results do not assume any form of linear independence of the L-function zeros involved.

Before we state our results, we need a few definitions. We let $\delta > 0$ and $\mathcal{S}_\delta \subset \mathcal{L}^1(\mathbb{R})$ be the set of all nontrivial differentiable even $\eta : \mathbb{R} \to \mathbb{R}$ such that, for all $t \in \mathbb{R}$,

$$\eta(t), \eta'(t) \ll \mathrm{e}^{-(1/2+\delta)|t|},$$

and moreover for all $\xi \in \mathbb{R}$, we have that[1]

$$0 \le \hat{\eta}(\xi) \ll (|\xi| + 1)^{-1}(\log(|\xi| + 2))^{-2-\delta}. \tag{1}$$

Here, the Fourier transform is defined by

$$\hat{\eta}(\xi) := \int_{\mathbb{R}} \mathrm{e}^{-2\pi i \xi u}\eta(u)\,\mathrm{d}u.$$

Finally for any $h \in \mathcal{L}^1(\mathbb{R})$ we define

$$\alpha(h) := \int_{\mathbb{R}} h(t)\,\mathrm{d}t.$$

In this notation, one of the goals of the paper [de la Bretèche and Fiorilli 2023] is to give lower bounds on moments of the error term

$$\sum_{\substack{n\ge 1\\ n\equiv 1 \bmod q}} \frac{\Lambda(n)}{n^{1/2}}\eta(\log(n/x)) - \frac{1}{\phi(q)} \sum_{\substack{n\ge 1\\ (n,q)=1}} \frac{\Lambda(n)}{n^{1/2}}\eta(\log(n/x)), \tag{2}$$

which is a weighted version of $\psi(x; q, 1) - (1/\phi(q))\psi(x, \chi_{0,q})$ where $\chi_{0,q}$ is the principal character modulo q.

In this paper we consider L/K a Galois extension of number fields of group $G = \mathrm{Gal}(L/K)$ and we fix a real-valued class function $t\colon G \to \mathbb{R}$.[2] Our goal will be to understand the moments of

$$\psi_\eta(x; L/K, t) := \sum_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ m\ge 1}} t(\varphi_{\mathfrak{p}}^m)\frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{m/2}}\eta(\log(\mathcal{N}\mathfrak{p}^m/x)), \tag{3}$$

which is a direct generalization of (2) (where, disregarding ramified primes, $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_q)$ and $t = \mathbf{1}_{1 \bmod q} - 1/\phi(q)$). First, we notice that with this smooth weight, the Chebotarev density theorem

[1] The upper bound on $\hat{\eta}(\xi)$ is a quite mild condition given the differentiability of η; going through the proof of the Riemann–Lebesgue lemma we see for instance that a stronger bound holds as soon as η' is monotonous. (A stronger bound holds if η is twice differentiable.) As for the positivity condition, we can take for example $\eta = \eta_1 \star \eta_1$ for some smooth and rapidly decaying η_1.

[2] We will require later the condition $\hat{t} \ge 0$. In particular, the results of our paper also apply to class functions of the form $\mathrm{Re}(t)$, where $t\colon G \to \mathbb{C}$ is a class function of nonnegative real part such that $\hat{t} \ge 0$.

reads

$$\psi_\eta(x; L/K, t) \sim \hat{t}(1)x^{1/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big),$$

where

$$\mathcal{L}_\eta(u) := \int_{\mathbb{R}} \mathrm{e}^{ux}\eta(x)\mathrm{d}x$$

(note that $\mathcal{L}_\eta(u) = \mathcal{L}_\eta(-u)$). Secondly, it follows from an analysis as in [Fiorilli and Jouve 2024] (see, e.g., [loc. cit., Theorem 2.1]) that under GRH, the remainder term $\psi_\eta(x; L/K, t) - \hat{t}(1)x^{1/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)$ has average value equal to $\hat{\eta}(0)z(L/K, t)$, where we define

$$z(L/K, t) := \sum_{\chi \in \mathrm{Irr}(G)} \hat{t}(\chi)\, \mathrm{ord}_{s=1/2} L(s, L/K, \chi).$$

With this in mind, we define $\mathcal{U}$ to be the set of even nontrivial integrable functions $\Phi\colon \mathbb{R} \to \mathbb{R}$ such that $\Phi, \widehat{\Phi} \geq 0$,[3] and we consider for $U > 0$, $\Phi \in \mathcal{U}$, $n \in \mathbb{Z}_{\geq 1}$, and $\eta \in \mathcal{S}_\delta$ the central moment

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) := \frac{1}{U\int_0^\infty \Phi} \int_0^\infty \Phi\Big(\frac{u}{U}\Big)\Big(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\Big(\frac{1}{2}\Big) - \hat{\eta}(0)z(L/K, t)\Big)^n \mathrm{d}u. \tag{4}$$

We will see that under GRH and AC, this integral converges.

Our main result is a lower bound on the even moments $\widetilde{M}_{2m}(U; L/K; t, \eta, \Phi)$, which is conditional on GRH as well as AC. More precisely, if AC holds for a Galois extension L/F where K/F is a subextension, then we obtain a bound which depends on F. For simplicity one can assume that $F = \mathbb{Q}$; in general, we expect to obtain the best possible (and in many families asymptotically optimal) bound with this choice. Our bounds will depend on the root discriminant

$$\mathrm{rd}_L := d_L^{1/[L:\mathbb{Q}]}, \tag{5}$$

where d_L is the absolute value of the discriminant of $L/\mathbb{Q}$. Our estimates will also involve various norms relative to the Galois groups G and G^+ of the extensions L/K and L/F respectively. For a finite group $\mathcal{G}$ and for a class function $t\colon \mathcal{G} \to \mathbb{C}$, these norms are defined as follows:

$$\lambda_{j,k}(t) := \sum_{\chi \in \mathrm{Irr}(\mathcal{G})} \chi(1)^j |\hat{t}(\chi)|^k \quad (j, k \geq 0). \tag{6}$$

Our main results (Theorems 1.1 and 1.4) show that the moments $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$ are asymptotically greater than or equal those of a Gaussian of expected variance. The implied variance will be expressed in terms of zeros of Artin L-functions of a Galois number field extension L/F. More precisely, denoting $t^+ := \mathrm{Ind}_G^{G^+} t$, this variance takes the shape

$$\nu(L/F, t^+; \eta) := \sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^2 b_0(\chi; \hat{\eta}^2), \tag{7}$$

[3]Note that those conditions imply that $\widehat{\Phi}(0) > 0$.

and where $\chi \in \mathrm{Irr}(\mathrm{Gal}(L/F))$,

$$b_0(\chi;\hat{\eta}^2) := \sum_{\rho_\chi \notin \mathbb{R}} \left| \hat{\eta}\left(\frac{\rho_\chi - \frac{1}{2}}{2\pi i}\right) \right|^2, \tag{8}$$

where ρ_χ is running over the nontrivial zeros of $L(s, L/F, \chi)$.

Theorem 1.1. *Let $L/K/F$ be a tower of number fields such that $L \neq \mathbb{Q}$, L/F is Galois, and assume GRH and AC for the extension L/F.*[4] *Define $G := \mathrm{Gal}(L/K)$, $G^+ := \mathrm{Gal}(L/F)$, let $\eta \in \mathcal{S}_\delta$, $\Phi \in \mathcal{U}$, and assume that $t\colon G \to \mathbb{R}$ is a nonzero class function such that $t^+ := \mathrm{Ind}_G^{G^+} t$, the class function on G^+ induced by t, satisfies $\widehat{t^+} \in \mathbb{R}_{\geq 0}$.*[5] *For $m \in \mathbb{N}$, we have the lower bound*

$$\begin{aligned}&\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)\\ &\quad \geq \mu_{2m}\nu(L/F, t^+;\eta)^m(1 + O_\eta(m^2 m!\, w_4(L/F, t^+;\eta))) + O\left(\frac{(\kappa_\eta[F:\mathbb{Q}]\lambda_{1,1}(t^+)\log(\mathrm{rd}_L))^{2m}}{U}\right),\end{aligned} \tag{9}$$

where $\kappa_\eta > 0$ is a constant which depends only on η and

$$w_4(L/F, t^+;\eta) := \frac{\sum_{\chi\in\mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 b_0(\chi;\hat{\eta}^2)}{\left(\sum_{\chi\in\mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^2 b_0(\chi;\hat{\eta}^2)\right)^2}. \tag{10}$$

In other words, the moments $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$ are at least Gaussian of variance $\nu(L/F, t^+;\eta)$. Our next main result is an estimation of this variance as well as an upper bound on the error term $w_4(L/F, t^+;\eta)$.

Remark 1.2. A version of the quantity $w_4(L/F, t^+;\eta)$ has already appeared in the probabilistic study of the error term in Chebotarev [Fiorilli and Jouve 2024, Section 5.2]. In particular, the condition $w_4(L/F, t^+;\eta) = o(1)$ was necessary in order to obtain the central limit theorem [loc. cit., Proposition 5.8]. However, there exists class functions for which this condition does not hold: taking for instance $t = 1$, we obtain a weighted version of the error term in the prime number theorem which under standard hypotheses is not Gaussian; this goes back to Wintner [1941]. Another instance of non-Gaussian moments is explored in [de la Bretèche et al. 2023].

In order to state our bounds on the variance $\nu(L/F, t^+;\eta)$, we define the following quantity attached to a nontrivial class function $t\colon G \to \mathbb{R}$:[6]

$$S_t := \max_{1\neq a\in G} \frac{\left|\sum_{\chi\in\mathrm{Irr}(G)} \chi(a)|\hat{t}(\chi)|^2\right|}{\sum_{\chi\in\mathrm{Irr}(G)} \chi(1)|\hat{t}(\chi)|^2} = \max_{1\neq a\in G} \frac{\left|\sum_{\chi\in\mathrm{Irr}(G)} \chi(a)|\hat{t}(\chi)|^2\right|}{\lambda_{1,2}(t)} \leq 1. \tag{11}$$

Remark 1.3. The quantity S_t is, in a sense, a measure of the size of the support of $\hat{t}$. For many groups, we expect S_t to be much smaller than 1 as soon as $\hat{t}$ has a "large" support in $\mathrm{Irr}(G)$ (see the example following Theorem 1.4 as well as Section 2).

[4] Note that AC for the extension L/F implies AC for the extension L/K.

[5] See the beginning of Section 4 for recollections on induction. Notice that the condition $\hat{t}^+ \geq 0$ is weaker than $\hat{t} \geq 0$. Indeed, by Frobenius reciprocity, we have that $\widehat{t^+}(\chi) = \hat{t}(\chi|_G)$, and moreover the character $\chi|_G$ is a sum of irreducible characters of G.

[6] Note that if $G = \{1\}$, then we define $S_t := 0$.

Here and throughout we denote by $\log_k$ the k-fold iterated logarithm.

Theorem 1.4. *With the same notations and assumptions as in Theorem 1.1, we have the following*:

- *Assume that the weight function* η *is such that* $\inf\{|z-z'| : z \neq z', \hat{\eta}(z) = \hat{\eta}(z') = 0\} > 0$.[7] *Then, we have the bounds*

$$\nu(L/F, t^+; \eta) \asymp_\eta \sum_{\chi \in \mathrm{Irr}(G^+)} |\widehat{t^+}(\chi)|^2 \log(A(\chi)+2),$$
$$w_4(L/F, t^+, \eta) \ll_\eta \frac{\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 \log(A(\chi)+2)}{\big(\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^2 \log(A(\chi)+2)\big)^2}.$$

Here, $A(\chi)$ *is the Artin conductor which is defined in* (18).

- *Assume that* $S_{t^+} \leq 1 - \kappa_\eta (\log_2(\mathrm{rd}_L + 2))^{-1}$ *where* $\kappa_\eta > 0$ *is a large enough constant which depends only on* η. *Then we have the more explicit bounds*

$$1 - S_{t^+} - O_\eta\bigg(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\bigg) \leq \frac{\nu(L/F, t^+; \eta)}{\alpha(|\hat{\eta}|^2)[F : \mathbb{Q}] \log(\mathrm{rd}_L) \lambda_{1,2}(t^+)} \leq 1 + S_{t^+} + O_\eta\bigg(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\bigg), \tag{12}$$

as well as[8]

$$w_4(L/F, t^+; \eta)[F : \mathbb{Q}] \log(\mathrm{rd}_L) \ll_\eta \frac{\lambda_{1,4}(t^+)}{\lambda_{1,2}(t^+)^2} \bigg(1 - S_{t^+} - O_\eta\bigg(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\bigg)\bigg)^{-2} \ll_\eta (\log_2 \mathrm{rd}_L)^2.$$

Remark 1.5. To see why the assumptions made in Theorem 1.4 are important, consider the case where $K = \mathbb{Q}$ and $t = t^+ = 1$, in which $S_{t^+} = 1$. Then we have that

$$\psi_\eta(x; L/K, t) - x^{1/2} \mathcal{L}_\eta\big(\tfrac{1}{2}\big) = \sum_{\substack{p \\ m \geq 1}} \frac{\log p}{p^{m/2}} \eta(\log(p^m/x)) - x^{1/2} \mathcal{L}_\eta\big(\tfrac{1}{2}\big),$$

and the moments of the limiting distribution of this function are much smaller than those of a Gaussian (in fact the limiting distribution has compact and uniformly bounded support, which does not depend on the extension L/K). This does not contradict Theorem 1.1, since in this case $w_4(L/F, t^+, \eta) \gg 1$ (hence we cannot extract any information from (9)).

Remark 1.6. The norms $\lambda_{j,k}(t) := \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^j |\hat{t}(\chi)|^k$ play a fundamental role in the analysis of the error term in the Chebotarev density theorem. Bellaïche [2016] coined the term "Littlewood norm" for $\lambda_{1,1}(t)$, which he thoroughly studied with applications to the sup norm of the error term in Chebotarev. The norm $\lambda_{1,2}(t)$ and its applications to the mean square of the error term in Chebotarev were studied in [Fiorilli and Jouve 2024].

[7] More generally, it is sufficient to assume that there exists an interval $[T_1, T_2]$ where $T_1 > \kappa$ and $T_2 - T_1 \geq \kappa(\log_2(T_1))^{-1}$ on which $\hat{\eta}$ does not vanish, where $\kappa > 0$ is a large enough absolute constant.

[8] Note that the second bound here shows that $w_4(L/F, t^+; \eta)$ is small as soon as the root discriminant is large. However, this bound is far from optimal, and we expect the quotient $\lambda_{1,4}(t^+)/\lambda_{1,2}(t^+)^2$ to also be small in many cases.

Remark 1.7. One can generalize the bound (12). If $\Xi \subset \mathrm{Irr}(G^+)$ is a set of irreducible characters, then one can drop the terms where $\chi \notin \Xi$ in the definition (7) of $\nu(L/F, t^+; \eta)$. Doing so, and assuming that

$$S_{t^+}(\Xi) := \max_{1\neq a\in G} \frac{\left|\sum_{\chi\in\Xi} \chi(a)|\hat{t}(\chi)|^2\right|}{\sum_{\chi\in\Xi} \chi(1)|\hat{t}(\chi)|^2} \leq 1 - \kappa_\eta(\log_2(\mathrm{rd}_L + 2))^{-1},$$

where $\kappa_\eta > 0$ is a large enough constant which depends only on η, we deduce the bound

$$\frac{\nu(L/F, t^+; \eta)}{\alpha(|\hat{\eta}|^2)[F:\mathbb{Q}]\log(\mathrm{rd}_L)\lambda_{1,2}(t^+;\Xi)} \geq 1 - S_{t^+}(\Xi) - O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right),$$

where $\lambda_{1,2}(t^+;\Xi) := \sum_{\chi\in\Xi}\chi(1)|\hat{t}(\chi)|^2$. This generalized bound will be useful in the case $G^+ = S_n$ (see Section 2.5).

The following example illustrates the relevance of introducing the quantities S_t and S_{t^+} in the statement of Theorem 1.4.

Example. Fix an abelian extension L/K of number fields and let $G = \mathrm{Gal}(L/K)$. Let t be real-valued with nonnegative Fourier coefficients of constant modulus (e.g., $t = \mathbf{1}_g$, for any $g \in G$), then, since by orthogonality $\sum_{\chi\in\mathrm{Irr}(G)}\chi(a) = 0$ for every $a \in G\setminus\{1\}$, we have $S_t = 0$. In particular (12) combined with (9) generalizes the situation considered in [de la Bretèche and Fiorilli 2021, page 7] where $t = \mathbf{1}_{1 \bmod q}$ and $G \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ is the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_q)/\mathbb{Q}$. For further examples, including nonabelian extensions, see Section 2.

Remark 1.8. In Theorem 1.1, one might wonder whether it is possible to bound the more familiar moments

$$M_n(U, L/K; t, \eta, \Phi) := \frac{1}{U\int_0^\infty \Phi}\int_0^\infty \Phi\left(\tfrac{u}{U}\right)\left(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\left(\tfrac{1}{2}\right)\right)^n \mathrm{d}u,$$

rather than $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$. This is indeed the case since in Theorem 1.1,

$$m_{L/K;t,\eta} := \hat{\eta}(0)z(L/K, t) = \hat{\eta}(0)z(L/F, t^+)$$

(this follows from [Fiorilli and Jouve 2024, Lemma 3.15]), which by our assumptions is nonnegative. Then, we have that

$$M_{2m}(U, L/K; t, \eta, \Phi) = \sum_{j=0}^{2m}\binom{2m}{j}\widetilde{M}_j(U; L/K, t)m_{L/K;t,\eta}^{2m-j} \geq \widetilde{M}_{2m}(U, L/K; t, \eta, \Phi).$$

Of course, if we can show that $m_{L/K;t,\eta} > 0$, then the last bound can be improved. As a result, we obtain the following corollary.

Corollary 1.9. *Under the assumptions of Theorem 1.1, the bound* (9) *holds with* $M_{2m}(U, L/K; t, \eta, \Phi)$ *in place of* $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$.

