SELF-DUAL ARTIN REPRESENTATIONS

DAVID E. ROHRLICH

Functional equations in number theory are relations between an L-function and some sort of dual L-function, and in general, the L-function and its dual need not coincide. For example, if χ is a primitive Dirichlet character then the functional equation relates $L(s,\chi)$ to $L(1-s,\overline{\chi})$, and $L(s,\overline{\chi}) = L(s,\chi)$ if and only if $\chi^2 = 1$. Or if f is a primitive cusp form of weight two for $\Gamma_1(N)$ and $f^\vee$ is the complex-conjugate form then the functional equation relates $L(s,f)$ to $L(2-s,f^\vee)$, and $L(s,f^\vee) = L(s,f)$ if and only if f is a cusp form for $\Gamma_0(N)$ with trivial character. Let us call an L-function *self-dual* if its functional equation is a relation between the L-function and itself. While self-dual L-functions are often of special interest, the preceding examples suggest that they may also be rare. Indeed the number of Dirichlet characters modulo N is the quantity

$$\varphi(N) = N\prod_{p|N}(1-p^{-1})$$

and is therefore $\gg N^{1-\varepsilon}$ for every $\varepsilon > 0$, but the number of quadratic Dirichlet characters modulo N is $\ll N^{\varepsilon}$. Similarly, if $N \geqslant 5$ then the dimension of the space $\mathrm{S}_2(\Gamma_1(N))$ of cusp forms of weight two for $\Gamma_1(N)$ is given by

$$\dim \mathrm{S}_2(\Gamma_1(N)) = 1 + \frac{N^2}{24}\prod_{p|N}(1-p^{-2}) - \frac{1}{4}\sum_{N_1N_2=N}\varphi(N_1)\varphi(N_2)$$

and is therefore $\gg N^2$, but the dimension of the space of cusp forms of weight two for $\Gamma_0(N)$ is $\ll N^{1+\varepsilon}$. Is it perhaps the case that self-dual L-functions are of density zero among all L-functions?

It is tidier, although not *a priori* equivalent, to replace the L-functions by the objects underlying them. If the L-functions are motivic then the underlying objects are motives, and one can ask whether "essentially self-dual motives" (in other words, pure motives which are self-dual up to Tate twist) have density zero among all pure motives of a given rank and weight. However if we insist on full generality then the preceding question is not yet amenable to a precise formulation, because the set of isomorpism classes of pure motives of a given rank and weight over a given number field with conductor below a given bound is not known to be finite. So instead we shall focus on motives of weight zero. By an *Artin representation* of a number field F we mean as usual a continuous representation ρ of $\mathrm{Gal}(\overline{F}/F)$ on a finite-dimensional complex vector space. Such a representation always factors through the quotient of $\mathrm{Gal}(\overline{F}/F)$ by an open normal subgroup and so will be regarded as a representation of $\mathrm{Gal}(L/F)$ for some finite Galois extension L of F. The conductor of ρ is an integral ideal $\mathfrak{q}(\rho)$ of F, the absolute norm of which will be denoted $q(\rho)$. According to a theorem of Ralph Greenberg (unpublished) and of Anderson, Blasius, Coleman, and Zettler [1] (who consider more generally the case of representations of the global Weil group of F), if we fix F and n then the set of isomorphism classes of n-dimensional Artin representations ρ of F with $q(\rho) \leqslant x$ is finite. Write $\vartheta_{F,n}(x)$ for the number of such isomorphism classes and $\vartheta^{\mathrm{sd}}_{F,n}(x)$ for the number of classes such that ρ is self-dual. Dropping the subscripts F and n for simplicity, we ask whether $\lim_{x\to\infty} \vartheta^{\mathrm{sd}}(x)/\vartheta(x) = 0$.

If $F = \mathbb{Q}$ and $n = 1$ then an affirmative answer is implicit already in our remarks about Dirichlet characters, and it is easy to see that in fact $\vartheta^{\mathrm{sd}}(x)/\vartheta(x) \sim \pi^2/(3x)$ in this case. Using the work of Bhargava [3], [4] and of Bhargava, Cojocaru, and Thorne [5], we shall prove that the answer is also affirmative for $F = \mathbb{Q}$ and $n = 2$. For $F = \mathbb{Q}$ and $n = 3$ we show at least that an affirmative answer would follow from a conjecture of Malle [26] on the distribution of Galois groups, but for $n \geqslant 4$ we are unable to derive an affirmative answer even conditionally, and if F is an arbitrary number field then already the case $n = 1$ is mysterious, a point to which we return.

Before describing the contents of the paper in more detail we introduce some refinements of $\vartheta_{F,n}(x)$. Recall that a finite-dimensional complex representation of a finite group G is *abelian* if it is a direct sum of one-dimensional characters of G, *reducible* if it is a direct sum of two proper subrepresentations, *irreducible* if it is of positive dimension but not reducible, *monomial* if it is induced by a one-dimensional character of a subgroup of G, and *primitive* if it is not induced from any proper subgroup of G. We use the superscripts "ab," "irr," "im," and "ip" to refer to abelian, irreducible, irreducible monomial, and irreducible primitive representations respectively. For example, $\vartheta^{\mathrm{ab}}_{F,n}(x)$ is the number of isomorphism classes of n-dimensional abelian Artin representations ρ of F with $q(\rho) \leqslant x$, and $\vartheta^{\mathrm{ab,sd}}_{F,n}(x)$ is the number of such isomorphism classes that are self-dual. The notation is illustrated by the self-evident assertions

$$\vartheta^{\mathrm{sd}}_{\mathbb{Q},2}(x) = \vartheta^{\mathrm{ab,sd}}_{\mathbb{Q},2} + \vartheta^{\mathrm{im,sd}}_{\mathbb{Q},2}(x) + \vartheta^{\mathrm{ip,sd}}_{\mathbb{Q},2}(x) \tag{1}$$

and

$$\vartheta^{\mathrm{sd}}_{\mathbb{Q},3}(x) = \vartheta^{\mathrm{ab,sd}}_{\mathbb{Q},3} + \vartheta^{1+2,\mathrm{sd}}_{\mathbb{Q},3}(x) + \vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},3}(x), \tag{2}$$

where $\vartheta^{1+2,\mathrm{sd}}_{\mathbb{Q},3}(x)$ is the number of isomorphism classes of self-dual Artin representations of $\mathbb{Q}$ of the form $\rho \cong \rho' \oplus \rho''$ with ρ' one-dimensional, ρ'' irreducible and two-dimensional, and $q(\rho')q(\rho'') \leqslant x$. Of course (1) and (2) remain valid without the superscript "sd" and with $\mathbb{Q}$ replaced by any number field F.

In addition to $\vartheta_{F,n}(x)$ and its refinements, we need two functions which count discriminants rather than conductors. Given a finite extension K of F, write $\mathfrak{d}_{K/F}$ for the relative discriminant ideal of K over F and $d_{K/F}$ for the absolute norm of $\mathfrak{d}_{K/F}$. If $F = \mathbb{Q}$ then we write simply $\mathfrak{d}_K$ and d_K. Now fix an integer $m \geqslant 2$. We write $\eta_{F,m}(x)$ for the number of extensions K of F inside our fixed algebraic closure $\overline{F}$ such that $[K : F] = m$ and $d_{K/F} \leqslant x$. Also, if G is a transitive subgroup of the symmetric group S_m, then $\eta^G_{F,m}(x)$ denotes the number of such extensions K for which $\mathrm{Gal}(L/F) \cong G$ as permutation groups, where L is a normal closure of K over F and $\mathrm{Gal}(L/F)$ is viewed as a permutation group via its action on the set of conjugates $\alpha_1, \alpha_2, \ldots, \alpha_m$ of a primitive element of K over F. The requirement that $\mathrm{Gal}(L/F)$ and G be isomorphic as permutation groups means of course that there is a bijection of $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ onto $\{1, 2, \ldots, m\}$ such that the resulting map $\mathrm{Gal}(L/F) \hookrightarrow S_m$ has image G.

With these notations in hand let us now describe the contents of the paper section by section. We have included a considerable amount of expository material throughout, because our aim is in part pedagogical.

The first four sections are devoted to the abelian case. The tauberian method, recalled in Section 1, leads to asymptotic formulas for $\vartheta_{\mathbb{Q},1}(x)$ and $\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(x)$ in Section 2 and for $\vartheta^{\mathrm{ab}}_{\mathbb{Q},n}(x)$ and $\vartheta^{\mathrm{ab,sd}}_{\mathbb{Q},n}(x)$ in Section 3. Our dicussion of the abelian case is completed in Section 4, where we attempt to replace $\mathbb{Q}$ by an arbitrary number field F. If F is neither $\mathbb{Q}$ nor an imaginary quadratic field then the asymptotic behavior of $\vartheta_{F,1}(x)$ appears to be unknown, and we argue that what is needed is a horizontal analogue of Leopoldt's conjecture.

In the next two sections we bound $\vartheta^{\mathrm{im,sd}}_{\mathbb{Q},2}(x)$. Whether monomial or not, an irreducible self-dual Artin representation is either *orthogonal* or *symplectic* – in other words, relative to an appropriate choice of basis, its image is contained in either the real orthogonal group $\mathrm{O}_n(\mathbb{R})$ or the complex symplectic group $\mathrm{Sp}_{2n}(\mathbb{C})$ – and hence in particular $\vartheta^{\mathrm{im,sd}}_{\mathbb{Q},2}(x)$ is the sum of an orthogonal term and a symplectic term. These terms are bounded in Sections 5 and 6 respectively. The orthogonal term is bounded by a reduction to the asymptotic formulas of Siegel [35], and then the symplectic term is bounded by a reduction to the orthogonal term.