We end this section by noting that Theorems 1.1 and 1.4 imply Ω-results on the classical (unweighted) prime ideal counting functions

$$\psi(x;\, L/K, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ m \geq 1}} t(\varphi_{\mathfrak{p}}^m) \log(\mathcal{N}\mathfrak{p}). \tag{13}$$

Corollary 1.10. *Let L/K be a Galois extension of number fields for which GRH holds. Let F be any subfield of K (i.e., $F \subset K \subset L$) which is such that L/F is Galois and satisfies AC. Define $G := \mathrm{Gal}(L/K)$, $G^+ := \mathrm{Gal}(L/F)$, and assume that $t\colon G \to \mathbb{R}$ is a nonzero class function such that $t^+ := \mathrm{Ind}_G^{G^+} t$ satisfies $\widehat{t^+} \in \mathbb{R}_{\geq 0}$. Assume that $S_{t^+} \leq 1 - \kappa(\log_2(\mathrm{rd}_L + 2))^{-1}$ where $\kappa > 0$ is a large enough absolute constant. Then there exists a sequence of values $x = x_{j;L/K,t}$ tending to infinity such that*

$$|\psi(x;\, L/K, t) - \hat{t}(1)x| \gg x^{1/2}([F:\mathbb{Q}] \log(\mathrm{rd}_L) \lambda_{1,2}(t^+))^{1/2} \biggl(1 - S_{t^+} - O\biggl(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\biggr)\biggr)^{1/2}, \tag{14}$$

where the implied constant is absolute. More precisely, there exists a large enough absolute constant $\kappa' > 0$ such that for any large enough $U > 0$ (in absolute terms), there exists $x > 1$ such that (14) *holds with $\log x \in [U, U \cdot \beta_{L,F,K,t}]$ where*

$$\beta_{L,F,K,t} := \kappa'[F:\mathbb{Q}] \lambda_{1,1}(t^+)^2 \log(\mathrm{rd}_L + 2) \log_2(\mathrm{rd}_L + 2) / \lambda_{1,2}(t^+).$$

Corollary 1.11. *Let L/K with $L \neq \mathbb{Q}$ be a Galois extension of number fields for which GRH holds, and define $G := \mathrm{Gal}(L/K)$. Then for any large enough $U > 0$, there exists $x > 1$ for which $\log x \in [U, \kappa' U \cdot \log(d_L + 2)]$ and such that*

$$|\psi(x;\, L/K, |G|\mathbf{1}_e) - x| \gg x^{1/2} (\log d_L)^{1/2}. \tag{15}$$

Here, κ' is a large enough absolute constant (in absolute terms).

The paper is organized as follows. In Section 2 we state applications of our main results to specific families of Galois extensions of number fields. The proofs of these statements are postponed to Section 6. Next, Sections 3 and 4 are dedicated to recollections and preparatory results concerning Artin conductors, and zeros of Artin L-functions, respectively. We prove our main results as well as Corollaries 1.10 and 1.11 in Section 5.

2. Explicit families of Galois extensions and class functions

In this section we study explicit infinite families of extensions for which Theorems 1.1 and 1.4 apply. The proofs of these results are contained in Section 6.

2.1. ***Abelian extensions: moments for prime ideals in ray classes.*** A natural way to generalize the questions addressed in [Hooley 1977; de la Bretèche and Fiorilli 2021; 2023] is to consider moments for the distribution of prime ideals in abelian number field extensions. Indeed, class field theory provides one with the exact transposition to any relative abelian extension of number fields of the classical approach to the study of primes in arithmetic progressions. Let $\mathfrak{m}$ be a nonzero ideal of the ring of integers $\mathcal{O}_K$ of a number field K, denote by $v_\mathfrak{p}$ the valuation on K with respect to a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and consider

$$\mathrm{I}_\mathfrak{m}(K) = \{\text{fractional ideals } \mathfrak{a} \text{ of } K : v_\mathfrak{p}(\mathfrak{a}) = 0 \text{ if } \mathfrak{p} \mid \mathfrak{m}\},$$
$$\mathrm{P}_\mathfrak{m}(K)^+ = \{\gamma\mathcal{O}_K : \gamma \in K, \gamma \text{ totally positive and } \gamma \equiv 1 \bmod \mathfrak{m}\}.$$

The (strict) ray class group attached to K and $\mathfrak{m}$ is defined as the quotient $\mathrm{Cl}_\mathfrak{m}(K) := \mathrm{I}_\mathfrak{m}(K)/\mathrm{P}_\mathfrak{m}(K)^+$. The quotient group $\mathrm{Cl}_\mathfrak{m}(K)$ is abelian and finite of order denoted $h_{K,\mathfrak{m}}$ (the strict ray class number attached to K and $\mathfrak{m}$). In the case $K = \mathbb{Q}$ and $\mathfrak{m} = m\mathbb{Z}$ for a positive integer m, we have

$$\mathrm{Cl}_\mathfrak{m}(K) = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times.$$

Class field theory asserts that, in general, there exists an (abelian) extension $L_\mathfrak{m}/K$ such that $G = \mathrm{Gal}(L_\mathfrak{m}/K) \simeq \mathrm{Cl}_\mathfrak{m}(K)$. In this setting, for any (class) function $t\colon \mathrm{Cl}_\mathfrak{m}(K) \to \mathbb{C}$, the prime counting function we are interested in takes the form

$$\psi_\eta(x; K, \mathfrak{m}, t) := \sum_{\substack{\mathfrak{p} \triangleleft \mathcal{O}_K \\ m \geq 1}} t([\mathfrak{p}]^m) \frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{m/2}} \eta(\log(\mathcal{N}\mathfrak{p}^m/x)),$$

where $[\mathfrak{p}]$ denotes the class of the prime ideal $\mathfrak{p}$ in $\mathrm{Cl}_\mathfrak{m}(K)$. Note that $\psi_\eta(x; K, \mathfrak{m}, t) = \psi_\eta(x; L_\mathfrak{m}/K, t)$, and thus this is a particular case of the setting in Theorem 1.1. The Chebotarev density theorem for $L_\mathfrak{m}/K$ and $t = h_{K,\mathfrak{m}} \mathbf{1}_{[\mathfrak{a}]}$, the (normalized) indicator function of a class $[\mathfrak{a}] \in \mathrm{Cl}_\mathfrak{m}(K)$, can be seen as a "prime number theorem in the ray class field of K corresponding to $\mathfrak{m}$". In this setting, applying Theorem 1.1 gives the following result.

Proposition 2.1. *For $\mathfrak{m}$ a nonzero ideal of the ring of integers $\mathcal{O}_K$ of a number field K, let $L_\mathfrak{m}/K$ be the corresponding ray class field extension, for which we assume that GRH holds. One has for the trivial class $[\mathfrak{e}] \in \mathrm{Cl}_\mathfrak{m}(K)$, any $m \geq 1$, any $\eta \in \mathcal{S}_\delta$ and any $\Phi \in \mathcal{U}$,*

$$\widetilde{M}_{2m}(U, L_\mathfrak{m}/K; h_{K,\mathfrak{m}} \mathbf{1}_{[\mathfrak{e}]}, \eta, \Phi) \geq \mu_{2m} (\alpha(|\hat{\eta}|^2) \log d_{L_\mathfrak{m}})^m (1 + o_{\mathrm{rd}_{L_\mathfrak{m}} \to \infty}(1)),$$

provided $(\log d_{L_\mathfrak{m}})^m/U \to 0$, *where the implied constant in $o(\,\cdot\,)$ depends on $\mathfrak{m}$.*

By analogy with the case of primes in arithmetic progressions (see [de la Bretèche and Fiorilli 2023, Theorem 1.3]), we expect that the dependency on the discriminant of $L_\mathfrak{m}$ can be made explicit in terms of the norm of $\mathfrak{m}$. This is indeed the case, as shown in [Cohen et al. 1998, Theorem 3.3(2)].

2.2. ***Dihedral extensions.*** A natural next step after analyzing the abelian case (see Remark 1.3) is to consider groups having an abelian subgroup of small index. Such is the case of dihedral groups. Let us start by recalling classical facts (see, e.g., [Serre 1977, Section 5.3]): for an odd integer $n \geq 3$, the dihedral group of order $2n$ is defined as follows,

$$D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle.$$

The nontrivial conjugacy classes of D_n are

$$\{\sigma^j, \sigma^{-j}\}\bigl(1 \le j \le \tfrac{1}{2}(n-1)\bigr), \quad \text{and} \quad \{\tau\sigma^k : 0 \le k \le n-1\}.$$

Proposition 2.2. *One has the following table of values of S_t for various choices of central functions $t\colon D_n \to \mathbb{R}$:*

n	≥ 3	≥ 3	≥ 5
t	$\lvert D_n\rvert \mathbf{1}_e$	$\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$	$2\mathbf{1}_e + \mathbf{1}_{\{\sigma,\sigma^{-1}\}}$
S_t	$\dfrac{1}{2n-1}$	$\dfrac{1-2/n}{2(1-1/n)}$	$< \frac{2}{3}$

The first column of the table is used to prove the following result.

Proposition 2.3. *For $n \ge 3$ odd, let $L/\mathbb{Q}$ be a D_n-extension of number fields for which GRH holds. One has for any $m \ge 1$, any $\eta \in \mathcal{S}_\delta$ and any $\Phi \in \mathcal{U}$,*

$$\widetilde{M}_{2m}(U, L/\mathbb{Q}; |D_n|\mathbf{1}_e, \eta, \Phi) \ge \mu_{2m}\bigl(\alpha(|\hat{\eta}|^2)\bigl(2 - \tfrac{1}{n}\bigr)\log d_L\bigr)^m (1 + o_{\mathrm{rd}_L \to \infty}(1)),$$

provided $(\log d_L)^m / U \to 0$, *where the implied constant in $o(\cdot)$ depends on n.*

2.3. ***Radical extensions.*** We consider the following Galois extension studied in [Fiorilli and Jouve 2024, Section 9.2]. Let a, p be distinct prime numbers such that $p \ne 2$ and $a^{p-1} \not\equiv 1 \bmod p^2$ and let $K_{a,p}$ be the splitting field (inside $\mathbb{C}$) of $X^p - a \in \mathbb{Q}[X]$. The Galois group $G := \mathrm{Gal}(K_{a,p}/\mathbb{Q})$ is isomorphic to the group of affine transformations of $\mathbb{A}^1_{\mathbb{F}_p}$. A convenient way to describe G is the following:

$$G \simeq \left\{ \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} : c \in \mathbb{F}_p^*, d \in \mathbb{F}_p \right\}. \tag{16}$$

One has $|G| = p(p-1)$ and G admits a real irreducible character ϑ of degree $p-1$ (see Section 6.3).

Proposition 2.4. *Let G be as in* (16). *One has the following table of values for S_t for various choices of central functions $t\colon G \to \mathbb{R}$:*

t	$\lvert G\rvert \mathbf{1}_e$	ϑ
S_t	$\dfrac{1}{p(1-2/p+2/p^2)}$	$\dfrac{1}{p-1}$

We deduce the following result on the moments attached to the class functions considered in the table of Proposition 2.4.

Proposition 2.5. *Let a, p be distinct prime numbers such that $p \ne 2$ and $a^{p-1} \not\equiv 1 \bmod p^2$. Let $K_{a,p}/\mathbb{Q}$ be the Galois extension of group G defined by* (16). *Assuming that GRH holds for $K_{a,p}$, one has for any $m \ge 1$, any $\eta \in \mathcal{S}_\delta$ and any $\Phi \in \mathcal{U}$,*

$$\widetilde{M}_{2m}(U, K_{a,p}/\mathbb{Q}; |G|\mathbf{1}_e, \eta, \Phi) \ge \mu_{2m}(\alpha(|\hat{\eta}|^2) p^3 \log p)^m (1 + o_{p\to\infty}(1)),$$
$$\widetilde{M}_{2m}(U, K_{a,p}/\mathbb{Q}; \vartheta, \eta, \Phi) \ge \mu_{2m}(\alpha(|\hat{\eta}|^2) p \log p)^m (1 + o_{p\to\infty}(1)),$$

provided $(p \log p)^m = o_{p\to\infty}(U)$.

Note that in this particular example of Galois extension $K_{a,p}/\mathbb{Q}$ the Artin conductors of the elements of $\mathrm{Irr}(G)$ can be explicitly computed (see [Fiorilli and Jouve 2024, Section 9.2] and [Viviani 2004]), therefore the last estimates of Theorem 1.4 can also be applied (yielding a weaker bound). Specific features of moments in the Chebotarev density theorem for Galois extensions of type generalizing the case of $K_{a,p}/\mathbb{Q}$ are studied in detail in [de la Bretèche et al. 2023].

2.4. ***Moments for irreducible characters.*** As already mentioned in Remark 1.3, choosing t such that $\hat{t}(\chi) = 0$ for many irreducible characters χ of G could lead to a value of S_t that is close to 1, however in a longer sum we can hope to have more cancellations (following, e.g., the philosophy of [Iwaniec and Kowalski 2004, Chapter 12], cancellations in character sums are believed to occur only when the sums are taken over a sufficiently large index set). However, in some cases where t is nontrivial but has a Fourier support of minimal size (e.g., when t is a nontrivial irreducible character of G, as in the case of $t = \vartheta$ in Section 2.3), one can still have $S_t < 1$ so that our main estimates in Theorem 1.1 and 1.4 apply. The following statement gives a setup where one can take t to be very close to an irreducible character and still apply our main results. This result covers the situation lying at the opposite of the generalization of the bound (12) discussed in Remark 1.7, where one discriminates the irreducible characters appearing in the Fourier support of the class function t according to the size of their degree.

Proposition 2.6. *Let $L/K/F$ be a tower of number fields such that $L \neq \mathbb{Q}$, L/F is Galois, and assume GRH and AC for the extension L/F. Define $G := \mathrm{Gal}(L/K)$ and $G^+ := \mathrm{Gal}(L/F)$. Let $t\colon G \to \mathbb{R}$ be a class function such that $t^+ = \frac{1}{2}(\chi + \overline{\chi})$ for some irreducible representation ρ of G^+ of character χ. Let $\eta \in \mathcal{S}_\delta$ and $\Phi \in \mathcal{U}$. Then $S_{t^+} < 1$ if and only if ρ is faithful and the center $Z(G^+)$ of G^+ has odd order.*[9] *In particular, if this last condition holds and if rd_L is large enough in terms of $1 - S_{t^+}$, then* (12) *applies.*

Finite groups admitting faithful irreducible characters are classified by a result of Gaschütz; see, e.g., [Huppert 1998, Theorem 42.7]. Finally note that even if ρ is not faithful or $2 \mid |Z(G^+)|$ then we may apply the first case in Theorem 1.4.

2.5. ***S_n-extensions.*** Perhaps what can be seen as the "generic" situation is when $L/\mathbb{Q}$ is Galois of group S_n the symmetric group on n letters. One can obtain explicit lower bounds for $\nu(L/F, t^+; \eta)$ by following the approach in [Fiorilli and Jouve 2024, Section 7], which involves Roichman's bound [1996]. For a large set of class functions t, one can show that S_t remains bounded away from 1 (where the distance to 1 is precisely evaluated as a function of n in [loc. cit.]). For instance this applies to the difference of normalized indicator functions

$$t_{C_1,C_2} = (|G|/|C_1|)\mathbf{1}_{C_1} - (|G|/|C_2|)\mathbf{1}_{C_2} \quad (\text{resp. } t_C = (|G|/|C|)\mathbf{1}_C)$$

as soon as C_1, C_2 are distinct conjugacy classes of S_n, one of which has size at most (resp. C is a conjugacy class of S_n of size at most) $n!^{1-(4+\varepsilon)/(\mathrm{e}\log n)}$. Using these ideas, we obtain the following result.

[9] Recall that a representation $\rho\colon G \to \mathrm{GL}(V)$ is said to be faithful if ρ is an injective group morphism.

Proposition 2.7. *Let n be large enough and assume that L/K is a Galois extension of number fields for which $L/\mathbb{Q}$ is Galois of group S_n and satisfies AC and GRH. Let C_1, C_2 be conjugacy classes of* $\mathrm{Gal}(L/K)$ *for which* $\min(|C_1^+|, |C_2^+|) \le n!^{1-(4+\varepsilon)/(\mathrm{e}\log n)}$, *where $\varepsilon > 0$ is fixed. Then for all fixed $m \ge 1$ we have the bound*

$$\widetilde{M}_{2m}(U, L/K; t_{C_1,C_2}, \eta, \Phi) \ge \mu_{2m}\left(c_\eta \frac{\log(n!/\min(|C_1^+|, |C_2^+|))}{\log n!} \frac{[K:\mathbb{Q}]\log(\mathrm{rd}_L) n!^{3/2}}{\min(|C_1^+|, |C_2^+|)^{3/2} p(n)^{1/2}}\right)^m (1 + o_{\mathrm{rd}_L\to\infty}(1)),$$

provided $([K:\mathbb{Q}]\log(\mathrm{rd}_L)\min(|C_1^+|, |C_2^+|)^3 p(n)/n!^3)^{m/2}/U \to 0$, *where $c_\eta > 0$ depends only on η. The same bound holds for the class function $t_{C_1} = (|G|/|C_1|)\mathbf{1}_{C_1}$, with the convention that in this case,* $\min(|C_1^+|, |C_2^+|) = |C_1^+|$.

Note that the factor $\log(n!/\min(|C_1^+|, |C_2^+|))/\log n! \gg_\theta 1$ as soon as $\min(|C_1^+|, |C_2^+|) \le n!^{1-\theta}$ for some $\theta > 0$.

3. Artin conductors

Let us first recall a few facts on Artin conductors. Consider a finite Galois extension of number fields L/K with Galois group G. For $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$, the higher ramification groups form a sequence $(G_i(\mathfrak{P}/\mathfrak{p}))_{i\ge 0}$ of subgroups of G (called filtration of the inertia group $\mathrm{I}(\mathfrak{P}/\mathfrak{p})$) defined as follows:

$$G_i(\mathfrak{P}/\mathfrak{p}) := \{\sigma \in G : \forall z \in \mathcal{O}_L, (\sigma z - z) \in \mathfrak{P}^{i+1}\}.$$

Each $G_i(\mathfrak{P}/\mathfrak{p})$ only depends on $\mathfrak{p}$ up to conjugation and $G_0(\mathfrak{P}/\mathfrak{p}) = \mathrm{I}(\mathfrak{P}/\mathfrak{p})$ (when conjugation is unimportant we will simply denote this group $I(\mathfrak{p})$). For clarity let us fix prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ as above and write G_i for $G_i(\mathfrak{P}/\mathfrak{p})$. Given a representation $\rho\colon G \to \mathrm{GL}(V)$ on a complex vector space V, the subgroups G_i act on V through ρ and we denote by $V^{G_i} \subset V$ the subspace of G_i-invariant vectors. Let χ be the character of ρ and

$$n(\chi, \mathfrak{p}) := \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|} \operatorname{codim} V^{G_i}, \tag{17}$$

which was shown by Artin to be an integer. The *Artin conductor of* χ is the ideal of $\mathcal{O}_K$

$$\mathfrak{f}(L/K, \chi) := \prod_{\mathfrak{p}} \mathfrak{p}^{n(\chi,\mathfrak{p})}.$$

Note that the set indexing the above product is finite since only finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ ramify in L/K. We set

$$A(\chi) := d_K^{\chi(1)} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{f}(L/K, \chi)), \tag{18}$$

where d_K is the absolute value of the absolute discriminant of the number field K and $\mathcal{N}_{K/\mathbb{Q}}$ is the relative ideal norm with respect to $K/\mathbb{Q}$ (we will use the slight abuse of notation that identifies the value taken by this relative norm map with the positive generator of the corresponding ideal).