Our treatment of the primitive case begins in Section 7 with some background on Schur covers. In Section 8 we bound $\vartheta^{\mathrm{ip,sd}}_{\mathbb{Q},2}(x)$ in terms of $\eta_{\mathbb{Q},4}(x)$ and $\eta^{A_5}_{\mathbb{Q},5}(x)$, to which we then apply the results of Bhargava [3] and Bhargava, Cojocaru, and Thorne [5] (the latter work being itself an application of Bhargava's asymptotics for quintic fields [4]). In principle we could have adopted a different strategy, in the spirit of Serre's paper [31]: bound the dimension of spaces of holomorphic cusp forms of weight one and spaces of Maass forms of eigenvalue 1/4, and then appeal to the Langlands correspondence to deduce a bound for $\vartheta^{\mathrm{ip,sd}}_{\mathbb{Q},2}(x)$. In fact the relevant bounds on spaces of automorphic forms can simply be quoted from the work of Michel and Venkatesh [28], who vastly generalize the original breakthrough (in the case of holomorphic cusp forms of weight one, prime level, and character the Legendre symbol) of Duke [11]. However, in spite of the enormous progress of recent years, the Langlands correspondence for two-dimensional Artin representations of $\mathbb{Q}$ of icosahedral type and *even* determinant remains conjectural, and for the sake of an unconditional result and a uniform treatment our argument will be carried out on the Galois side of the correspondence.

By the end of Section 8 we will have assembled upper bounds for each of the terms on the right-hand side of (1). The upshot will be that

$$\vartheta^{\mathrm{sd}}_{\mathbb{Q},2}(x) = O(x^{2-\gamma}) \tag{3}$$

for every $\gamma < 1/60$. On the other hand, from our asymptotic formula for $\vartheta^{\mathrm{ab}}_{\mathbb{Q},n}(x)$ we will also have

$$\vartheta^{\mathrm{ab}}_{\mathbb{Q},2}(x) \gg x^2 \log x. \tag{4}$$

Since $\vartheta_{\mathbb{Q},2}(x) \geqslant \vartheta^{\mathrm{ab}}_{\mathbb{Q},2}(x)$, it follows from (3) and (4) that $\lim_{x\to\infty} \vartheta^{\mathrm{sd}}(x)/\vartheta(x)$ is indeed 0 for $F = \mathbb{Q}$ and $n = 2$.

Perhaps it is disappointing to arrive at this conclusion by comparing the totality of self-dual representations with the abelian representations only. Thus in Section 9 we go on to show that $\lim_{x\to\infty} \vartheta^{\mathrm{irr,sd}}(x)/\vartheta^{\mathrm{irr}}(x) = 0$ for $F = \mathbb{Q}$ and $n = 2$. But even the latter assertion rests on the trivial inequalities $\vartheta^{\mathrm{irr,sd}}(x) \leqslant \vartheta^{\mathrm{sd}}(x)$ and

$\vartheta^{\mathrm{irr}}(x) \geqslant \vartheta^{\mathrm{im}}(x)$. Unfortunately, a direct comparison between, say, $\vartheta^{\mathrm{ip,sd}}(x)$ and $\vartheta^{\mathrm{ip}}(x)$ seems to be out of our reach.

Apart from two appendices, the remainder of the paper is devoted to Malle's conjecture and two of its consequences. One consequence, derived in Sections 10 and 11, is an upper bound for $\vartheta^{\mathrm{ip,sd}}(x)$ valid for arbitrary F and $n \geqslant 2$. The other conesquence, a variant of the first, is a bound for the term $\vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},3}(x)$ in (2). Using this bound we prove in Section 12 that under Malle's conjecture we have $\lim_{x\to\infty} \vartheta^{\mathrm{sd}}(x)/\vartheta(x) = 0$ for $F = \mathbb{Q}$ and $n = 3$.

The many questions left open by this paper are so glaringly obvious that it would be superfluous to enumerate them. But it may be worthwhile to point out a parallel line of inquiry in the domain of automorphic forms: Do lifts from orthogonal and symplectic groups have density zero among all cuspidal automorphic representations of $\mathrm{GL}(n)$? The question seems amenable to a precise formulation, and perhaps also to a solution.

I am deeply grateful to Manjul Bhargava for providing me with a preprint of [5] before publication. I would also like to thank Josh Zelinsky for drawing my attention to the paper of Collins [7].