We recall the following pointwise bounds on the Artin conductor.

Lemma 3.1 [Fiorilli and Jouve 2024, Lemma 4.1]. *Let L/K be a finite Galois extension. For any nontrivial irreducible character χ of $G = \mathrm{Gal}(L/K)$, one has the bounds*

$$\max\bigl(1, \tfrac{1}{2}[K:\mathbb{Q}]\bigr)\chi(1) \le \log A(\chi) \le 2\chi(1)[K:\mathbb{Q}]\log(\mathrm{rd}_L),$$

where the root discriminant rd_L is defined by (5)*. The upper bound is unconditional. The lower bound is unconditional if $K/\mathbb{Q}$ is nontrivial and holds assuming AC for the Artin L-function $L(s, L/\mathbb{Q}, \chi)$.*[10]

We will also use the following average bounds, which generalize [Fiorilli and Jouve 2024, Lemma 4.2].

Lemma 3.2. *Let L/K be a Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. Let $\{c_\chi\}_{\chi\in\mathrm{Irr}(G)}$ be a family of nonnegative real numbers. Then we have the bounds*

$$(1 - S(c)) \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)c_\chi \le \sum_{\chi\in\mathrm{Irr}(G)} \frac{c_\chi \log A(\chi)}{[K:\mathbb{Q}]\log(\mathrm{rd}_L)} \le (1 + S(c)) \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)c_\chi,$$

where $S(c) := S_t$ (recall (11)*) for the choice $t = \sum_{\chi\in\mathrm{Irr}(G)} c_\chi \cdot \chi$.*

Proof. Denoting by χ_{reg} the character of the regular representation of G, we have the equality

$$\sum_{\chi\in\mathrm{Irr}(G)} c_\chi \left(\frac{\chi(1)}{|G|} n(\chi_{\mathrm{reg}}, \mathfrak{p}) - n(\chi, \mathfrak{p}) \right) = \frac{1}{|G_0|} \sum_{i\ge 0} \sum_{1\ne a\in G_i} \sum_{\chi\in\mathrm{Irr}(G)} \chi(a)c_\chi.$$

Summing over the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, we deduce that

$$\left| \sum_{\chi\in\mathrm{Irr}(G)} \frac{c_\chi \log A(\chi)}{[K:\mathbb{Q}]\log(\mathrm{rd}_L)} - \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)c_\chi \right| \le S(c) \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)|c_\chi|,$$

from which the claimed bounds follow. □

We will also use the following bound.

Lemma 3.3. *Let L/K be a Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. For all $\chi \in \mathrm{Irr}(G)$, we have*

$$\frac{\log(A(\chi)+2)}{\log_2((A(\chi)+2)^{3/\chi(1)[K:\mathbb{Q}]})} \ll [K:\mathbb{Q}]\chi(1) \frac{\log(\mathrm{rd}_L+2)}{\log_2(\mathrm{rd}_L+2)}.$$

Proof. This follows form the fact that the function $\cdot/\log\cdot$ is eventually increasing, combined with the upper bound in Lemma 3.1. □

4. Sums over zeros of Artin L-functions

The goal of this section is to express the function $\psi_\eta(x; L/K, t)$ defined by (3) in terms of a sum over zeros of Artin L-functions, which will allow us to give a lower bound on the moments $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$ through an application of positivity. This lower bound will be expressed as a convergent sum over zeros, which we will evaluate explicitly.

[10] It actually also holds for the trivial character in this case.

First we recall a few facts about Artin L-functions. If χ is the character of an irreducible representation $\rho\colon G=\mathrm{Gal}(L/K)\to\mathrm{GL}(V)$, the corresponding Artin L-function is defined for $\mathrm{Re}(s)>1$ by the Euler product

$$L(s,L/K,\chi)=\prod_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}}L_{\mathfrak{p}}(s,\chi),\quad \big(L_{\mathfrak{p}}(s,\chi)=\det(\mathrm{Id}-\mathcal{N}\mathfrak{p}^{-s}\rho(\varphi_{\mathfrak{p}})|_{V^{I_{\mathfrak{p}}}}),\ \mathfrak{p}\lhd\mathcal{O}_K\text{ prime}\big),$$

where $V^{I_{\mathfrak{p}}}$ is the subspace of V which is invariant under the inertia group $I_{\mathfrak{p}}$ (see Section 3). AC states that $L(s,L/K,\chi)$ can be extended to an entire function (except when χ is the trivial character, in which case there is a simple pole at $s=1$). Following [Artin 1931], we recall the definition of the archimedean part $L(s,\chi_\infty)$ of the completed L-function associated to the irreducible character χ. Let v be an infinite place of K (that is, v is a real embedding or a pair of conjugate complex embeddings). Let w be a place of L over v. For the couple (w,v), the analogue of the decomposition group is a subgroup $G_{w/v}$ of G which is trivial if v and w are both real or both complex, and which is the group of order two generated by complex conjugation otherwise. If we denote

$$\Gamma_{\mathbb{R}}(s)=\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big),\quad \Gamma_{\mathbb{C}}(s)=\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1),$$

then the Euler factor at v is

$$\gamma_v(\chi,s)=\begin{cases}\Gamma_{\mathbb{R}}(s)^{\dim V^{G_{w/v}}}\Gamma_{\mathbb{R}}(s+1)^{\operatorname{codim}V^{G_{w/v}}} & \text{if } v \text{ is real},\\ \Gamma_{\mathbb{C}}(s)^{\chi(1)} & \text{if } v \text{ is complex}.\end{cases}$$

The Archimedean part of the completed L-function associated to χ is then defined by the formula (recall the definition (18) of the Artin conductor $A(\chi)$)

$$L(s,\chi_\infty)=A(\chi)^{s/2}\prod_v\gamma_v(\chi,s). \tag{19}$$

We are ready to prove the following explicit formula for the function

$$\psi_\eta(x;L/K,\chi):=\sum_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ m\geq 1}}\chi(\varphi_{\mathfrak{p}}^m)\frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{m/2}}\eta(\log(\mathcal{N}\mathfrak{p}^m/x)).$$

Lemma 4.1. *Let L/K be a Galois extension of number fields, denote $G=\mathrm{Gal}(L/K)$, and let $\chi\in\mathrm{Irr}(G)$. Under AC for $L(s,L/K,\chi)$, for any $\eta\in\mathcal{S}_\delta$ and $x\geq 1$ we have the formula*

$$\psi_\eta(x;L/K,\chi)=x^{1/2}\mathcal{L}_\eta\big(\tfrac12\big)\delta_{\chi=\chi_0}-\sum_{\rho_\chi}x^{\rho_\chi-\frac12}\hat{\eta}\bigg(\frac{\rho_\chi-\frac12}{2\pi i}\bigg)+O_\eta(x^{-1/2}\log(A(\chi)+2)),$$

where ρ_χ runs through the nontrivial zeros of $L(s,L/K,\chi)$.

Proof. Let

$$\gamma_\chi(s)=L(s,\chi_\infty)A(\chi)^{-s/2}.$$

Since we assume AC, we can use [Iwaniec and Kowalski 2004, Theorem 5.11] for the test function $\varphi\colon n\mapsto\eta(\log(n/x))/n^{1/2}$. Note that our assumptions are weaker than those in [loc. cit., Theorem 5.11], however going through the proof one sees that our hypotheses are sufficient for [loc. cit., (5.44)] to apply; see, e.g., [Montgomery and Vaughan 2007, Theorem 12.13] and [de la Bretèche and Fiorilli 2023]. Let us recall what is the relevant von Manglodt function Λ_χ in this case (it should satisfy [Iwaniec and Kowalski 2004, (5.25)]):

$$\Lambda_\chi(p^t)=\sum_{f\ell=t}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\log(p^f)\chi(\varphi_{\mathfrak{p}}^{\ell})\quad(p\text{ prime}, t\in\mathbb{N}).$$

Indeed, by [Martinet 1977, page 11],

$$-\frac{L'(s,L/K,\chi)}{L(s,L/K,\chi)}=\sum_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}}\sum_{\ell\geq 1}\frac{\chi(\varphi_{\mathfrak{p}}^{\ell})\log\mathcal{N}\mathfrak{p}}{\mathcal{N}\mathfrak{p}^{s\ell}}=\sum_{p}\sum_{f,\ell\geq 1}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\frac{\chi(\varphi_{\mathfrak{p}}^{\ell})\log(p^f)}{p^{s\ell f}}=\sum_{p}\sum_{t\geq 1}\frac{\Lambda_\chi(p^t)}{p^{ts}}.$$

Then, the first term on the left-hand side of [Iwaniec and Kowalski 2004, (5.44)] is given by

$$\begin{aligned}\sum_{n\geq 1}\Lambda_\chi(n)\frac{\eta(\log(n/x))}{n^{1/2}}&=\sum_{p,t}\sum_{f\ell=m}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\frac{\log(p^f)\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(p^m/x))}{p^{m/2}}\\&=\sum_{p,m}\sum_{f\ell=m}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}\\&=\sum_{p,\ell}\sum_{m\equiv 0\bmod \ell}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=m/\ell}}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}.\end{aligned}$$

Reindexing the sums, we obtain

$$\begin{aligned}\sum_{n\geq 1}\Lambda_\chi(n)\frac{\eta(\log(n/x))}{n^{1/2}}&=\sum_{p,\ell}\sum_{m'\geq 1}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=m'}}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}\\&=\sum_{p,\ell}\sum_{\mathfrak{p}\mid p}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}\\&=\sum_{\mathfrak{p},\ell}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}=\psi_\eta(x;L/K,\chi).\end{aligned}$$

A similar calculation shows that the second term on the left-hand side of [Iwaniec and Kowalski 2004, (5.44)] is exactly $\psi_\eta(x^{-1};L/K,\overline{\chi})$. This translates into the formula

$$\begin{aligned}&\psi_\eta(x;L/K,\chi)+\psi_\eta(x^{-1};L/K,\overline{\chi})\\&\quad=\eta(\log(x))\log A(\chi)+\delta_{\chi=\chi_0}x^{1/2}\mathcal{L}_\eta\big(\tfrac12\big)\\&\qquad+\tfrac{1}{2\pi}\int_{-\infty}^{\infty}\bigg(\frac{\gamma_\chi'\big(\frac12+it\big)}{\gamma_\chi\big(\frac12+it\big)}+\frac{\gamma_\chi'\big(\frac12-it\big)}{\gamma_\chi\big(\frac12-it\big)}\bigg)\widehat{\eta}\big(\tfrac{t}{2\pi}\big)x^{it}\,dt-\sum_{\rho_\chi}x^{\rho_\chi-\frac12}\hat{\eta}\bigg(\frac{\rho_\chi-\frac12}{2\pi i}\bigg)+O_\eta(x^{-1/2}),\end{aligned}\tag{20}$$

where the error term accounts for possible trivial zeros of $L(s,L/K,\chi)$ at $s=0$.

To handle the contribution of the integral of γ-factors we use (19) as well as [Montgomery and Vaughan 2007, Lemma 12.14] that applies to our case with the choice $J(u) = \eta(2\pi(u - \log x))$. Up to the multiplicative constant $\chi(1)$ the contribution of any infinite place v of K is bounded by an analogous integral where the γ-factor appearing is the Euler Γ function. We can then combine [Montgomery and Vaughan 2007, Theorem 12.13 and Lemma 12.14] and [de la Bretèche and Fiorilli 2023, proof of Lemma 2.2] (note that we are using the assumption that η is differentiable here). To conclude, we use the upper bound $[K:\mathbb{Q}]\chi(1) \ll \log(A(\chi))$ from Lemma 3.1. □

In Section 5, we will apply Lemma 4.1 to approximate $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ (recall (4)). A positivity argument will then be applied to this approximation producing convergent sums over zeros of the form

$$b(\chi; h) := \sum_{\rho_\chi} h\left(\frac{\rho_\chi - \frac{1}{2}}{2\pi i}\right), \quad b_0(\chi; h) := \sum_{\rho_\chi \notin \mathbb{R}} h\left(\frac{\rho_\chi - \frac{1}{2}}{2\pi i}\right), \tag{21}$$

where ρ_χ runs through the nontrivial zeros of $L(s, L/K, \chi)$. Note that these sums take into account the multiplicities of zeros, by convention. As for the involved test function, we will work with $\mathcal{T}_\delta$, the set of nontrivial measurable functions $h\colon \mathbb{R} \to \mathbb{R}$ having the following properties. We require that $\xi \mapsto \xi h(\xi)$ is integrable, and that, for all $\xi \in \mathbb{R}$, we have the bounds

$$0 \le h(\xi) \ll (1 + |\xi|)^{-1}(\log(2 + |\xi|))^{-2-2\delta}.$$

Moreover, for all $t \in \mathbb{R}$, we have that[11]

$$\hat{h}(t), \hat{h}'(t) \ll \mathrm{e}^{-(1/2+\delta/2)|g|}.$$

Note that if $\eta \in \mathcal{S}_\delta$ is nontrivial, then $h_\eta := \hat{\eta}^2 \in \mathcal{T}_\delta$. We may extend h to the domain $\left\{s \in \mathbb{C} \colon |\Im\mathrm{m}(s)| \le \frac{1}{4\pi}\right\}$ by writing

$$h(s) := \int_{\mathbb{R}} \mathrm{e}^{2\pi i s\xi} \hat{h}(\xi)\, \mathrm{d}\xi. \tag{22}$$

Lemma 4.2. *Let L/K be a Galois extension of number fields of group G, and let $\chi \in \mathrm{Irr}(G)$. Assume AC for the extension L/K. Then for any $h \in \mathcal{T}_\delta$, we have the pointwise estimates*

$$\begin{aligned} b(\chi; h) &= \hat{h}(0) \log A(\chi) + O_h(\chi(1)[K:\mathbb{Q}]), \\ b(\chi; h) &\ll_h \log(A(\chi) + 2). \end{aligned} \tag{23}$$

Proof. To estimate the sum $b(\chi; h)$ defined in (21), we set $x = 1$ and $\eta = \hat{h}$ in the explicit formula (20), resulting in the identity

$$b(\chi; h) = \mathcal{L}_\eta\left(\tfrac{1}{2}\right)\delta_{\chi=\chi_0} + \hat{h}(0)\log A(\chi) + \tfrac{1}{2\pi}\int_{-\infty}^{\infty}\left(\frac{\gamma_\chi'\left(\frac{1}{2}+it\right)}{\gamma_\chi\left(\frac{1}{2}+it\right)} + \frac{\gamma_\chi'\left(\frac{1}{2}-it\right)}{\gamma_\chi\left(\frac{1}{2}-it\right)}\right) h\left(\frac{t}{2\pi}\right) \mathrm{d}t \\ - \psi_{\hat{h}}(1; L/K, \chi) - \psi_{\hat{h}}(1; L/K, \overline{\chi}) + O_h(1). \tag{24}$$

[11] The integrability of $\xi \mapsto \xi h(\xi)$ implies that $\hat{h}$ is differentiable; see [Kolmogorov and Fomin 1989, page 430].

We have already seen in the proof of Lemma 4.1 that the contribution of the gamma factors is $\ll \chi(1)$. Moreover, we have the bound

$$\psi_{\hat{h}}(1; L/K, \chi) \ll_h \chi(1) \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ m \geq 1}} \frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{(1+\delta/2)m}} \ll \chi(1) \sum_p \sum_{f \geq 1} \frac{\log(p^f)}{p^{f(1+\delta/2)}} \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \mathfrak{p} \mid p \\ f(\mathfrak{p}/p) = f}} 1 \ll_\delta \chi(1)[K : \mathbb{Q}]. \quad (25)$$

The first claimed bound follows. As for the second, it is a consequence of Odlyzko type bounds; see, e.g., [Pizarro-Madariaga 2011, Theorem 3.2]. □

The next step will be to obtain an average bound on $b_0(\chi; \hat{\eta}^2)$. Precisely if $t : G \to \mathbb{C}$ is a class function and $\eta \in \mathcal{S}_\delta$ (recall the definition involving condition (1)) for some fixed $\delta > 0$, then we analyze in the following lemma the variance defined in (7).