1. A tauberian theorem

The tauberian theorem that will be needed in this paper is a special case of Theorem 7.7 on p. 154 of the book [2] by Bateman and Diamond. Let $\psi(1), \psi(2), \psi(3), \ldots$ be a sequence of nonnegative real numbers, and let

$$D(s) = \sum_{q\geqslant 1} \psi(q) q^{-s}$$

be the associated Dirichlet series and

$$\vartheta(x) = \sum_{q\leqslant x} \psi(q)$$

the associated summatory function. We assume that there are positive real numbers a and a' with $a' < a$ together with an integer $b \geqslant 1$ such that the following conditions are satisfied:

(i) The series $\sum_{q\geqslant 1} \psi(q)q^{-s}$ converges for $\Re(s) > a$ and thus defines $D(s)$ as a holomorphic function in this region.
(ii) $D(s)$ extends to a meromorphic function in the region $\Re(s) > a'$.
(iii) $D(s)$ has a pole of order b at $s = a$ and is otherwise holomorphic for $\Re(s) > a'$.

Let κ be the residue of $(s-a)^{b-1}D(s)$ at $s = a$, and put $c = \kappa/(a \cdot (b-1)!)$. It follows from the hypotheses that $\kappa > 0$ and hence that $c > 0$.

Proposition 1. $\vartheta(x) \sim cx^a(\log x)^{b-1}$.

To deduce Proposition 1 from Theorem 7.7 of [2], note the definition of $\widehat{F}$ given on p. 109 of [2], the special case of the definition embodied in the displayed equation at the top of p. 110, and the definition of $\sigma_c(\widehat{F})$ on p. 119, and keep in mind that our a, a', and b correspond to the constants α, β, and γ of [2].

2. Dirichlet characters

Given a positive integer q, write $\psi(q)$ for the number of primitive Dirichlet characters of conductor q. We consider the Dirichlet series

$$D(s) = \sum_{q \geqslant 1} \psi(q) q^{-s},$$

convergent for $\Re(s) > 2$.

Proposition 2. $D(s) = \zeta(s-1)/\zeta(s)^2$.

Proof. Assertions of this sort are antique (cf. [14], p. 268, Theorem 330), but we include a proof nonetheless. Let μ and φ denote as usual the Möbius and Euler functions, and put $C(s) = \sum_{q \geqslant 1} \varphi(q) q^{-s}$. Since $\psi(q) = \sum_{q' | q} \mu(q/q')\varphi(q')$ we have

$$D(s) = C(s)/\zeta(s). \tag{5}$$

Now φ is multiplicative, so

$$C(s) = \prod_p \Big(\sum_{\nu \geqslant 0} \varphi(p^\nu) p^{-\nu s}\Big).$$

Write $C_p(s)$ for the Euler factor on the right-hand side. Since $\varphi(1) = 1$ and $\varphi(p^\nu) = (p-1)p^{\nu-1}$ for $\nu \geqslant 1$, we have

$$C_p(s) = 1 + \sum_{\nu \geqslant 1} (p-1)p^{-1} p^{\nu(1-s)} = 1 + (p-1)p^{-s}/(1-p^{1-s})$$

and consequently

$$C_p(s) = 1 + \frac{p^{1-s} - p^{-s}}{1 - p^{1-s}} = \frac{1 - p^{-s}}{1 - p^{1-s}}.$$

Hence $C(s) = \zeta(s-1)/\zeta(s)$. The proposition now follows from (5). □

Identifying one-dimensional characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with primitive Dirichlet characters in the usual way, we see that

$$\vartheta_{\mathbb{Q},1}(x) = \sum_{q \leqslant x} \psi(q).$$

In other words $\vartheta_{\mathbb{Q},1}(x)$ is the summatory function corresponding to $D(s)$. On the other hand, it follows from Proposition 2 that $D(s)$ is holomorpic for $\Re(s) > 1$ apart from a simple pole at $s = 2$ with residue $36/\pi^4$. Hence Proposition 1 gives:

Corollary. $\vartheta_{\mathbb{Q},1}(x) \sim 18x^2/\pi^4$.

Next consider the Dirichlet series

$$D^{\mathrm{sd}}(s) = \sum_{q \geqslant 1} \psi^{\mathrm{sd}}(q) q^{-s},$$

where $\psi^{\mathrm{sd}}(q)$ is the number of primitive Dirichlet characters χ of conductor q such that $\chi^2 = 1$.

Proposition 3. $D^{\mathrm{sd}}(s) = (1 + 4^{-s} + 2 \cdot 8^{-s}) \dfrac{\zeta(s)(1-2^{-s})}{\zeta(2s)(1-2^{-2s})}$.

Proof. The conductor of a primitive quadratic Dirichlet character can be written $2^\nu r$, where $\nu = 0$, 2, or 3 and r is a square-free odd positive integer. Conversely, every number of this form is the conductor of exactly one (if $\nu = 0$ or 2) or exactly two (if $\nu = 3$) primitive Dirichlet characters χ with $\chi^2 = 1$. It follows that

$$D^{\mathrm{sd}}(s) = (1 + 4^{-s} + 2 \cdot 8^{-s})R(s), \tag{6}$$

where $R(s)$ is the Dirichlet series $\sum r^{-s}$, the sum being taken over square-free odd positive integers r. Now if the sum were taken over all square-free positive integers then the resulting Dirichlet series would be $\zeta(s)/\zeta(2s)$, so to deduce a formula for $R(s)$ we remove the Euler factor at 2 in $\zeta(s)/\zeta(2s)$. Substitution in (6) yields the stated formula. □

Another appeal to Proposition 1 gives:

Corollary. $\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(x) \sim 6x/\pi^2$.

Comparing this corollary with the previous one, we see that

$$\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(x)/\vartheta_{\mathbb{Q},1}(x) \sim \pi^2/(3x), \tag{7}$$

as mentioned in the introduction.

3. Abelian representations

Given positive integers n and q, let $\psi_n(q)$ be the number of isomorphism classes of n-dimensional abelian Artin representations of $\mathbb{Q}$ of conductor q. We put

$$D_n(s) = \sum_{q \geqslant 1} \psi_n(q) q^{-s}.$$

In the notation of Section 2 we have $\psi_1(q) = \psi(q)$ and hence $D_1(s) = D(s)$.

Proposition 4. *For $n \geqslant 1$,*

$$D_n(s) = \sum_{k=1}^{n} \frac{1}{k!} \sum_{\nu_1+\nu_2+\cdots+\nu_k=n} \frac{D(\nu_1 s)D(\nu_2 s)\cdots D(\nu_k s)}{\nu_1\nu_2\cdots\nu_k},$$

where the inner sum on the right runs over k-tuples $(\nu_1, \nu_2, \cdots, \nu_k)$ of positive integers summing to n.

Proof. Given a one-dimensional character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let us write $\chi^{\oplus\nu}$ for the direct sum of ν copies of χ. If

$$\rho \cong \chi_1^{\oplus n_1} \oplus \chi_2^{\oplus n_2} \oplus \cdots \oplus \chi_k^{\oplus n_k}$$

with one-dimensional characters $\chi_1, \chi_2, \ldots, \chi_k$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and positive integers $n_1, n_2, \ldots, n_k$ then

$$q(\rho) = q(\chi_1)^{n_1} q(\chi_2)^{n_2} \cdots q(\chi_k)^{n_k}.$$

Thus we have the following identity of formal power series in x with coefficients in the ring of formal Dirichlet series:

$$\sum_\rho q(\rho)^{-s} x^{\dim(\rho)} = \prod_\chi (1 - q(\chi)^{-s}x)^{-1},$$

where ρ runs over a set of representatives for the distinct isomorphism classes of abelian Artin representations of $\mathbb{Q}$ and χ runs over one-dimensional characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Equivalently,

$$1 + \sum_{n\geqslant 1}\sum_{q\geqslant 1}\psi_n(q)q^{-s}x^n = \prod_{q\geqslant 1}(1-q^{-s}x)^{-\psi(q)}.$$

Summing over q on the left-hand side while expressing the right-hand side as the exponential of its logarithm, we obtain

$$1 + \sum_{n\geqslant 1} D_n(s)x^n = \exp\left(\sum_{\nu\geqslant 1} D(\nu s)\frac{x^\nu}{\nu}\right).$$

The proposition follows on comparing the coefficient of x^n on both sides. $\square$

Proposition 5. *$D_n(s)$ is holomorphic for $\Re(s) > 1$ except for a pole of order n at $s = 2$. Furthermore, the residue of $(s-2)^{n-1}D_n(s)$ at $s = 2$ is $(1/n!)(36/\pi^4)^n$.*

Proof. Rewrite Proposition 4 in the form

$$D_n(s) = \frac{D(s)^n}{n!} + \sum_{k=1}^{n-1}\frac{1}{k!}\sum_{\nu_1+\nu_2+\cdots+\nu_k=n}\frac{D(\nu_1 s)D(\nu_2 s)\cdots D(\nu_k s)}{\nu_1\nu_2\cdots\nu_k}. \tag{8}$$

From Proposition 2 we know that $D(s)$ is holomorphic for $\Re(s) > 1$ except for a simple pole at $s = 2$ with residue $36/\pi^4$. Thus $D(s)^n/n!$ has the properties claimed for $D_n(s)$. To deduce that $D_n(s)$ itself has these properties it suffices to observe that for $k \leqslant n-1$ the term $D(\nu_1 s)D(\nu_2 s)\cdots D(\nu_k s)/(\nu_1\nu_2\cdots\nu_k)$ on the right-hand side of (8) has at most $n-2$ factors $D(\nu_i s)$ with $\nu_i = 1$. Hence the pole (if any) of such a term at $s = 2$ is of order at most $n-2$. $\square$

As $\vartheta^{\mathrm{ab}}_{\mathbb{Q},n}(x)$ is the summatory function of $D_n(s)$, Proposition 1 gives:

Theorem 1. $\vartheta^{\mathrm{ab}}_{\mathbb{Q},n}(x) \sim (1/2)(1/n!)(36/\pi^4)^n \cdot x^2(\log x)^{n-1}$.