Lemma 4.3. *Assume AC and GRH for the Galois extension of number fields L/K, and let $\eta \in \mathcal{S}_\delta$. Then we have the estimate*

$$\nu(L/K, t; \eta) = \alpha(|\hat{\eta}|^2) \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \log A(\chi) + E(L/K, t; \eta) + O_\eta([K : \mathbb{Q}]\lambda_{1,2}(t)), \quad (26)$$

where[12]

$$E(L/K, t; \eta) \ll_\eta \min\left\{ [K : \mathbb{Q}]\lambda_{1,2}(t) \frac{\log(\mathrm{rd}_L + 2)}{\log_2(\mathrm{rd}_L + 2)}, \left(\max_{\chi \in \mathrm{Irr}(G)} \frac{|\hat{t}(\chi)|^2}{\chi(1)} \right) \frac{\log(d_L + 2)}{\log_2(d_L + 2)} \right\}. \quad (27)$$

Moreover, we have the bounds

$$\alpha(|\hat{\eta}|^2)\lambda_{1,2}(t)\left(1 - S_t - O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right) \leq \frac{\nu(L/K, t; \eta)}{[K : \mathbb{Q}] \log(\mathrm{rd}_L)} \leq \alpha(|\hat{\eta}|^2)\lambda_{1,2}(t)\left(1 + S_t + O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right). \quad (28)$$

Proof. First observe that by (23), we have the estimate

$$\sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 b(\chi, |\hat{\eta}|^2) = \alpha(|\hat{\eta}|^2) \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \log A(\chi) + O_\eta([K : \mathbb{Q}]\lambda_{1,2}(t)).$$

Then, we remove the contribution of real zeros as follows:

$$\sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 (b(\chi, |\hat{\eta}|^2) - b_0(\chi, |\hat{\eta}|^2)) \ll_\eta \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \operatorname{ord}_{s=1/2} L(s, L/K, \chi)$$
$$\ll_\eta \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \frac{\log(A(\chi) + 2)}{\log_2(A(\chi) + 2)^{3/(\chi(1)[K:\mathbb{Q}])}},$$

[12]Note that only the first term of this minimum will be used in this paper — the second is present for future reference.

by [Iwaniec and Kowalski 2004, Proposition 5.21]. The first bound on $E(L/K,t;\eta)$ then follows directly from Lemma 3.3. As for the second, we have that

$$\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2(b(\chi,|\hat{\eta}|^2)-b_0(\chi,|\hat{\eta}|^2))\ll_\eta\Big(\max_{\chi\in\mathrm{Irr}(G)}\frac{|\hat{t}(\chi)|^2}{\chi(1)}\Big)\cdot\mathrm{ord}_{s=1/2}\,\zeta_L(s)$$
$$\ll_\eta\Big(\max_{\chi\in\mathrm{Irr}(G)}\frac{|\hat{t}(\chi)|^2}{\chi(1)}\Big)\frac{\log(d_L+2)}{\log_2(d_L+2)},$$

thanks to the decomposition $\zeta_L(s)=\prod_{\chi\in\mathrm{Irr}(G)}L(s,L/K,\chi)^{\chi(1)}$ and [Iwaniec and Kowalski 2004, Proposition 5.34]. Finally, (28) follows from combining (26) with the bounds in Lemma 3.2. □

In view of (28), one may wonder if we can still produce a lower bound if S_t is close to 1. In the next two lemmas we show that in this case we can still estimate $b_0(\chi,h)$ in terms of $\log A(\chi)$. The idea here is that if $\hat{\eta}$ does not vanish on an interval containing sufficiently many imaginary parts of L-function zeros then we can deduce the required estimate. For $\chi\in\mathrm{Irr}(\mathrm{Gal}(L/K))$ we will denote

$$N(T,\chi)=\{\rho:0<\Re\mathrm{e}(\rho)<1,|\Im\mathrm{m}(\rho)|\le T,L(\rho,L/K,\chi)=0\}\quad(T\ge 0).$$

Lemma 4.4. *Assume AC and GRH for the Galois extension of number fields L/K. Let $G=\mathrm{Gal}(L/K)$ and $\chi\in\mathrm{Irr}(G)$. For all $T>0$ and all $0<\varepsilon\le 1$ one has*

$$N(T+\varepsilon,\chi)-N(T,\chi)$$
$$=\frac{\varepsilon}{\pi}\log\bigg(A(\chi)\Big(\frac{T+\varepsilon}{2\pi\mathrm{e}}\Big)^{\chi(1)[K:\mathbb{Q}]}\bigg)+O\bigg(\frac{\log((A(\chi)+2)(4T+1)^{\chi(1)[K:\mathbb{Q}]})}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])}(4T+1))}+[K:\mathbb{Q}]\chi(1)\bigg).$$

In particular, if $\varepsilon\ge\kappa(\log_2(T+3))^{-1}$ and

$$(1-S_t)^{-1}\le\kappa^{-1}\varepsilon\log_2(\mathrm{rd}_L+2)\Big(1+\frac{[K:\mathbb{Q}]\log T}{\log(\mathrm{rd}_L+2)}\Big),\tag{29}$$

where $\kappa>0$ is a large enough absolute constant, then we have the bound

$$\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2(N(T+\varepsilon,\chi)-N(T,\chi))\ge\frac{\varepsilon}{8\pi}\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log\bigg(A(\chi)\Big(\frac{T+\varepsilon}{2\pi\mathrm{e}}\Big)^{\chi(1)[K:\mathbb{Q}]}\bigg).$$

In case $\mathrm{rd}_L\ll 1$, then the assumption $\varepsilon\gg\kappa(\log_2(T+3))^{-1}$ is sufficient (i.e., (29) is not required).

Note that the condition $\varepsilon\gg\kappa(\log_2(T+3))^{-1}$ implies that ε or T is large enough, which ensures that $N(T+\varepsilon,\chi)-N(T,\chi)\ne 0$.

Proof. Recalling the definition (19) of $L(s,\chi_\infty)$, we combine Theorem 5 and (4.1) of [Carneiro et al. 2015] to obtain

$$N(T{+}\varepsilon,\chi){-}N(T,\chi)=\frac{1}{\pi}\int_{T<|g|<T+\varepsilon}\mathrm{Re}\Big(\frac{L'}{L}\Big(\frac12{+}it,\chi_\infty\Big)\Big),\mathrm{d}t$$
$$+O\bigg(\frac{\log((A(\chi){+}2)(4T{+}1)^{\chi(1)[K:\mathbb{Q}]})}{\log_2((A(\chi){+}2)^{3/(\chi(1)[K:\mathbb{Q}])}(4T{+}1))}\bigg)+O([K:\mathbb{Q}]\chi(1)).\tag{30}$$

To evaluate the main term we use the computations [Iwaniec and Kowalski 2004, (5.35) and (5.36)] in the context of [Carneiro et al. 2015, (4.1)]. Precisely the factors of $L(s,\chi_\infty)$ have the following contribution in the range $[T, T+\varepsilon]$ of imaginary parts of critical zeros:

$$\frac{\varepsilon}{\pi}\log\Big(\frac{A(\chi)}{\pi^{[K:\mathbb{Q}]\chi(1)}}\Big)+\frac{[K:\mathbb{Q}]\chi(1)}{\pi}\Big((T+\varepsilon)\log\frac{T+\varepsilon}{2}-T\log\frac{T}{2}-\varepsilon\Big)+O([K:\mathbb{Q}]\chi(1))$$
$$=\frac{\varepsilon}{\pi}\log\Big(\frac{A(\chi)}{\pi^{[K:\mathbb{Q}]\chi(1)}}\Big)+\frac{[K:\mathbb{Q}]\chi(1)}{\pi}\varepsilon\log\Big(\frac{T+\varepsilon}{2\mathrm{e}}\Big)+O([K:\mathbb{Q}]\chi(1)),$$

which leads to the first estimate. In order to prove the second part of the statement, note that

$$\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\frac{\log((A(\chi)+2)(4T+1)^{\chi(1)[K:\mathbb{Q}]})}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])}(4T+1))}$$
$$\ll\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\frac{\log(A(\chi)+2)}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])})}+[K:\mathbb{Q}]\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)|\hat{t}(\chi)|^2\frac{\log(4T+1)}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])})}.$$

Moreover, Lemma 3.2 implies the bound (recall (11))

$$\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log A(\chi)\geq(1-S_t)\log(\mathrm{rd}_L)\lambda_{1,2}(t)[K:\mathbb{Q}].$$

The stated lower bound then follows from (30) and from Lemmas 3.3 and 3.1. Indeed the main term is greater than twice the error term under the stated assumption. Finally note that if $2\leq\mathrm{rd}_L\ll 1$, then Lemma 3.1 implies that $\log(A(\chi)+2)\asymp[K:\mathbb{Q}]\chi(1)$ which is sufficient to obtain the stated lower bound. The only case not covered by this condition, which corresponds to $L=K=\mathbb{Q}$, can be trivially handled separately. □

Building on Lemma 4.4, we can now deduce an estimate on $b_0(\chi,\hat{\eta}^2)$ (recall (8)) in terms of $\log A(\chi)$ under a support condition on $\hat{\eta}$.

Lemma 4.5. *Assume AC and GRH for the Galois extension of number fields L/K. Let $G=\mathrm{Gal}(L/K)$ and let $\varepsilon, T>0$ be such that $T\geq\kappa$ and $\varepsilon\geq\kappa(\log_2(T+3))^{-1}$, where $\kappa>0$ is absolute and large enough. Assuming that $\hat{\eta}$ does not vanish on $[T, T+\varepsilon]$,*[13] *then we have*

$$\nu(L/K,t;\eta)\asymp_\eta\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log(A(\chi)+2). \tag{31}$$

Proof. By definition, we have the lower bound

$$b_0(\chi;\hat{\eta}^2)\geq(N(T+\varepsilon,\chi)-N(T,\chi))\min_{|g|\in[T,T+\varepsilon]}|\hat{\eta}|^2\gg_\eta\log(A(\chi)+2),$$

by Lemma 4.4 and our hypotheses on ε and T, which imply that the main term in this lemma dominates the error term. As a result,

$$\nu(L/K,t;\eta)\gg_\eta\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log(A(\chi)+2).$$

The upper bound follows directly from (23). □

[13] Recall that in (29) the constant $\kappa>0$ is absolute. Note moreover that if $\hat{\eta}$ does not vanish, the condition on $\hat{\eta}$ is always fulfilled with $\varepsilon=\infty$.

5. Proof of Theorems 1.1 and 1.4: induction and positivity

In this section our main goal is to prove Theorems 1.1 and 1.4. This will be carried out through an application of positivity in the explicit formula obtained in Lemma 4.1 (positivity will circumvent the need for the LI hypothesis). Notice however that doing so directly with the Fourier decomposition (recall the definition (3))

$$\psi_\eta(x; L/K, t) = \sum_{\chi \in \mathrm{Irr}(G)} \hat{t}(\chi)\psi_\eta(x; L/K, \chi)$$

would yield bounds which we believe not to be optimal (unless $K = \mathbb{Q}$). To obtain conjecturally optimal bounds, we will first apply the inductive property of Artin L-functions. This is the purpose of Lemma 5.1. The following step, Lemma 5.2, will consist of approximating the moment we study $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ by the quantity $\widetilde{D}_n(U, L/K; t, \eta, \Phi)$ which involves zeros of Artin L-functions. A lower bound for $\widetilde{D}_n(U, L/K; t, \eta, \Phi)$ will be produced in Lemma 5.7 by combining two preparatory results: a combinatorial inequality which we believe is of intrinsic interest (Lemma 5.3) and a statement which is more representation theoretic in nature and deals with L-function zeros relevant to the moment $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ (Lemma 5.6).

We recall that L/K is a Galois extension of number fields of Galois group G, and $t\colon G \to \mathbb{C}$ is a class function. If F is a subfield of K such that L/F is Galois of group G^+, then we form the class function on G^+ induced by t in the following way:

$$t^+ = \mathrm{Ind}_G^{G^+}(t)\colon G^+ \to \mathbb{C}, \quad t^+(g) = \sum_{\substack{aG \in G^+/G:\\ a^{-1}ga \in G}} t(a^{-1}ga) (g \in G^+).$$

The property of invariance of Artin L-functions under induction (see [Artin 1931, (18)]) can be stated, in our situation, as the equality $L(s, L/K, t) = L(s, L/F, t^+)$: it is crucial to our analysis and implies in particular Lemma 5.1 below.

Through this section, one should keep in mind that if we assume AC for $L/\mathbb{Q}$, then we expect in most cases to obtain the best bounds by selecting $F = \mathbb{Q}$. On the other extreme, one may always take $F = K$ and obtain nontrivial bounds.

Lemma 5.1. *Let $L/K/F$ be a tower of number fields for which L/F is Galois, let $G = \mathrm{Gal}(L/K)$ and $G^+ = \mathrm{Gal}(L/F)$. For $\eta \in \mathcal{S}_\delta$ and for any class function $t\colon G \to \mathbb{C}$, we have the identity*

$$\psi_\eta(x; L/K, t) = \psi_\eta(x; L/F, t^+). \tag{32}$$

As a consequence, for any $\Phi \in \mathcal{U}$ we have the identity

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) = \widetilde{M}_n(U, L/F; t^+, \eta, \Phi). \tag{33}$$

Proof. The equality (32) is stated and proved in [Fiorilli and Jouve 2024, Proposition 3.11]. As for (33), it is a consequence of (32) combined with [loc. cit., Lemma 3.15], which asserts that $z(L/K, t) = z(L/\mathbb{Q}, t^+)$

(the limiting expectation involved in (4)), and the equality $\widehat{t^+}(1) = \hat{t}(1)$, which is a straightforward application of Frobenius reciprocity. □

We now approximate the moment $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ by a sum over zeros of Artin L-functions. If L/F is a Galois extension of group G^+, then we define for every integer $n \geq 1$

$$\widetilde{D}_n(U, L/F; t, \eta, \Phi) := \frac{(-1)^n}{2\int_0^\infty \Phi} \sum_{\chi_1,\dots,\chi_n \in \mathrm{Irr}(G^+)} \biggl(\prod_{j=1}^n \hat{t}(\chi_j)\biggr) \sum_{\gamma_{\chi_1},\dots,\gamma_{\chi_n} \neq 0} \widehat{\Phi}\Bigl(\frac{U}{2\pi}(\gamma_{\chi_1} + \cdots + \gamma_{\chi_n})\Bigr) \prod_{j=1}^n \hat{\eta}\Bigl(\frac{\gamma_{\chi_j}}{2\pi}\Bigr), \tag{34}$$

where $\gamma_{\chi_1}, \dots, \gamma_{\chi_n}$ run over the imaginary parts of the nontrivial zeros of the Artin L-functions

$$L(s, L/F, \chi_1), \dots, L(s, L/F, \chi_n).$$

Lemma 5.2. *Let $L/K/F$ be a tower of number fields in which L/F is a Galois extension satisfying AC and GRH. Let $t\colon \mathrm{Gal}(L/K) \to \mathbb{C}$ be a class function and let $t^+ := \mathrm{Ind}_{\mathrm{Gal}(L/K)}^{\mathrm{Gal}(L/F)} t$. Then for $\eta \in \mathcal{S}_\delta$, $\Phi \in \mathcal{U}$, and $n \in \mathbb{Z}_{\geq 1}$ we have the estimate*

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) = \widetilde{D}_n(U, L/F; t^+, \eta, \Phi) + O\biggl(\frac{(\kappa_\eta [F:\mathbb{Q}] \lambda_{1,1}(t^+) \log(\mathrm{rd}_L + 2))^n}{U}\biggr),$$

where $\kappa_\eta > 0$ is a constant which depends only on η.

Proof. Let $G^+ = \mathrm{Gal}(L/F)$, and recall that by Lemma 5.1, one has

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) = \widetilde{M}_n(U, L/F; t^+, \eta, \Phi).$$

Combining the Fourier decomposition

$$\psi_\eta(\mathrm{e}^u; L/F, t^+) = \sum_{\chi \in \mathrm{Irr}(G^+)} \widehat{t^+}(\chi) \psi_\eta(\mathrm{e}^u; L/F, \chi)$$

and Lemma 4.1 results in the estimate (recall that Frobenius reciprocity implies $\widehat{t^+}(1) = \hat{t}(1)$)

$$\psi_\eta(\mathrm{e}^u; L/F, t^+) = \hat{t}(1) x^{1/2} \mathcal{L}_\eta\Bigl(\frac{1}{2}\Bigr) - \sum_{\chi \in \mathrm{Irr}(G^+)} \widehat{t^+}(\chi) \sum_{\gamma_\chi} \mathrm{e}^{i\gamma_\chi u} \hat{\eta}\Bigl(\frac{\gamma_\chi}{2\pi}\Bigr) + O_\eta\biggl(\mathrm{e}^{-u/2} \sum_{\chi \in \mathrm{Irr}(G^+)} |\widehat{t^+}(\chi)| \log(A(\chi)+2)\biggr). \tag{35}$$

By Lemma 3.1, the error term is $\ll_\eta \mathrm{e}^{-u/2} [F:\mathbb{Q}] \log(\mathrm{rd}_L) \lambda_{1,1}(t^+)$. The claimed estimate follows from substituting this expression in the definition (4) and applying the bound

$$\sum_{\gamma_\chi} \mathrm{e}^{i\gamma_\chi u} \hat{\eta}\Bigl(\frac{\gamma_\chi}{2\pi}\Bigr) \ll_\eta \log(A(\chi) + 2),$$

which is a direct consequence of the Riemann-von Mangoldt formula; see, e.g., [Iwaniec and Kowalski 2004, Theorem 5.8]. □

Our goal will be to apply positivity on the right-hand side of (34). The idea here is that by our conditions on $\widehat{\Phi}$, $\widehat{t^+}$ and $\hat{\eta}$, the quantity $\widetilde{D}_n(U, L/F; t^+, \eta, \Phi)$ is a sum of positive terms. The rapid decay of $\widehat{\Phi}$ should imply that only the terms where $\gamma_{\chi_1} + \cdots + \gamma_{\chi_n}$ is very small contribute substantially to the inner sum in (34). However, if the zeros enjoy on average the diophantine properties of "random" real numbers, then we expect this to be the case only when the ρ_{χ_j} come in conjugate pairs, that is for each j there exists $\pi(j)$ such that $\gamma_{\chi_j} = -\gamma_{\chi_{\pi(j)}}$. Moreover, we also believe that this should force $\chi_j = \overline{\chi_{\pi(j)}}$. Those two facts follow from an effective version of the linear independence hypothesis for Artin L-functions; see [Fiorilli and Jouve 2024, Introduction] for the precise statement. The positivity condition will allow us to circumvent this hypothesis.

Let us first establish the following combinatorial result.

Lemma 5.3. *Let $\Gamma \subset \mathbb{R}_{>0}$ be a countable multiset, and let $\boldsymbol{a} = \{a_\gamma\}_{\gamma\in\Gamma\cup-\Gamma}$ be a sequence of complex numbers such that $a_{-\gamma} = \overline{a_\gamma}$ and moreover $\sum_{\gamma\in\Gamma}|a_\gamma|^2 < \infty$, where by convention sums over $\gamma \in \Gamma$ take multiplicities into account. Define*

$$S_{2\ell}(\boldsymbol{a}) := \sum_{\substack{\gamma_1,\dots,\gamma_\ell\in\Gamma,\gamma'_1,\dots,\gamma'_\ell\in-\Gamma \\ \forall\gamma\in\mathbb{R},\#\{j:\gamma_j=\gamma\}=\#\{j:\gamma'_j=-\gamma\}}} \prod_{j=1}^{\ell} a_{\gamma_j} a_{\gamma'_j}.$$

Then, $S_{2\ell}(\boldsymbol{a}) \in \mathbb{R}$, and moreover for every positive integer ℓ, we have the inequality

$$S_{2\ell}(\boldsymbol{a}) \geq \ell! \left(\sum_{\gamma\in\Gamma}|a_\gamma|^2\right)^{\ell-1} \max\left\{\sum_{\gamma\in\Gamma}|a_\gamma|^2 - \ell!\,\ell(\ell-1)M^2\mathrm{e}^{1/\ell}, 0\right\}, \tag{36}$$

where $M := \sup\{|a_\gamma| : \gamma \in \Gamma\}$.

Remark 5.4. For $\ell = 1$, note that $\ell!\,\ell(\ell-1)M^2\mathrm{e}^{1/\ell} = 0$. In fact, in this case we have

$$S_2(\boldsymbol{a}) = \sum_{\gamma\in\Gamma} m_\gamma |a_\gamma|^2 \geq \sum_{\gamma\in\Gamma}|a_\gamma|^2,$$

where m_γ is the multiplicity of γ in Γ. Indeed, by definition $m_{-\gamma} = m_\gamma$.

Proof of Lemma 5.3. By Remark 5.4, we may assume that $\ell \geq 2$. For any integer $r \geq 1$ and any r-tuple $\boldsymbol{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$, which is a partition of ℓ in the sense that $n_i \leq n_{i+1}$ for all i, and $\sum_i n_i = \ell$, we denote by s_1 the number of indices $i \geq 1$ such that $n_i = n_1$, and inductively by s_j the number of indices i such that $n_i = n_{s_{j-1}+1}$. Note that if k is the "number of distinct parts" in the partition $(n_1, \dots, n_r)$ of ℓ, in particular $s_k = \#\{i : n_i = n_r\}$, then one has $s_1 + \dots + s_k = r$. We set

$$c(\boldsymbol{n}) = c(n_1, \dots, n_r) = \binom{\ell}{n_1, \dots, n_r} \frac{1}{s_1! \cdots s_k!}.$$

where we recall the definition of the multinomial coefficient

$$\binom{\ell}{n_1, \dots, n_r} = \frac{\ell!}{n_1! \cdots n_r!}.$$

In particular $c(1, \dots, 1) = 1$ since in this case $k = 1$ and $s_1 = r = \ell$.

For every $\gamma \in \Gamma$, let m_γ be the multiplicity of γ in Γ. On one hand we have the following expansion (here we use the notation $\sum^*$ to denote a sum "without multiplicity")

$$\left(\sum_{\gamma\in\Gamma}|a_\gamma|^2\right)^\ell = \left(\sideset{}{^*}\sum_{\gamma\in\Gamma} m_\gamma |a_\gamma|^2\right)^\ell = \sum_{\substack{n_1+\dots+n_r=\ell \\ n_1\leq n_2\leq\dots\leq n_r}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j}. \tag{37}$$

Here, we have used the fact that for a given $(n_1, \dots, n_r) \in \mathbb{N}^r$ such that $n_1 + \cdots + n_r = \ell$, the number of permutations of the n_j such that $n_1 \le n_2 \le \cdots \le n_r$ is exactly $s_1! \cdots s_k!$.

On the other hand we have

$$\begin{aligned} S_{2\ell}(\boldsymbol{a}) &= \sum_{\substack{n_1+\cdots+n_r=\ell \\ n_1\le n_2\le\cdots\le n_r}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} a_{\gamma_j}^{n_j} \sideset{}{^*}\sum_{\substack{\gamma_1',\dots,\gamma_\ell'\in\Gamma \\ \forall i, \#\{j\le\ell:\gamma_j'=-\gamma_i\}=n_i}} \prod_{j=1}^{\ell} m_{\gamma_j}^{n_j} a_{-\gamma_j}^{n_j}, \\ &= \sum_{\substack{n_1+\cdots+n_r=\ell \\ n_1\le n_2\le\cdots\le n_r}} c(\boldsymbol{n}) \binom{\ell}{n_1, \dots, n_r} \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{2n_j} |a_{\gamma_j}|^{2n_j} \end{aligned} \tag{38}$$

which is a real number. The additional factor $\binom{\ell}{n_1,\dots,n_r}$ comes from the number of the sets $\#\{j \le \ell : \gamma_j' = -\gamma_i\} = n_i$. Since the multiplicities m_γ are positive integers, the contribution of $\boldsymbol{n} = (1, \dots, 1)$ to the right-hand side of (38) admits the lower bound

$$\ell! \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_\ell\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j}} \prod_{j=1}^{\ell} m_{\gamma_j}^2 |a_{\gamma_j}|^2 \ge \ell! \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_\ell\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j}} \prod_{j=1}^{\ell} m_{\gamma_j} |a_{\gamma_j}|^2. \tag{39}$$

Using (37) we see that the lower bound in (39) equals

$$\ell! \Big(\sum_{\gamma\in\Gamma} |a_\gamma|^2 \Big)^{\ell} - \ell! \sum_{\substack{n_1+\cdots+n_r=\ell \\ n_1\le n_2\le\cdots\le n_r \\ n_r>1}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j},$$

and therefore we deduce from (38) and (39) that

$$\begin{aligned} S_{2\ell}(\boldsymbol{a}) &\ge \ell! \Big(\sum_{\gamma\in\Gamma} |a_\gamma|^2 \Big)^{\ell} + \sum_{\substack{n_1+\cdots+n_r=\ell \\ n_1\le n_2\le\cdots\le n_r \\ n_r\ge 2}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j} \Big(\binom{\ell}{n_1, \dots, n_r} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} - \ell! \Big) \\ &\ge \ell! \Big(\sum_{\gamma\in\Gamma} |a_\gamma|^2 \Big)^{\ell} - \ell!\, S_{2\ell}'(\boldsymbol{a}), \end{aligned} \tag{40}$$

where we denote

$$S_{2\ell}'(\boldsymbol{a}) := \sum_{\substack{n_1+\cdots+n_r=\ell \\ n_1\le n_2\le\cdots\le n_r \\ n_r\ge 2}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j \\ \prod_{j=1}^r m_{\gamma_j}^{n_j} \le n_1!\cdots n_r!}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j}.$$

Here we emphasize the extra condition $\prod_{j=1}^r m_{\gamma_j}^{n_j} \le n_1! \cdots n_r!$ appearing in the index set of the inner sum. This is explained by the fact that r-tuples $\boldsymbol{n}$ such that $\prod_{j=1}^r m_{\gamma_j}^{n_j} > n_1! \cdots n_r!$ contribute a positive term to the second summand in (40).

To obtain an upper bound for $S_{2\ell}'(\boldsymbol{a})$, we write

$$S_{2\ell}'(\boldsymbol{a}) = \sum_{2\le n_r\le\ell} \sum_{\substack{(n_1,\dots,n_{r-1}): \\ n_1+\cdots+n_{r-1}=\ell-n_r \\ n_1\le n_2\le\cdots\le n_r}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma \\ \forall i\neq j, \gamma_i\neq\gamma_j \\ \prod_{j=1}^r m_{\gamma_j}^{n_j} \le n_1!\cdots n_r!}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j}.$$

Note that (37) can then be used for the partition $(n_1,\dots,n_{r-1})$ of $\ell-n_r$ since we have

$$c(\boldsymbol{n})=c(n_1,\dots,n_r)=\binom{\ell}{n_1,\dots,n_r}\frac{1}{s_1!\cdots s_t!}\le c(n_1,\dots,n_{r-1})\binom{\ell}{n_r}.$$

We deduce that

$$S'_{2\ell}(\boldsymbol{a})\le\sum_{2\le n_r\le\ell}\binom{\ell}{n_r}\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-n_r}\Big(\sideset{}{^*}\sum_{\substack{\gamma\in\Gamma\\ m_\gamma^{n_r}\le\ell!}}m_\gamma^{n_r}|a_\gamma|^{2n_r}\Big).\tag{41}$$

Next we use the condition $m_\gamma^{n_r}\le\ell!$ in the index set of the innermost sum of (41) as well as the inequality

$$\binom{\ell}{n_r}\le\ell(\ell-1)\binom{\ell-2}{n_r-2},$$

to compute

$$\begin{aligned}S'_{2\ell}(\boldsymbol{a})&\le\ell!\sum_{2\le n_r\le\ell}\binom{\ell}{n_r}\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-n_r}\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^{2n_r}\Big)\\&\le\ell!\,\ell(\ell-1)M^2\sum_{2\le n_r\le\ell}\binom{\ell-2}{n_r-2}\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-n_r}M^{2(n_r-2)}\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)\\&\le\ell!\,\ell(\ell-1)M^2\Big(M^2+\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-1},\end{aligned}$$

where we have used the upper bound $|a_\gamma|^{2n_r}\le M^{2n_r-2}|a_\gamma|^2$ and the binomial formula for the last step. Plugging this into (40) we deduce that

$$\frac{S_{2\ell}(\boldsymbol{a})}{\ell!}\ge\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell}-\ell!\,\ell(\ell-1)M^2\Big(M^2+\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-1}.\tag{42}$$

To conclude, note that if $\sum_{\gamma\in\Gamma}|a_\gamma|^2\le\ell(\ell-1)\ell!\,M^2$ then we have obtained a trivial lower bound since $S_{2\ell}(\boldsymbol{a})\ge0$ by (38). However if $\sum_{\gamma\in\Gamma}|a_\gamma|^2>\ell(\ell-1)\ell!\,M^2$ then we have

$$\Big(M^2+\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-1}\le\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-1}\Big(1+\frac{1}{\ell(\ell-1)}\Big)^{\ell-1}\le\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-1}\mathrm{e}^{1/\ell}\tag{43}$$

and therefore (42) yields in both cases the asserted lower bound

$$\frac{S_{2\ell}(\boldsymbol{a})}{\ell!}\ge\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell-1}\max\Big\{\sum_{\gamma\in\Gamma}|a_\gamma|^2-\ell!\,\ell(\ell-1)M^2\mathrm{e}^{1/\ell},0\Big\}.\qquad\square$$

Next we state and prove Lemma 5.6 below, which is an application of Lemma 5.3. It makes use of the classification of irreducible characters χ of G according to their *Frobenius–Schur indicator* $\epsilon_2(\chi)$. In view of its importance, we first recall the definition and properties of this invariant. If χ denotes the character of a representation ρ of G, the number

$$\epsilon_2(\chi)=\frac{1}{|G|}\sum_{g\in G}\chi(g^2)$$

is called the *Frobenius–Schur indicator* of χ. If χ is irreducible, then $\epsilon_2(\chi) \in \{-1, 0, 1\}$ (see [Huppert 1998, Theorem 8.7]), and each of these three possible values has a precise meaning in terms of the $\mathbb{R}$-rationality of χ and ρ, as we now recall; see, e.g., [Huppert 1998, Theorem 13.1] for a proof.

Theorem 5.5 (Frobenius, Schur). *Let G be a finite group, and let $\chi \in \mathrm{Irr}(G)$ be the character of an irreducible complex representation $\rho\colon G \to \mathrm{GL}(V)$:*

(1) *If $\epsilon_2(\chi) = 0$, then $\chi \neq \overline{\chi}$, χ is not the character of an $\mathbb{R}[G]$-module, and there does not exist a G-invariant, $\mathbb{C}$-bilinear form $\neq 0$ on V. We say that ρ is a unitary representation.*

(2) *If $\epsilon_2(\chi) = 1$, then $\chi = \overline{\chi}$ is the character of some $\mathbb{R}[G]$-module, and there exists a G-invariant, $\mathbb{C}$-bilinear form which is symmetric and nonsingular, unique up to factors in $\mathbb{C}$. We say that ρ is an orthogonal representation.*

(3) *If $\epsilon_2(\chi) = -1$, then $\chi = \overline{\chi}$ is not the character of any $\mathbb{R}[G]$-module, and there exists a G-invariant, $\mathbb{C}$-bilinear form which is skew-symmetric and nonsingular, unique up to factors in $\mathbb{C}$. We say that ρ is a symplectic (or quaternionic) representation.*

In the sequel, we will say that a character is unitary (resp. orthogonal, symplectic) if it is the character of a unitary (resp. orthogonal, symplectic) representation.

Lemma 5.6. *Let L/F be a Galois extension of number fields for which AC and GRH hold. Define $G^+ := \mathrm{Gal}(L/F)$, and let $t^+\colon G^+ \to \mathbb{R}$ be a class function. For $\ell \in \mathbb{N}$, let $\eta \in \mathcal{S}_\delta$, $\psi \in \mathrm{Irr}(G^+)$, and let $\chi_1, \dots, \chi_{2\ell} \in \{\psi, \overline{\psi}\}$. If ψ is unitary then we have the estimate*

$$\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_\ell}>0\\ \gamma_{\chi_{\ell+1}},\dots,\gamma_{\chi_{2\ell}}<0\\ \forall\gamma\in\mathbb{R},\\ \#\{k\le 2\ell:\chi_k\in\{\psi,\overline{\psi}\},\gamma_{\chi_k}=\gamma\}=\#\{k\le 2\ell:\chi_k\in\{\psi,\overline{\psi}\},\gamma_{\chi_k}=-\gamma\}}} \prod_{k=1}^{2\ell} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big) \ge \max\big\{\ell!\, b_0(\psi; |\hat{\eta}|^2)^\ell - O_\eta(\ell!^2 \ell(\ell-1) b_0(\psi; |\hat{\eta}|^2)^{\ell-1}), 0\big\}, \tag{44}$$

where the γ_{χ_j} run through the multiset of imaginary parts of the zeros of $L(s, L/F, \psi)L(s, L/F, \overline{\psi})$ (with multiplicity).

If ψ is either orthogonal or symplectic then we have

$$\sum_{\substack{\gamma_1,\dots,\gamma_\ell>0\\ \gamma'_1,\dots,\gamma'_\ell<0\\ \forall\gamma\in\mathbb{R},\\ \#\{k\le\ell:\gamma_k=\gamma\}=\#\{k\le\ell:\gamma'_k=-\gamma\}}} \prod_{k=1}^{\ell} \hat{\eta}\Big(\frac{\gamma_k}{2\pi}\Big)\hat{\eta}\Big(\frac{\gamma'_k}{2\pi}\Big) \ge \max\big\{2^{-\ell}\ell!\, b_0(\psi; |\hat{\eta}|^2)^\ell - O_\eta(2^{-\ell}\ell!^2 \ell(\ell-1) b_0(\psi; |\hat{\eta}|^2)^{\ell-1}), 0\big\},$$

where the $\gamma_1, \dots, \gamma_\ell, \gamma'_1, \dots, \gamma'_\ell$ run through the imaginary parts of the zeros of $L(s, L/F, \psi)$ (with multiplicity).

Proof. We will split the proof into two cases, depending on whether ψ is real-valued (orthogonal or symplectic) or not (unitary). Because of the symmetry properties of zeros of $L(s, L/F, \psi)$, this will lead to two distinct combinatorial approaches.

Let us start with the case where ψ is unitary. In this case ψ and $\overline{\psi}$ are distinct irreducible characters of G. One of the difficulties comes from the fact that some γ may satisfy $L\big(\frac{1}{2}+i\gamma, L/F, \psi\big) = L\big(\frac{1}{2}+i\gamma, L/F, \overline{\psi}\big) = 0$. We have

$$\#\{k \le 2\ell : \chi_k \in \{\psi, \overline{\psi}\}, \gamma_{\chi_k} = \gamma\} = \#\{k \le 2\ell : \chi_k \in \{\psi, \overline{\psi}\}, \gamma_{\chi_k} = -\gamma\}.$$

We define the multisets

$$\Gamma_1(\psi) := \big\{\gamma > 0 \colon L\big(\tfrac{1}{2}+i\gamma, L/F, \psi\big) = L\big(\tfrac{1}{2}-i\gamma, L/F, \psi\big) = 0\big\}$$

and

$$\Gamma_2(\psi) := \big\{\gamma > 0 \colon L\big(\tfrac{1}{2}+i\gamma, L/F, \psi\big) = 0, \quad L\big(\tfrac{1}{2}-i\gamma, L/F, \psi\big) \neq 0\big\},$$

so that $\Gamma_1(\psi) \cap \Gamma_2(\psi) = \varnothing$, $\Gamma_2(\psi) \cap \Gamma_2(\overline{\psi}) = \varnothing$, and $\Gamma_1(\psi) \cup \Gamma_2(\psi)$ (respectively $\Gamma_1(\psi) \cup \Gamma_2(\overline{\psi})$) is a multiset whose elements are the positive imaginary parts of the nontrivial zeros of $L(s, L/F, \psi)$ (respectively $L(s, L/F, \overline{\psi})$). In the multiset $\Gamma_1(\psi)$, we define the multiplicity associated to γ as the sum of the multiplicity of $\frac{1}{2}+i\gamma$ for $L(s, L/F, \psi)$ and the multiplicity of $\frac{1}{2}-i\gamma$ for $L(s, L/F, \psi)$. Note that $\Gamma_1(\psi) = \Gamma_1(\overline{\psi})$. Now, among the γ_{χ_k} in the sum on the left-hand side of (44), there are $2r$ elements in $\Gamma_1(\psi)$ where $0 \le r \le \ell$. Thus we can write

$$\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_\ell} > 0 \\ \gamma_{\chi_{\ell+1}},\dots,\gamma_{\chi_{2\ell}} < 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le 2\ell : \chi_k \in \{\psi,\overline{\psi}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \le 2\ell : \chi_k \in \{\psi,\overline{\psi}\}, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2\ell} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big)$$

$$= \sum_{r=0}^{\ell} \binom{\ell}{r}^2 \Bigg(\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_r} \in \Gamma_1(\psi) \\ \gamma_{\chi_{r+1}},\dots,\gamma_{\chi_{2r}} \in -\Gamma_1(\psi) \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le 2r : \gamma_{\chi_k} = \gamma\} = \\ \#\{k \le 2r : \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2r} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big)\Bigg) \Bigg(\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{\ell-r}} \in \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi}) \\ \gamma_{\chi_{\ell-r+1}},\dots,\gamma_{\chi_{2\ell-2r}} \in -(\Gamma_2(\psi) \cup \Gamma_2(\overline{\psi})) \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le 2\ell-2r : \chi_k = \psi, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \le 2\ell-2r : \chi_k = \overline{\psi}, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2\ell-2r} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big)\Bigg). \tag{45}$$

Here, we use the convention that when $r = 0$, the first sum is equal to 1 whereas when $r = \ell$, the second sum is equal to 1.