A similar argument can be applied in the self-dual case. Write $\psi^{\mathrm{sd}}_n(q)$ for the number of isomorphism classes of n-dimensional self-dual abelian Artin representations of $\mathbb{Q}$ of conductor q, and put

$$D^{\mathrm{sd}}_n(s) = \sum_{q\geqslant 1}\psi^{\mathrm{sd}}_n(q)q^{-s}.$$

Then $\psi^{\mathrm{sd}}_1 = \psi^{\mathrm{sd}}$ and $D^{\mathrm{sd}}_1 = D^{\mathrm{sd}}$ in the notation of Section 2. Given a positive integer ν, it is also convenient to set

$$D[\nu](s) = \begin{cases} D^{\mathrm{sd}}(\nu s) & \text{if } \nu \text{ is odd}\\ D(\nu s) & \text{if } \nu \text{ is even.}\end{cases}$$

Note in particular that $D[1] = D^{\mathrm{sd}}$.

Proposition 6. *For $n \geqslant 1$,*

$$D^{\mathrm{sd}}_n(s) = \sum_{k=1}^{n}\frac{1}{k!}\sum_{\nu_1+\nu_2+\cdots+\nu_k=n}\frac{D[\nu_1](s)D[\nu_2](s)\cdots D[\nu_k](s)}{\nu_1\nu_2\cdots\nu_k},$$

where the inner sum on the right runs over k-tuples $(\nu_1,\nu_2,\cdots,\nu_k)$ of positive integers summing to n.

Proof. An abelian Artin representation ρ of $\mathbb{Q}$ is self-dual if and only if it has the form

$$\rho \cong \Big(\bigoplus\nolimits_{\chi^2=1} \ \chi^{\oplus\nu(\chi)}\Big) \oplus \Big({\bigoplus}'_{\chi^2\neq 1} \ (\chi\oplus\chi^{-1})^{\oplus\nu(\chi)}\Big),$$

where the direct sum inside the first set of parentheses runs over one-dimensional characters χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of order $\leqslant 2$, the direct sum inside the second set of parentheses runs over *pairs* $\{\chi,\chi^{-1}\}$ of complex conjugate characters (this is the significance of the prime) of order $\geqslant 3$, and $\nu(\chi)=0$ for all but finitely many χ. As $q(\chi\oplus\chi^{-1})=q(\chi)^2$, it follows that

$$\begin{aligned}1+\sum_{n\geqslant 1} D_n^{\mathrm{sd}}(s)x^n &= \prod\nolimits_{\chi^2=1}(1-q(\chi)^{-s}x)^{-1}\cdot{\prod}'_{\chi^2\neq 1}(1-q(\chi)^{-2s}x^2)^{-1}\\ &=\prod_{q\geqslant 1}(1-q^{-s}x)^{-\psi^{\mathrm{sd}}(q)}\cdot\prod_{q\geqslant 1}(1-q^{-2s}x^2)^{-\psi^*(q)}\end{aligned}\tag{9}$$

with $\psi^*(q)=(\psi(q)-\psi^{\mathrm{sd}}(q))/2$. Set $D^*(s)=\sum_{q\geqslant 1}\psi^*(q)q^{-s}$. Then $D^*(s)=(D(s)-D^{\mathrm{sd}}(s))/2$. Writing the two products in the last expression in (9) as the exponentials of their logarithms, we obtain

$$\begin{aligned}1+\sum_{n\geqslant 1} D_n^{\mathrm{sd}}(s)x^n &= \exp\Big(\sum_{\nu\geqslant 1} D^{\mathrm{sd}}(\nu s)x^\nu/\nu\Big)\cdot\exp\Big(\sum_{\mu\geqslant 1} D^*(2\mu s)x^{2\mu}/\mu\Big)\\ &=\exp\Big(\sum_{\nu\geqslant 1} D[\nu](s)x^\nu/\nu\Big).\end{aligned}$$

The proposition follows on inspecting the coefficient of x^n in this last expression. □

Proposition 7. *$D_n^{\mathrm{sd}}(s)$ is holomorphic for $\Re(s)>1/2$ except for a pole of order n at $s=1$. Furthermore, the residue of $(s-1)^{n-1}D_n^{\mathrm{sd}}(s)$ at $s=1$ is $(1/n!)(6/\pi^2)^n$.*