Reindexing the innermost sum in (45), we see that

$$\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{\ell-r}} \in \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi}) \\ \gamma_{\chi_{\ell-r+1}},\dots,\gamma_{\chi_{2\ell-2r}} \in -(\Gamma_2(\psi) \cup \Gamma_2(\overline{\psi})) \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le 2\ell-2r : \chi_k = \psi, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \le 2\ell-2r : \chi_k = \overline{\psi}, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2\ell-2r} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big) = S_{2\ell-2r}(\boldsymbol{a}),$$

where $S_{2\ell-2r}(\boldsymbol{a})$ is defined in Lemma 5.3, with the choices

$$\Gamma := \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi}), \quad a_\gamma := \hat{\eta}\Big(\frac{\gamma}{2\pi}\Big).$$

By Lemma 5.3, it is

$$\geq \max\big\{(\ell-r)!\, b_2(\psi;\,|\hat\eta|^2)^{\ell-r} - O_\eta((\ell-r)!^2(\ell-r)(\ell-r-1)b_2(\psi;\,|\hat\eta|^2)^{\ell-r-1}),\, 0\big\},$$

where $b_2(\psi;\,|\hat\eta|^2)$ is the contribution of $\gamma\in\Gamma_2(\psi)\cup\Gamma_2(\overline{\psi})$ in $b_0(\psi;\,|\hat\eta|^2)$ so that

$$b_0(\psi;\,|\hat\eta|^2)+b_0(\overline{\psi};\,|\hat\eta|^2)=b_1(\psi;\,|\hat\eta|^2)+b_2(\psi;\,|\hat\eta|^2),$$

with

$$b_1(\psi;\,|\hat\eta|^2)=2\sum_{\gamma\in\Gamma_1(\psi)}\left|\hat\eta\left(\frac{\gamma}{2\pi}\right)\right|^2,\quad b_2(\psi;\,|\hat\eta|^2)=2\sum_{\gamma\in\Gamma_2(\psi)\cup\Gamma_2(\overline{\psi})}\left|\hat\eta\left(\frac{\gamma}{2\pi}\right)\right|^2.$$

In the same fashion, we may estimate the first bracketed sum on the right-hand side of (45) using Lemma 5.3, with the choices

$$\Gamma:=\Gamma_1(\psi),\quad a_\gamma:=\hat\eta\left(\frac{\gamma}{2\pi}\right).$$

By the same argument, the first sum is

$$\geq \max\{r!\, b_1(\psi;\,|\hat\eta|^2)^r - O_\eta(r!^2 r(r-1)b_1(\psi;\,|\hat\eta|^2)^{r-1}),\,0\}.$$

Summing over r yields the claimed estimate.

If ψ is either orthogonal or symplectic, then it is real-valued and thus the combinatorics are simpler in this case. Indeed, the claimed bound follows at once from Lemma 5.3 with the choices

$$\Gamma:=\big\{\gamma>0: L\big(\tfrac12+i\gamma,\,L/F,\,\psi\big)=0\big\},\quad a_\gamma:=\hat\eta\left(\frac{\gamma}{2\pi}\right). \qquad \square$$

Lemma 5.7. *Let L/F be a Galois extension of number fields for which AC and GRH hold. Define $G^+:=\mathrm{Gal}(L/F)$, and let $t^+\colon G^+\to\mathbb{R}$ be a class function. Assume that $\hat t^+\in\mathbb{R}_{\geq 0}$ and let $\eta\in\mathcal{S}_\delta$, $\Phi\in\mathcal{U}$. For $m\in\mathbb{N}$, we have the lower bound*

$$\widetilde{D}_{2m}(U,L/F;t^+,\eta,\Phi)\geq \mu_{2m}\nu(L/F,t^+;\eta)^m\big(1+O_\eta(m^2m!\,w_4(L/F,t^+;\eta))\big),$$

where we recall (7) *and*

$$w_4(L/F,t^+;\eta):=\frac{\sum_{\chi\in\mathrm{Irr}(G^+)}|\hat t^+(\chi)|^4 b_0(\chi;\,\hat\eta^2)}{\big(\sum_{\chi\in\mathrm{Irr}(G^+)}|\hat t^+(\chi)|^2 b_0(\chi;\,\hat\eta^2)\big)^2}. \tag{46}$$

Proof. Firstly, in (34), we may replace $\mathrm{Irr}(G^+)$ by $C_t:=\mathrm{supp}(\widehat{t^+})\subset\mathrm{Irr}(G^+)$. For simplicity, let us write (since t is real-valued)

$$C_t=\{\psi_1,\psi_2,\dots,\psi_{r_1},\psi_{r_1+1},\overline{\psi_{r_1+1}},\psi_{r_1+2},\dots,\psi_{r_1+r_2},\overline{\psi_{r_1+r_2}}\},$$

where $\psi_1,\dots\psi_{r_1}$ are real and $\psi_{r_1+1},\dots,\psi_{r_1+r_2}$ are complex. Note that C_t depends only on G and t, and $r_1+2r_2=|C_t|$. Given a vector $\boldsymbol{\chi}=(\chi_1,\dots\chi_{2m})\in(C_t)^{2m}$, define

$$E_j(\boldsymbol{\chi}):=\{1\leq k\leq 2m\colon\, \chi_k\in\{\psi_j,\overline{\psi_j}\}\}\quad (1\leq j\leq r_1+r_2),$$

$\ell_j(\boldsymbol{\chi}):=|E_j(\boldsymbol{\chi})|$. Note that $\sum_{j=1}^{r_1+r_2}\ell_j(\boldsymbol{\chi})=2m$.

Secondly, by positivity of $\widehat{t^+}$ and $\hat{\eta}$, we may obtain a lower bound on $\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi)$ by restricting the sum over characters to those $\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m})$ that are elements of $(C_t)^{2m}$ and $(\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}})$ for which for any $j \le r_1 + r_2$ and $\gamma \in \mathbb{R}$ we have

$$|\{k \in E_j(\boldsymbol{\chi})\colon \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\}| = |\{k \in E_j(\boldsymbol{\chi})\colon \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}|.$$

Finally, we may further impose that $k_j(\boldsymbol{\chi}) := \frac{1}{2}\ell_j(\boldsymbol{\chi}) \in \mathbb{N}$, and we may restrict the sum over characters to the subset $\mathcal{C}_{t,2m}$ of vectors of characters $\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in C_t^{2m}$ which satisfy $|\{\ell \le 2m : \chi_\ell = \psi_j\}| = |\{\ell \le 2m : \chi_\ell = \overline{\psi_j}\}|$, for every $r_1 + 1 \le j \le r_1 + r_2$. We will also use the fact that for any $j \le r_1 + r_2$ and for all $(\chi_1, \dots, \chi_{2k_j})$ and $(\gamma_{\chi_1}, \dots, \gamma_{\chi_{2k_j}})$ appearing in the index set of the double sum (34), we have that

$$\begin{aligned}\#\{\ell \in E_j(\boldsymbol{\chi})\} &= \sum_{\gamma \in \mathbb{R}_{>0}} \#\{\ell\colon \chi_\ell \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_\ell} = \gamma\} + \sum_{\gamma \in \mathbb{R}_{<0}} \#\{\ell\colon \chi_\ell \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_\ell} = \gamma\} \\ &= 2 \sum_{\gamma \in \mathbb{R}_{>0}} \#\{\ell\colon \chi_\ell \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_\ell} = \gamma\}.\end{aligned}$$

As a result, one deduces the following lower bound:

$$\begin{aligned}\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi) \ge \frac{1}{2\int_0^\infty \Phi} &\sum_{\substack{\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in \mathcal{C}_{t,2m} \\ \forall j, k_j(\boldsymbol{\chi}) \in \mathbb{N}}} \Big(\prod_{j=1}^{2m} \hat{t}^+(\chi_j) \Big) \\ &\times \sum_{\substack{\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}} \neq 0 \\ \#\{k \in E_j(\boldsymbol{\chi}) : \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \in E_j(\boldsymbol{\chi}) : \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}}} \widehat{\Phi}\Big(\frac{U}{2\pi}(\gamma_{\chi_1} + \dots + \gamma_{\chi_{2m}}) \Big) \prod_{j=1}^{2m} \hat{\eta}\Big(\frac{\gamma_{\chi_j}}{2\pi} \Big).\end{aligned}$$

At this point, we notice that the conditions in the inner sum automatically imply that $\gamma_{\chi_1} + \dots + \gamma_{\chi_n} = 0$, resulting in the bound

$$\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi) \ge \sum_{\substack{\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in \mathcal{C}_{t,2m} \\ \forall j, k_j(\boldsymbol{\chi}) \in \mathbb{N}}} \Big(\prod_{j=1}^{2m} \hat{t}^+(\chi_j) \Big) \sum_{\substack{\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}} \neq 0 \\ \forall j \le r_1 + r_2, \forall \gamma \in \mathbb{R}, \\ \#\{k \in E_j(\boldsymbol{\chi}) : \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \in E_j(\boldsymbol{\chi}) : \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}}} \prod_{j=1}^{2m} \hat{\eta}\Big(\frac{\gamma_{\chi_j}}{2\pi} \Big).$$

Next we stratify the first sum according to the values assumed by $k_j(\boldsymbol{\chi})$. Given a vector $\boldsymbol{k} = (k_1, \dots, k_{r_1+r_2}) \in \mathbb{N}^{r_1+r_2}$ such that $k_1 + \dots + k_{r_1+r_2} = m$, we need to evaluate the sum

$$D(\boldsymbol{k}) := \sum_{\substack{\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in \mathcal{C}_{t,2m} \\ \forall j, k_j(\boldsymbol{\chi}) = k_j}} \Big(\prod_{j=1}^{2m} \hat{t}^+(\chi_j) \Big) \sum_{\substack{\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}} \neq 0 \\ \forall j \le r_1 + r_2, \forall \gamma \in \mathbb{R}, \\ \#\{k \in E_j(\boldsymbol{\chi}) : \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \in E_j(\boldsymbol{\chi}) : \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}}} \prod_{j=1}^{2m} \hat{\eta}\Big(\frac{\gamma_{\chi_j}}{2\pi} \Big).$$

Now, note that since t^+ and $\hat{t}^+$ are real-valued, we have that

$$\hat{t}^+(\chi)\hat{t}^+(\overline{\chi}) = \hat{t}^+(\chi)\overline{\hat{\bar{t}}(\chi)} = (\hat{t}^+(\chi))^2.$$

Hence, after reindexing we obtain the identity

$$D(\boldsymbol{k}) = \binom{2m}{2k_1, \dots, 2k_{r_1+r_2}} \prod_{j=1}^{r_1+r_2} \Bigg((\hat{t}^+(\psi_j))^{2k_j} \sum_{\substack{(\chi_1,\dots,\chi_{2k_j}) \in \mathcal{C}_{t,2k_j} \\ \forall \ell \le 2k_j, \chi_\ell \in \{\psi_j, \overline{\psi_j}\}}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{2k_j}} \neq 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le 2k_j : \gamma_{\chi_k} = \gamma\} = \\ \#\{k \le 2k_j : \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2k_j} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big) \Bigg).$$

Let us now evaluate the inner sum

$$\sigma_j(k_j) := \sum_{\substack{(\chi_1,\dots,\chi_{2k_j}) \in \mathcal{C}_{t,2k_j} \\ \forall \ell \le 2k_j, \chi_\ell \in \{\psi_j, \overline{\psi_j}\}}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{2k_j}} \neq 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le 2k_j : \gamma_{\chi_k} = \gamma\} = \\ \#\{k \le 2k_j : \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2k_j} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big).$$

Reindexing, we obtain the identity

$$\sigma_j(k_j) = \binom{2k_j}{k_j} \sum_{\substack{\gamma_1,\dots,\gamma_{k_j} > 0, \gamma'_1,\dots,\gamma'_{k_j} < 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le k_j : \gamma_k = \gamma\} = \#\{k_j < k \le 2k_j : \gamma'_k = -\gamma\}}} \prod_{k=1}^{k_j} \hat{\eta}\Big(\frac{\gamma_k}{2\pi}\Big) \eta\Big(\frac{\gamma'_k}{2\pi}\Big),$$

where the γ_j and the γ'_j are running over the positive (respectively negative) imaginary parts of the zeros of $L(s, L/K, \psi_j) L(s, L/K, \overline{\psi_j})$. Applying Lemma 5.6, we deduce that for $j \ge r_1 + 1$ (i.e., ψ_j is unitary),

$$\sigma_j(k_j) \ge 2^{k_j} \mu_{2k_j} b_0(\psi_j; |\hat{\eta}|^2)^{k_j} \max\bigg\{ 1 - O_\eta\Big(\frac{k_j!\, k_j(k_j-1)}{b_0(\psi_j; |\hat{\eta}|^2)} \Big), 0 \bigg\},$$

since

$$\binom{2k_j}{k_j} k_j! = 2^{k_j} \mu_{2k_j}.$$

Now, if ψ_j is either orthogonal or symplectic (i.e., $j \le r_1$), then we may fix the sign of the imaginary parts γ_{χ_j} and deduce that

$$\sigma_j(k_j) = \binom{2k_j}{k_j} \sum_{\substack{\gamma_1,\dots,\gamma_{k_j} > 0, \gamma'_1,\dots,\gamma'_{k_j} < 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \le k_j : \gamma_k = \gamma\} = \#\{k_j < k \le 2k_j : \gamma'_k = -\gamma\}}} \prod_{k=1}^{2k_j} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big).$$

We invoke Lemma 5.6 once more and deduce the bound

$$\sigma_j(k_j) \ge \mu_{2k_j} b_0(\psi_j; |\hat{\eta}|^2)^{k_j} \max\bigg\{ 1 - O_\eta\Big(\frac{k_j!\, k_j(k_j-1)}{b_0(\psi_j; |\hat{\eta}|^2)} \Big), 0 \bigg\}.$$

Putting everything together, we deduce the overall bound

$$\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi) \ge \sum_{\substack{k_1,\dots,k_{r_1+r_2} \in \mathbb{N} \\ k_1 + \cdots + k_{r_1+r_2} = m}} \binom{2m}{2k_1, \dots, 2k_{r_1+r_2}} \prod_{\ell=1}^{r_1} (\mu_{2k_\ell} \hat{t}^+(\psi_j)^{2k_\ell} b_0(\psi_\ell; |\hat{\eta}|^2)^{k_\ell})$$
$$\times \prod_{\ell=r_1+1}^{r_1+r_2} (2^{k_\ell} \mu_{2k_\ell} \hat{t}^+(\psi_\ell)^{2k_\ell} b_0(\psi_\ell; |\hat{\eta}|^2)^{k_\ell}) \prod_{\ell=1}^{r_1+r_2} \max\bigg\{ 1 - O_\eta\Big(\frac{k_\ell!\, k_\ell(k_\ell - 1)}{b_0(\psi_\ell; |\hat{\eta}|^2)} \Big), 0 \bigg\}. \quad (47)$$

Let us first evaluate the main term in this expression. By the identity

$$\binom{2m}{2k_1, \ldots, 2k_{r_1+r_2}} \prod_{j=1}^{r_1+r_2} \mu_{2k_j} = \binom{m}{k_1, \ldots, k_{r_1+r_2}} \mu_{2m}$$

and the multinomial theorem, the main term is equal to

$$\mu_{2m}\biggl(\sum_{\ell=1}^{r_1} \hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell; |\hat{\eta}|^2) + 2\sum_{\ell=r_1}^{r_1+r_2} \hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell; |\hat{\eta}|^2)\biggr)^m = \mu_{2m}\nu(L/F, t^+; \eta)^m,$$

which is equal to the claimed main term.

As for the error terms in (47), recall first that they vanish whenever $k_\ell \in \{0, 1\}$ (see Remark 5.4). Next we handle the contribution of indices $k_j \geq 2$ to the error terms. Using the identity

$$\prod_{\ell=1}^{r_1+r_2} \max\{1 - x_\ell, 0\} \geq 1 - \sum_{j=1}^{r_1+r_2} x_j \quad (x_\ell \geq 0),$$

we see that we need to multiply the main term in (47) by

$$\prod_{\ell=1}^{r_1+r_2} \max\biggl\{1 + O\biggl(\frac{k_\ell!\, k_\ell(k_\ell - 1)}{b_0(\psi_\ell; |\hat{\eta}|^2)}\biggr), 0\biggr\} \geq 1 + O\biggl(\sum_{\substack{j=1\\ k_j \geq 2}}^{r_1+r_2} \frac{k_j!\, k_j(k_j - 1)}{b_0(\psi_j; |\hat{\eta}|^2)}\biggr).$$

We obtain an error term which is

$$\ll \mu_{2m} \sum_{j=1}^{r_1+r_2} \frac{1}{b_0(\psi_j, |\hat{\eta}|^2)} \sum_{\substack{k_1,\ldots,k_{r_1+r_2} \in \mathbb{N}\\ k_1+\cdots+k_{r_1+r_2}=m\\ k_j \geq 2}} k_j!\, k_j(k_j - 1)\binom{m}{k_1, \ldots, k_{r_1+r_2}}$$
$$\times \prod_{\ell=1}^{r_1}(\hat{t}^+(\psi_\ell)^{2k_\ell} b_0(\psi_\ell; |\hat{\eta}|^2)^{k_\ell}) \prod_{\ell=r_1+1}^{r_1+r_2} (2^{k_\ell}\hat{t}^+(\psi_\ell)^{2k_\ell} b_0(\psi_\ell; |\hat{\eta}|^2)^{k_\ell}).$$

Finally, notice that

$$k_j(k_j - 1)\binom{m}{k_1, \ldots, k_{r_1+r_2}} = m(m - 1)\binom{m-2}{k_1, \ldots, k_j-2, \ldots, k_{r_1+r_2}},$$

and hence the error term above is

$$\ll m^2 m!\, \mu_{2m}\biggl(\sum_{j=1}^{r_1+r_2} \hat{t}^+(\psi_j)^4 b_0(\psi_j; |\hat{\eta}|^2)\biggr)\biggl(\sum_{\ell=1}^{r_1}\hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell; |\hat{\eta}|^2)+2\sum_{\ell=r_1}^{r_1+r_2} \hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell; |\hat{\eta}|^2)\biggr)^{m-2}$$
$$\ll \mu_{2m}\nu(L/F, t^+; \eta)^{m-2} m^2 m!\biggl(\sum_{j=1}^{r_1+r_2} \hat{t}^+(\psi_j)^4 b_0(\psi_j; |\hat{\eta}|^2)\biggr). \qquad \square$$

Proof of Theorem 1.1. The claimed bound (9) follows from combining Lemmas 5.2 and 5.7. □

Proof of Theorem 1.4. The first part follows from Lemmas 4.2 and 4.5. More precisely, the bound

$$\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 b_0(\chi; \hat{\eta}^2) \ll_\eta \sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}(\chi)|^4 \log(A(\chi) + 2)$$

follows directly from Lemma 4.2.