Proof. We observe first of all that if ν is a positive integer then $D[\nu](s)$ is holomorphic for $\Re(s)>1/2$ except possibly for a simple pole at $s=1$. Indeed if ν is odd then $D[\nu](s)=D^{\mathrm{sd}}(\nu s)$ and our assertion follows from Proposition 3, while if ν is even then $D[\nu](s)=D(\nu s)$ with $\nu\geqslant 2$ and $D(s)=\zeta(s-1)/\zeta(s)^2$ (Proposition 2). Now Proposition 6 gives

$$D_n^{\mathrm{sd}}(s)=\frac{1}{n!}D^{\mathrm{sd}}(s)^n+\sum_{k=1}^{n-1}\frac{1}{k!}\sum_{\nu_1+\nu_2+\cdots+\nu_k=n}\frac{D[\nu_1](s)D[\nu_2](s)\cdots D[\nu_k](s)}{\nu_1\nu_2\cdots\nu_k},\tag{10}$$

and by Proposition 3 we know that $D^{\mathrm{sd}}(s)$ is holomorphic for $\Re(s)>1/2$ except for a simple pole at $s=1$ with residue $6/\pi^2$. Thus $D^{\mathrm{sd}}(s)^n/n!$ has the properties claimed for $D_n^{\mathrm{sd}}(s)$. These properties are inherited by $D_n^{\mathrm{sd}}(s)$ itself, because for $k<n$ the term $D[\nu_1](s)D[\nu_2](s)\cdots D[\nu_k](s)/(\nu_1\nu_2\cdots\nu_k)$ on the right-hand side of (10) has at most $n-1$ factors of the form $D[\nu](s)$, and thus its pole (if any) at $s=1$ is of order at most $n-1$. Of course each such factor and hence their product is holomorphic elsewhere in the region $\Re(s)>1/2$. □

Once again we appeal to Proposition 1, obtaining:

Theorem 2. $\vartheta_{\mathbb{Q},n}^{\mathrm{ab,sd}}(x)\sim(1/n!)(6/\pi^2)^n\cdot x(\log x)^{n-1}$.

Combining Theorems 1 and 2, we see that

$$\vartheta_{\mathbb{Q},n}^{\mathrm{ab,sd}}(x)/\vartheta_{\mathbb{Q},n}^{\mathrm{ab}}(x)\sim 2\cdot\pi^{2n}/(6^n x),\tag{11}$$

a straightforward generalization of (7).

4. Does Leopoldt's conjecture have a horizontal analogue?

Our asymptotic estimate $\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(x) \sim 6x/\pi^2$ has the following generalization to the case of an arbitrary number field F:

Theorem 3. *$\vartheta^{\mathrm{sd}}_{F,1}(x) \sim cx$ with a constant $c > 0$ depending on F.*

To prove Theorem 3 we will exploit the fact that in the quadratic case, $\mathfrak{d}_{K/F}$ equals the conductor of the relevant quadratic character. In other words, let $\mathcal{K}$ be the set of extensions K of F (inside some fixed algebraic closure $\overline{F}$ of F) with $[K : F] \leqslant 2$, and given $K \in \mathcal{K}$ let $\chi_K : \mathrm{Gal}(\overline{F}/F) \to \{\pm 1\}$ be the character with kernel $\mathrm{Gal}(\overline{F}/K)$. Then the map $K \mapsto \chi_K$ is a bijection from $\mathcal{K}$ to the set of self-dual characters of $\mathrm{Gal}(\overline{F}/F)$, and $\mathfrak{q}(\chi_K) = \mathfrak{d}_{K/F}$, whence $q(\chi_K) = d_{K/F}$. Consequently $\vartheta^{\mathrm{sd}}_{F,1}(x) = 1 + \eta_{F,2}(x)$ for $x \geqslant 1$, and Theorem 3 simply asserts that

$$\eta_{F,2}(x) \sim cx \tag{12}$$

with a positive constant c depending on F.

The proof of (12) is straightforward but laborious, and we relegate it to an appendix (Section 14). For now the main point is that we are able to count quadratic characters of $\mathrm{Gal}(\overline{F}/F)$ by counting quadratic extensions of F, so in effect by counting elements of $F^{\times}/F^{\times 2}$. This approach is no longer available if we want to count one-dimensional characters of $\mathrm{Gal}(\overline{F}/F)$ of arbitrary order, and in fact if F is not $\mathbb{Q}$ or an imaginary quadratic field then the asymptotic behavior of $\vartheta_{F,1}(x)$ seems to be unknown. However it is easy to give an upper bound:

Proposition 8. *$\vartheta_{F,1}(x) = O(x^2)$, where the implied constant depends on F.*