Next (12) follows from Lemma 4.3. We will also apply this lemma to prove the last claimed bound on $w_4(L/F, t^+; \eta)$. Note that by Lemmas 3.2 and 4.2 we have the upper bound

$$\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 b_0(\chi; \hat{\eta}^2) \ll_\eta \lambda_{1,4}(t^+)[F:\mathbb{Q}] \log(\mathrm{rd}_L + 2).$$

Lemma 4.3 then implies that

$$w_4(L/F, t^+; \eta) \ll_\eta \frac{1}{[F:\mathbb{Q}]\log(\mathrm{rd}_L+2)} \frac{\lambda_{1,4}(t^+)}{\lambda_{1,2}(t^+)^2}\bigg(1 - S_{t^+} - O\bigg(\frac{1}{\log_2(\mathrm{rd}_L+2)}\bigg)\bigg)^{-2}.$$

Moreover, we have the trivial bound

$$\frac{\lambda_{1,4}(t^+)}{\lambda_{1,2}(t^+)^2} \le \frac{\lambda_{2,4}(t^+)}{\lambda_{1,2}(t^+)^2} \le 1.$$

The result follows. □

Finally, we prove Corollaries 1.10 and 1.11.

Proof of Corollary 1.10. We will argue by contradiction. Assume otherwise that for all large enough x,

$$|\psi(x; L/K, t) - \hat{t}(1)x| \le \varepsilon(x) x^{1/2} C_{F,L,t^+}^{1/2},$$

where

$$C_{F,L,t^+} = [F:\mathbb{Q}]\log(\mathrm{rd}_L)\lambda_{1,2}(t^+)\bigg(1 - S_{t^+} - \frac{A}{\log_2(\mathrm{rd}_L+2)}\bigg),$$

$A > 0$ is an absolute and large enough constant and $\varepsilon(x)$ monotonically tends to zero as x tends to ∞. Let $\eta = \eta_0 \star \eta_0$, where η_0 is a nontrivial smooth even function supported in $[-1, 1]$. We then have that for large enough x,

$$\begin{aligned}\psi_\eta(x; L/K, t) - \hat{t}(1)x^{1/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big) &= \int_0^\infty \frac{\eta(\log(y/x))}{y^{1/2}} \mathrm{d}(\psi(y; L/K, t) - \hat{t}(1)y) \\ &= -\int_{\mathrm{e}^{-2}x}^{\mathrm{e}^{2}x} \frac{\eta'(\log(y/x)) - \frac{1}{2}\eta(\log(y/x))}{y^{3/2}} (\psi(y; L/K, t) - \hat{t}(1)y)\,\mathrm{d}y \\ &\ll \varepsilon(\mathrm{e}^{-2}x) C_{F,L,t^+}^{1/2}.\end{aligned}$$

Now, for any large enough $0 < U_1 < U_2$, this implies the bound

$$\int_{U_1}^{U_2} \big(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)\big)^2 \mathrm{d}u \ll \varepsilon(\mathrm{e}^{-2}\mathrm{e}^{U_1})^2 (U_2 - U_1) C_{F,L,t^+}.$$

Moreover, (32) implies that

$$\psi_\eta(\mathrm{e}^u; L/K, t) = \psi_\eta(\mathrm{e}^u; L/F, t^+) = \sum_{\chi \in \mathrm{Irr}(G^+)} \hat{t}^+(\chi)\psi_\eta(\mathrm{e}^u; L/F, \chi).$$

We may apply Lemma 4.1 in which we can bound the second term on the right-hand side trivially (under GRH), resulting in the overall bound (recall that $\hat{t}(1) = \widehat{t^+}(1)$)

$$\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta(\tfrac{1}{2}) \ll \sum_{\chi\in\mathrm{Irr}(G^+)} |\hat{t}^+(\chi)| \log(A(\chi)+2) \ll \lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L+2).$$

This then implies that

$$\int_0^{U_1} \big(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)\big)^2 \,\mathrm{d}u \ll U_1(\lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L+2))^2.$$

As a result, picking any even integrable function Φ supported in $[-1, 1]$, we deduce that

$$M_2(U_2, L/K, t, \eta, \Phi) \ll \frac{U_1}{U_2}(\lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L))^2 + \varepsilon(\mathrm{e}^{-2}\mathrm{e}^{U_1})^2 \frac{U_2-U_1}{U_2} C_{F,L,t^+}.$$

Picking for instance $U_2 = U_1^2$, this will eventually contradict the lower bound in Corollary 1.9 (combined with Theorem 1.4). Indeed, the bound $S_{t^+} \le 1 - \kappa(\log_2(\mathrm{rd}_L+2))^{-1}$ implies that rd_L is large enough (since κ itself is large enough), which in turns implies that $w_4(L/F, t^+, \eta)$ is small enough by Theorem 1.4.

We now show that there exists a value $\mathrm{e}^{U_1} \le x \le \mathrm{e}^{U_2}$ such that

$$|\psi(x; L/K, t) - \hat{t}(1)x| \gg x^{1/2} C_{F,L,t^+}^{1/2},$$

where $U_1 = U$ and $U_2 = \beta_{L,F,K,t}U$. Assume otherwise that for all $\varepsilon > 0$ and for all extensions L/K and class functions t, there exists arbitrarily large values of U (depending on ε, L/K and t) for which for all $x \in [\mathrm{e}^{U_1}, \mathrm{e}^{U_2}]$,

$$|\psi(x; L/K, t) - \hat{t}(1)x| \le \varepsilon x^{1/2} C_{F,L,t^+}^{1/2}.$$

One can deduce following the lines above that

$$M_2(\mathrm{e}^{-2}U_2, L/K, t^+, \eta, \Phi) \ll \frac{U_1}{U_2}(\lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L))^2 + \varepsilon C_{F,L,t^+}.$$

Once more, this will contradict Corollary 1.9 if

$$U_2 > \kappa_2[F:\mathbb{Q}]\log(\mathrm{rd}_L+2)\log_2(\mathrm{rd}_L+2)\lambda_{1,1}(t^+)^2/\lambda_{1,2}(t^+),$$
$$U_1 = \kappa_1 U_2 \lambda_{1,2}(t^+)/([F:\mathbb{Q}]\lambda_{1,1}(t^+)^2\log(\mathrm{rd}_L+2)\log_2(\mathrm{rd}_L+2)),$$

where $\kappa_2 > 0$ is large enough and $\kappa_1 > 0$ is small enough (both in absolute terms). □

Proof of Corollary 1.11. The proof goes along the lines of that of Corollary 1.10. By Lemma 5.1 applied to the tower $L/L/K$ and Lemma 5.2 applied to the trivial tower $L/L/L$,

$$\begin{aligned}\widetilde{M}_n(U, L/K; |G|\mathbf{1}_e, \eta, \Phi) &= \widetilde{M}_n(U, L/L; \mathbf{1}_e, \eta, \Phi)\\ &= \widetilde{D}_n(U, L/L; \mathbf{1}_e, \eta, \Phi) + O\bigg(\frac{(\kappa_\eta[K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^n}{U}\bigg).\end{aligned}$$

Moreover, by Lemma 5.7,

$$\widetilde{D}_{2m}(U, L/L; \mathbf{1}_e, \eta, \Phi) \ge \mu_{2m}\nu(L/L, \mathbf{1}_e; \eta)^m(1 + O_\eta(m^2 m!\, w_4(L/L, \mathbf{1}_e; \eta))),$$

where

$$\nu(L/L, \mathbf{1}_e; \eta) = b_0(\chi_0; \hat{\eta}^2), \quad w_4(L/L, \mathbf{1}_e; \eta) = \frac{1}{b_0(\chi_0; \hat{\eta}^2)}.$$

Now, Lemma 4.2 implies that

$$b(\chi; \hat{\eta}^2) = \hat{h}(0)\log d_L + O_\eta([L:\mathbb{Q}]) = \hat{h}(0)\log d_L\biggl(1 + O\biggl(\frac{1}{\log(\mathrm{rd}_L + 2)}\biggr)\biggr), \tag{48}$$

resulting in the overall bound

$$\begin{aligned}&\widetilde{M}_{2m}(U, L/K; |G|\mathbf{1}_e, \eta, \Phi)\\ &\quad\geq \mu_{2m}(\hat{h}(0)\log d_L)^m\biggl(1 + O_\eta\biggl(\frac{m}{\log(\mathrm{rd}_L + 2)} + \frac{m^2 m!}{\log(d_L + 2)}\biggr)\biggr) + O\biggl(\frac{(\kappa_\eta \log(d_L + 2))^{2m}}{U}\biggr).\end{aligned}$$

The rest of the proof is similar. □

6. Application to specific extensions and class functions: proofs

This section is dedicated to the proofs of our results for specific Galois extensions, which were stated in Section 2. The statements and their proofs make use of the terminology coming from the classical representation theory of finite groups and we refer the reader, e.g., to [Huppert 1998] or [Serre 1977] for recollections on the necessary background.

6.1. ***Moments for prime ideals in ray class groups.*** We prove Proposition 2.1.

Proof of Proposition 2.1. We apply Theorem 1.1 for $K = F$, and $L = L_{\mathfrak{m}}$. In particular we have $G = G^+ \simeq \mathrm{Cl}_{\mathfrak{m}}(K)$. For the choice $t = h_{K,\mathfrak{m}}\mathbf{1}_{[\mathfrak{a}]}$, where $[\mathfrak{a}]$ is any fixed class in $\mathrm{Cl}_{\mathfrak{m}}(K)$, one computes the norms (6) for all positive integers i, j:

$$\lambda_{i,j}(t) = h_{K,\mathfrak{m}},$$

since $\hat{t}(\chi) = \overline{\chi([\mathfrak{a}])}$ for every irreducible character (all of which have degree 1) of $\mathrm{Cl}_{\mathfrak{m}}(K)$. For the same reason, one has $S_t = 0$ (recall (11)), and if $[\mathfrak{a}] = [\mathfrak{e}]$, then $\hat{t}(\chi)$ is positive (and constant, equal to 1) for every character χ. Therefore applying Theorem 1.4 yields the upper bound

$$w_4(L_{\mathfrak{m}}/K, t; \eta) \ll \frac{1}{\log d_{L_{\mathfrak{m}}}}.$$

As for the variance, Theorem 1.4 gives

$$\left|\frac{\nu(L_{\mathfrak{m}}/K, t; \eta)}{\alpha(|\hat{\eta}|^2)\log d_{L_{\mathfrak{m}}}} - 1\right| \ll \frac{1}{\log_2(\mathrm{rd}_{L_{\mathfrak{m}}} + 2)}.$$

Putting this together, Theorem 1.1 gives that for fixed $m \in \mathbb{N}$,

$$\begin{aligned}\widetilde{M}_{2m}(U, L_{\mathfrak{m}}/K; t, \eta, \Phi) &\geq \mu_{2m}\nu(L_{\mathfrak{m}}/K, t; \eta)^m(1 + o_{\mathrm{rd}_{L_{\mathfrak{m}}}\to\infty}(1))\\ &\geq \mu_{2m}(\alpha(|\hat{\eta}|^2)\log d_{L_{\mathfrak{m}}})^m(1 + o_{\mathrm{rd}_{L_{\mathfrak{m}}}\to\infty}(1)),\end{aligned}$$

provided $((\log d_{L_{\mathfrak{m}}})^m/U) \to 0$ as $d_{L_{\mathfrak{m}}} \to \infty$. □

6.2. D_n-examples. In this section, we prove Propositions 2.2 and 2.3. With notation as in these statements, we recall that among the $\frac{1}{2}(n+3)$ isomorphism classes of irreducible representations of D_n, exactly two have degree 1: the trivial representation and the lift of the nontrivial character of $D_n/\langle\sigma\rangle$ which is defined by

$$\psi(\sigma^j)=1,\quad \psi(\tau\sigma^k)=-1.$$

The remaining $\frac{1}{2}(n-1)$ irreducible representations of D_n have degree 2; the associated characters are given by

$$\chi_h(\sigma^j)=2\cos(2\pi hj/n),\quad \chi_h(\tau\sigma^k)=0,\quad \bigl(h\in\bigl\{1,\dots,\tfrac{1}{2}(n-1)\bigr\}\bigr).$$

Proof of Proposition 2.2. First note the following useful fact: for any integer j such that $n\nmid j$ we have

$$\frac{1}{2}\sum_{h=1}^{(n-1)/2}\chi_h(\sigma^j)=\sum_{h=1}^{(n-1)/2}\cos\frac{2\pi hj}{n}=\frac{\sin(\pi j/2-\pi j/(2n))}{\sin(\pi j/n)}\cos\Bigl(\frac{\pi j}{2}+\frac{\pi j}{2n}\Bigr)=-\frac{1}{2}. \tag{49}$$

(1) If one considers $t=|D_n|\mathbf{1}_e$, the indicator function of the neutral element of D_n, then $\hat{t}(\chi)=\chi(1)$ for any $\chi\in\mathrm{Irr}(D_n)$ and thus one computes for any $a\in D_n$

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(a)|\hat{t}(\chi)|^2=1+\psi(a)+4\sum_{h=1}^{(n-1)/2}\chi_h(a).$$

If $a=e$, this sum equals $\lambda_{1,2}(t)=2+4(n-1)=4n-2$. If a is in the conjugacy class of τ, then this sum vanishes, and finally if $a=\sigma^j$, then the sum equals -2 by (49). Therefore $S_t=1/(2n-1)$.

(2) Consider the class function $t=\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$ (for which $\hat{t}(\chi)=\chi(\sigma)/n$ for any $\chi\in\mathrm{Irr}(D_n)$). One has for any $a\in D_n$,

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(a)|\hat{t}(\chi)|^2=\frac{1+\psi(a)}{n^2}+\frac{4}{n^2}\sum_{h=1}^{(n-1)/2}\chi_h(a)\Bigl(\cos\frac{2\pi h}{n}\Bigr)^2.$$

If a is conjugate to τ then this quantity vanishes. Also, for any $j'\in\bigl\{1,\dots,\frac{1}{2}(n-1)\bigr\}$, one has

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(\sigma^{j'})|\hat{t}(\chi)|^2=\frac{2}{n^2}+\frac{8}{n^2}\sum_{h=1}^{(n-1)/2}\cos\frac{2\pi hj'}{n}\Bigl(\cos\frac{2\pi h}{n}\Bigr)^2.$$

By linearizing the product on the right-hand side, we see that the maximal value of the left-hand side is attained at $j'=2$. Using (49) we can compute

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(\sigma^2)|\hat{t}(\chi)|^2=\frac{2}{n^2}+\frac{4}{n^2}\sum_{h=1}^{(n-1)/2}\biggl(\cos\frac{4\pi h}{n}+\Bigl(\cos\frac{4\pi h}{n}\Bigr)^2\biggr)=\frac{n-2}{n^2}.$$

Moreover one has

$$\lambda_{1,2}(t)=\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(1)|\hat{t}(\chi)|^2=\frac{2}{n^2}+\frac{4}{n^2}\sum_{h=1}^{(n-1)/2}\Bigl(1+\cos\frac{4\pi h}{n}\Bigr)=\frac{2(n-1)}{n^2}.$$

We conclude that $S_t=(1-2/n)/(2(1-1/n))$.

(3) Finally consider $t = 2\mathbf{1}_e + \mathbf{1}_{\{\sigma,\sigma^{-1}\}}$. Unlike $\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$, this class function has nonnegative Fourier coefficients. Indeed one has

$$\hat{t}(1) = \hat{t}(\psi) = \frac{2}{n}, \quad \hat{t}(\chi_h) = \frac{2}{n}\left(1 + \cos\frac{2\pi h}{n}\right) = \frac{4}{n}\left(\cos\frac{4\pi h}{n}\right)^2 \quad \left(1 \le h \le \tfrac{1}{2}(n-1)\right).$$

Therefore one has for any $a \in D_n$,

$$\sum_{\chi \in \mathrm{Irr}(D_n)} \chi(a)|\hat{t}(\chi)|^2 = \frac{4(1+\psi(a))}{n^2} + \frac{16}{n^2}\sum_{h=1}^{(n-1)/2} \chi_h(a)\left(\cos\frac{4\pi h}{n}\right)^4.$$

Using (49), one finds that this sum equals $(2/n)(3-4/n)$ if $a = e$. If a is in the conjugacy class of τ, the sum vanishes. If $a = \sigma^j$ and assuming $n \ge 5$, applying standard trigonometric identities as well as (49), we see that this sum is equal to

$$\begin{aligned}\frac{2}{n^2} + \frac{32}{n^2}\bigg\{&\frac{1}{4}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv -4 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv -4 \bmod n}\Big) + \frac{1}{4}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv 4 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv 4 \bmod n}\Big)\\ &+ \frac{1}{16}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv -8 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv -8 \bmod n}\Big) + \frac{1}{16}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv 8 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv 8 \bmod n}\Big)\bigg\}.\end{aligned}$$

Clearly, this quantity is maximized when $j = \pm 4 \bmod n$, in which case it is equal to $(2/n)(2-4/n)$. Overall one concludes that $S_t \le (2-4/n)/(3-4/n) < \frac{2}{3}$. □

Proof of Proposition 2.3. Set $t = |D_n|\mathbf{1}_e$. One has

$$\lambda_{1,1}(t) = \sum_{\chi \in \mathrm{Irr}(D_n)} \chi(1)^2 = |D_n| = 2n, \quad \lambda_{1,4}(t) = \sum_{\chi \in \mathrm{Irr}(D_n)} \chi(1)^5 = 2 + \tfrac{1}{2}(32(n-1)) = 2(8n-7).$$

We apply Theorem 1.4 for $K = F = \mathbb{Q}$ and $L/\mathbb{Q}$ a D_n-extension. Therefore $G^+ = G$ and $t^+ = t$. Moreover AC holds for L since it is a supersolvable extension of $\mathbb{Q}$. Therefore applying Theorem 1.4 we deduce

$$w_4(L/\mathbb{Q}, t; \eta) \ll \frac{1}{n \log \mathrm{rd}_L}.$$

As for the variance, Theorem 1.4 gives

$$\left|\frac{\nu(L/\mathbb{Q}, t; \eta)}{\alpha(|\hat{\eta}|^2)(4n-2)\log \mathrm{rd}_L} - 1\right| \le \frac{1}{2n-1} + O\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right).$$

Putting this together, Theorem 1.1 gives that for fixed $m \in \mathbb{N}$,

$$\begin{aligned}\widetilde{M}_{2m}(U, L/\mathbb{Q}; t, \eta, \Phi) &\ge \mu_{2m}\nu(L/K, t; \eta)^m(1 + o_{\mathrm{rd}_L\to\infty}(1))\\ &\ge \mu_{2m}\Big(\alpha(|\hat{\eta}|^2)\Big(2 - \frac{1}{n}\Big)\log d_L\Big)^m(1 + o_{\mathrm{rd}_L\to\infty}(1)),\end{aligned}$$

as soon as $((\log d_L)^m/U) \to 0$ as $d_L \to \infty$. □

6.3. ***Example of a radical extension.*** In this section we prove Propositions 2.4 and 2.5.

Notation is as in Section 2.3. The nontrivial conjugacy classes of G are

$$U := \left\{ \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} : \star \neq 0 \right\}, \quad T_c := \left\{ \begin{pmatrix} c & \star \\ 0 & 1 \end{pmatrix} \star \in \mathbb{F}_p \right\} \quad (c \neq 1).$$

One has $|U| = p-1$ and $|T_c| = p$ for every $c \in \mathbb{F}_p \setminus \{0, 1\}$. As for the characters of G, exactly $p-1$ of them have degree 1: these are the lifts of Dirichlet characters χ modulo p

$$\psi_\chi : \left\{ \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} : c \in \mathbb{F}_p^\times, d \in \mathbb{F}_p \right\} \to (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times, \quad \psi_\chi\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right) = \chi(c).$$

Finally G has a unique irreducible character ϑ of degree > 1. The character table of G summarizes the information:

	$\{\mathrm{Id}\}$	U	$T_c, c \neq 1$
ψ_χ	1	1	$\chi(c)$
ϑ	$p-1$	-1	0

Proof of Proposition 2.4. Take $t = |G|\mathbf{1}_e$, so that $\hat{t}(\chi) = \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$. Then for any $a \in G$, we have

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(a)|\hat{t}(\chi)^2| = \sum_{\chi \bmod p} \chi(a_{1,1}) + (p-1)^2 \vartheta(a).$$

(Here $a_{1,1}$ denotes the coefficients in position (1, 1) of the matrix $a \in G$.) This sum vanishes at $a \in T_c$ for any c. The value of the sum at $a \in U$ is $-p(p-1)$ and finally, at $a = 1$, the sum is $(p-1) + (p-1)^3$. Therefore

$$S_t = \frac{1}{p(1 - 2/p + 2/p^2)}.$$

Take $t = \vartheta$ which is real-valued with $\hat{t}$ nonnegative. Then

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(a)|\widehat{\vartheta}(\chi)|^2 = \vartheta(a) \quad (a \in G).$$

Therefore $S_\vartheta = 1/(p-1)$. □

Proof of Proposition 2.5. One has

$$\lambda_{1,1}(|G|\mathbf{1}_e) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = p(p-1), \quad \lambda_{1,1}(\vartheta) = \vartheta(1) = p-1.$$

Moreover in the course of the proof of Proposition 2.4, we have shown that

$$\lambda_{1,2}(|G|\mathbf{1}_e) = (p-1)(1 + (p-1)^2), \quad \lambda_{1,2}(\vartheta) = p-1.$$

Finally one computes

$$\lambda_{1,4}(|G|\mathbf{1}_e) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^5 = (p-1)(1 + (p-1)^4), \quad \lambda_{1,4}(\vartheta) = \vartheta(1) = p-1.$$

Let t be either $|G|\mathbf{1}_e$ or ϑ. We apply Theorem 1.4 for $K = F = \mathbb{Q}$, and $L = K_{a,p}$. Therefore $G^+ = G$ and $t^+ = t$. Moreover AC holds for $K_{a,p}$ since it is a supersolvable extension of $\mathbb{Q}$. Finally one has $d_L = |\mathrm{disc}(K_{a,p}/\mathbb{Q})| = p^{p^2-2}a^{(p-1)^2}$; see [Komatsu 1976, end of the proof of the Theorem] and [Westlund 1910, Section 3.I]. Therefore

$$\log d_L = p^2 \log p(1 + o_{p\to\infty}(1)), \quad \log \mathrm{rd}_L = (1 + o_{p\to\infty}(1)) \log p.$$

For every $\eta \in \mathcal{S}_\delta$, the last bound of Theorem 1.4 gives

$$w_4(K_{a,p}/\mathbb{Q}, t; \eta) \ll \frac{1}{p \log \mathrm{rd}_L} = \frac{1}{p \log p}(1 + o_{p\to\infty}(1)).$$

As for the variance, Theorem 1.4 gives

$$\left| \frac{\nu(K_{a,p}/\mathbb{Q}, t; \eta)}{\alpha(|\hat{\eta}|^2)\lambda_{1,2}(t) \log \mathrm{rd}_L} - 1 \right| \le S_t + O\left(\frac{1}{\log_2(p+2)}\right).$$

Next we use the value of S_t computed in Proposition 2.4: $S_t = o_{p\to\infty}(1)$. Plugging these bounds into (9), we conclude the proof. □

6.4. *Real parts of characters as class functions.* In this section we prove Proposition 2.6. We will need the following group theoretic preparatory result.

Lemma 6.1. *Let G be a finite group and let $\rho\colon G \to \mathrm{GL}(V)$ be an irreducible finite dimensional complex representation of G. Let χ be the character of ρ and let $a \in G$. We denote by $[a]$ the class of a in $G/\ker\rho$. Then we have the following equivalences*:

(1) $|\chi(a)| = \chi(1)$ *if and only if* $[a]$ *lies in the center* $Z(G/\ker\rho)$ *of* $G/\ker\rho$.

(2) $|\chi(a) + \overline{\chi(a)}| = 2\chi(1)$ *if and only if* $[a]$ *is an element of order* 1 *or* 2 *in* $Z(G/\ker\rho)$.

Proof. (1) First assume $|\chi(a)| = \chi(1)$. Since $\chi(a)$ is a sum of $\chi(1)$ roots of unity and by the triangle inequality, we obtain that $\rho(a)$ has a unique root of unity as eigenvalue. Being diagonalizable (since the separable polynomial $X^{|G|} - 1$ vanishes at $\rho(a)$) we deduce that $\rho(a)$ is a scalar matrix, thus commutes with every element of $\mathrm{End}(V)$. Since ρ induces a faithful representation of $G/\ker\rho$ with representation space V, we conclude that the class of a in $G/\ker\rho$ lies in its center. Conversely, assume $[a]$ commutes with every element of $G/\ker\rho$. Then $\rho(a)$ commutes with every element of $\mathrm{End}(V)$. Since ρ is irreducible, Schur's lemma implies that $\rho(a)$ is a scalar matrix and thus $|\chi(a)| = \chi(1)$.

(2) Since $|\chi(a)| \le \chi(1)$, the equality $|\chi(a) + \overline{\chi(a)}| = 2\chi(1)$ is equivalent to $\chi(a) = \pm\chi(1)$. By (1), this condition on a implies that $[a]$ lies in the center of $G/\ker\rho$ with $\rho(a)$ a scalar matrix of trace $\pm\chi(1)$. In other words $\rho(a) = \pm\,\mathrm{Id}$, i.e., $\rho(a^2) = \mathrm{Id}$. Since ρ induces a faithful representation of $G/\ker\rho$ this is in turn equivalent to $[a]$ having order at most 2 in $Z(G^+/\ker\rho)$. The converse holds since if $[a]$ is an element of order at most 2 in $Z(G/\ker\rho)$, then $\rho(a) = \pm\,\mathrm{Id}$ and therefore $\chi(a) = \pm\chi(1)$. □

Proof of Proposition 2.6. Since $t^+ = (\chi + \overline{\chi}/2)$, then $\widehat{t^+}(\psi) = \frac{1}{2}$ if $\psi \in \{\chi, \overline{\chi}\}$, and $\widehat{t^+}(\psi) = 0$ for every other irreducible character of G^+. We deduce that $S_{t^+} = \max_{a\neq 1}|\chi(a) + \overline{\chi}(a)|/(2\chi(1))$. By

Lemma 6.1(2), we deduce that $S_{t^+} = 1$ if and only if $Z(G/\ker\rho)$ has an element of order 1 or 2. This is in turn equivalent to $\ker\rho = \{e\}$ and $|Z(G^+)|$ odd. □

We see that the particular case where $\mathbb{Q} = F = K$ and $G^+ = \mathrm{Gal}(L/\mathbb{Q})$ admits a faithful irreducible character χ and where $Z(G^+)$ has odd order is precisely that of Section 2.3.

6.5. *S_n-extensions.* In the section, we prove Proposition 2.7.

Proof of Proposition 2.7. We begin by noting that following [Fiorilli and Jouve 2024, Proof of Lemma 7.4], one can show that Roichman's bound [1996] combined with the hook-length formula imply that for any $\chi \in \mathrm{Irr}(S_n)$,

$$\max_{\mathrm{id}\neq\pi\in S_n} \frac{\chi(\pi)}{\chi(1)} \le \left(\max\left(q, \frac{\log(kn!/\chi(1)) + 2n/\mathrm{e}}{\log n!}\right)\right)^b, \tag{50}$$

where $0 < q < 1$, $k \ge 1$ and $b > 0$ are absolute constants. For simplicity, let us denote $t = t_{C_1,C_2}$. We will apply the bound (50) on characters for which $\chi(1) \ge \|t\|_2(4p(n)^{1/2}\|t\|_1)^{-1}$. Note that

$$\|t\|_2^2 = \frac{n!}{|C_1|} + \frac{n!}{|C_2|}, \quad \|t\|_1 = 2.$$

We may now apply Theorem 1.4, in the generalized form given in Remark 1.7. Setting

$$\Xi_{n;C_1,C_2} := \{\chi \in \mathrm{Irr}(S_n) : \chi(1) \ge \|t\|_2(8p(n)^{1/2})^{-1}\},$$

it follows that for all large enough n,

$$\begin{aligned} S_t(\Xi_{n;C_1,C_2}) &\le \left(\max\left(q, \frac{\log(kn!^{1/2}\min(|C_1|,|C_2|)^{1/2}) + 2n/\mathrm{e}}{\log n!}\right)\right)^b \\ &\le \max\left(\theta_1, \left(1 - \frac{\log(n!/\min(|C_1|,|C_2|))}{2\log n!} + \frac{2 + o_{n\to\infty}(1)}{\mathrm{e}\log n}\right)^b\right) \\ &\le 1 - \theta_2 \frac{\log(n!/\min(|C_1|,|C_2|))}{2\log n!}, \end{aligned}$$

where $0 < \theta_1 < 1$ and $\theta_2 > 0$ are absolute. We now claim that $\lambda_{1,2}(t, \Xi) \gg \lambda_{1,2}(t)$. To see this, we argue as in [Fiorilli and Jouve 2024, Proposition 4.7]. We have the bound

$$\lambda_{1,2}(t, \mathrm{Irr}(G)\setminus\Xi) \le \frac{\|t\|_2}{8p(n)^{1/2}}\lambda_{0,2}(t) = \frac{\|t\|_2^3}{8p(n)^{1/2}},$$

by Parseval's identity in the form $\lambda_{0,2}(t) = \|t\|_2^2$. Moreover, [Fiorilli and Jouve 2024, (111)] implies that

$$\lambda_{1,2}(t) \ge \frac{\|t\|_2^3}{2\sqrt{2}p(n)^{1/2}\|t\|_1},$$

and as a result we deduce that

$$\lambda_{1,2}(t;\, \Xi_{n;C_1,C_2}) \gg \frac{\|t\|_2^3}{p(n)^{1/2}}.$$

We can now apply Theorem 1.1 to deduce the claimed bound. For the case $t = t_{C_1}$, the proof is identical. □

Acknowledgements

The work of Jouve was partly funded by the ANR through project FLAIR (ANR-17-CE40-0012). The authors would like to thank *Villa La Stella* in Florence for their hospitality and excellent working conditions during a stay in March 2022 where substantial parts of this work were accomplished. Finally we would like to thank the referee for the careful reading of our manuscript and for providing numerous helpful suggestions.

References

[Artin 1931] E. Artin, "Zur Theorie der L-reihen mit allgemeinen Gruppencharakteren", *Abh. Math. Sem. Univ. Hamburg* **8**:1 (1931), 292–306. MR Zbl

[Bellaïche 2016] J. Bellaïche, "Théorème de Chebotarev et complexité de Littlewood", *Ann. Sci. École Norm. Sup.* (4) **49**:3 (2016), 579–632. MR Zbl

[de la Bretèche and Fiorilli 2021] R. de la Bretèche and D. Fiorilli, "On a conjecture of Montgomery and Soundararajan", *Math. Ann.* **381**:1-2 (2021), 575–591. MR Zbl

[de la Bretèche and Fiorilli 2023] R. de la Bretèche and D. Fiorilli, "Moments of moments of primes in arithmetic progressions", *Proc. Lond. Math. Soc.* (3) **127**:1 (2023), 165–220. MR Zbl

[de la Bretèche et al. 2023] R. de la Bretèche, D. Fiorilli, and F. Jouve, "Moments in the Chebotarev density theorem: non-Gaussian families", preprint, 2023. arXiv 2301.12826

[Carneiro et al. 2015] E. Carneiro, V. Chandee, and M. B. Milinovich, "A note on the zeros of zeta and L-functions", *Math. Z.* **281**:1-2 (2015), 315–332. MR Zbl

[Cohen et al. 1998] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Computing ray class groups, conductors and discriminants", *Math. Comp.* **67**:222 (1998), 773–795. MR Zbl

[Fiorilli and Jouve 2024] D. Fiorilli and F. Jouve, "Distribution of Frobenius elements in families of Galois extensions", *J. Inst. Math. Jussieu* **23**:3 (2024), 1169–1258. MR Zbl

[Fiorilli and Martin 2013] D. Fiorilli and G. Martin, "Inequities in the Shanks–Rényi prime number race: an asymptotic formula for the densities", *J. Reine Angew. Math.* **676** (2013), 121–212. MR Zbl

[Hooley 1977] C. Hooley, "On the Barban–Davenport–Halberstam theorem, VII", *J. Lond. Math. Soc.* (2) **16**:1 (1977), 1–8. MR Zbl

[Huppert 1998] B. Huppert, *Character theory of finite groups*, de Gruyter Expo. Math. **25**, de Gruyter, Berlin, 1998. MR Zbl

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ. **53**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[Kolmogorov and Fomin 1989] A. N. Kolmogorov and S. V. Fomin, Елементы теории функции и функционалного анализа, 6th ed., "Nauka", Moscow, 1989. MR Zbl

[Komatsu 1976] K. Komatsu, "An integral basis of the algebraic number field $Q(\sqrt{t}a, \sqrt{t}1)$", *J. Reine Angew. Math.* **288** (1976), 152–153. MR Zbl

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Martinet 1977] J. Martinet, "Character theory and Artin L-functions", pp. 1–87 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Stud. Adv. Math. **97**, Cambridge Univ. Press, 2007. MR Zbl

[Pizarro-Madariaga 2011] A. Pizarro-Madariaga, "Lower bounds for the Artin conductor", *Math. Comp.* **80**:273 (2011), 539–561. MR Zbl

[Roichman 1996] Y. Roichman, “Upper bound on the characters of the symmetric groups”, *Invent. Math.* **125**:3 (1996), 451–485. MR Zbl

[Rubinstein and Sarnak 1994] M. Rubinstein and P. Sarnak, “Chebyshev’s bias”, *Exp. Math.* **3**:3 (1994), 173–197. MR Zbl

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Grad. Texts in Math. **42**, Springer, 1977. MR Zbl

[Viviani 2004] F. Viviani, “Ramification groups and Artin conductors of radical extensions of $\mathbb{Q}$”, *J. Théor. Nombres Bordeaux* **16**:3 (2004), 779–816. MR Zbl

[Westlund 1910] J. Westlund, “On the fundamental number of the algebraic number-field $k(\sqrt[p]{m})$”, *Trans. Amer. Math. Soc.* **11**:4 (1910), 388–392. MR Zbl

[Wintner 1941] A. Wintner, “On the distribution function of the remainder term of the prime number theorem”, *Amer. J. Math.* **63** (1941), 233–248. MR Zbl

Communicated by Philippe Michel
Received 2023-02-06 Revised 2023-12-19 Accepted 2024-05-23

regis.de-la-breteche@imj-prg.fr *Institut de Mathématiques de Jussieu-Paris Rive Gauche, Université Paris Cité, Sorbonne Université, CNRS UMR 7586, Paris, France*

daniel.fiorilli@universite-paris-saclay.fr *Institut de mathématiques d’Orsay, Université Paris Saclay, Orsay, France*

florent.jouve@math.u-bordeaux.fr *Université de Bordeaux, CNRS UMR 5251, Bordeaux INP, Talence, France*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 19 No. 3 2025

The Lyndon–Demushkin method and crystalline lifts of G_2-valued Galois representations 415
ZHONGYIPAN LIN

Fermat's last theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 457
MALEEHA KHAWAJA and FRAZER JARVIS

Moments in the Chebotarev density theorem: general class functions 481
RÉGIS DE LA BRETÈCHE, DANIEL FIORILLI and FLORENT JOUVE

Abelian varieties over finite fields and their groups of rational points 521
STEFANO MARSEGLIA and CALEB SPRINGER

Algebraic cycles and functorial lifts from G_2 to PGSp_6 551
ANTONIO CAUCHI, FRANCESCO LEMMA and JOAQUÍN RODRIGUES JACINTO