In the case where F has units of infinite order, Josh Zelinsky has proved the stronger assertion that $\vartheta_{F,1}(x) = o(x^2)$. But let us prove Proposition 8 as it stands: First of all, we identify one-dimensional characters of $\mathrm{Gal}(\overline{F}/F)$ with idele class characters of F of finite order, or equivalently with primitive ray class characters of F. Given a nonzero integral ideal $\mathfrak{q}$ of F, write $h^{\mathrm{nar}}_F(\mathfrak{q})$ for the order of the narrow ray class group of F to the modulus $\mathfrak{q}$. Then

$$\vartheta_{F,1}(x) \leqslant \sum_{\mathbf{N}\mathfrak{q} \leqslant x} h^{\mathrm{nar}}_F(\mathfrak{q}), \tag{13}$$

because $h^{\mathrm{nar}}_F(\mathfrak{q})$ is equal to the number of primitive ray class characters of F of conductor dividing $\mathfrak{q}$ and is thus an upper bound for the number of such characters of conductor exactly $\mathfrak{q}$.

On the other hand, let $\mathcal{O}_F$ be the ring of integers of F and $\mathcal{O}_F^{\times}$ its unit group. It is convenient to put $U_F = \mathcal{O}_F^{\times}$ and to write $U_F(\mathfrak{q})$ for the subgroup of U_F consisting of units congruent to 1 modulo $\mathfrak{q}$. We also write $U_F^{+}(\mathfrak{q})$ for the subgroup of totally positive units in $U_F(\mathfrak{q})$. Finally, let h_F be the class number and $r_1(F)$ and $2r_2(F)$ the number of real and complex embeddings of F. According to a classic formula (cf. [23], p. 127, Theorem 1),

$$h^{\mathrm{nar}}_F(\mathfrak{q}) = 2^{r_1(F)} \cdot h_F \cdot \varphi_F(\mathfrak{q}) / [U_F : U_F^{+}(\mathfrak{q})], \tag{14}$$

where $\varphi_F(\mathfrak{q}) = |(\mathcal{O}_F/\mathfrak{q})^{\times}|$. As $\varphi_F(\mathfrak{q}) \leqslant \mathbf{N}\mathfrak{q}$ and $[U_F : U_F^{+}(\mathfrak{q})] \geqslant 1$, we see on returning to (13) that $\vartheta_{F,1}(x)$ is bounded by a constant times $\sum_{\mathbf{N}\mathfrak{q} \leqslant x} \mathbf{N}(\mathfrak{q})$. The latter expression is the summatory function associated to $\zeta_F(s-1)$, where $\zeta_F(s)$ is the Dedekind zeta function of F, so Proposition 8 now follows from Proposition 1.

Problem. *Determine whether* $\vartheta_{F,1}(x) \sim c \cdot x^a$ *with constants* $c > 0$ *and* $a > 1$ *depending on* F.

The underlying issue here is the average size of $[U_F : U_F^+(\mathfrak{q})]$, about which little seems to be known. Of some relevance, perhaps, is the literature on analogues of Artin's primitive root conjecture for units of number fields (see for example [9], [18], [19], [20], [25], [29], and [30]). In any case, $[U_F : U_F^+(\mathfrak{q})]$ differs by a factor dividing $2^{r_1(F)}$ from the order of the image of the natural map from U_F to $(\mathcal{O}_F/\mathfrak{q})^\times$, so the problem is to understand the image of the global units in an approximation to a group of local units. This formulation is reminiscent of Leopoldt's conjecture, which we now revisit for the sake of the analogy.

Fix a prime number p and let θ_n be the number of one-dimensional characters of $\mathrm{Gal}(\overline{F}/F)$ of conductor dividing $p^n\mathcal{O}_F$. We think of θ_n as a vertical analogue of $\vartheta_{F,1}(x)$. To simplify the notation, write $U_F^+(p^n\mathcal{O}_F)$ as $U_F^+(p^n)$, and put

$$E_n = U_F^+(p^n) \tag{15}$$

for $n \geqslant 2$. Also put $E = E_2$. Via the map $u \mapsto u \otimes 1$ we may view E as a subset of $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and more precisely as a subgroup of $(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ and indeed of $1 + p^2(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. We denote the p-adic closure of a subset S of $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ by $\overline{S}$, and we write $r_1(F)$ and $r_2(F)$ simply as r_1 and r_2. Leopoldt's conjecture is usually stated as (i) or (ii) below.

Proposition 9. *The following statements are equivalent:*

(i) $\mathrm{rk}_{\mathbb{Z}_p}\mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), \mathbb{Z}_p) = r_2 + 1$.
(ii) $\mathrm{rk}_{\mathbb{Z}_p}\overline{E} = r_1 + r_2 - 1$.
(iii) $\log\theta_n \sim (r_2 + 1)\log p \cdot n$.

Thus (iii) *is another formulation of Leopoldt's conjecture.*

Proof. The equivalence of (i) and (ii) is well known, cf. [36], p. 265, Theorem 13.4. (Strictly speaking, the unit group E_1 in [36] is not quite the same as our E, but our E is a subgroup of finite index in E_1 and so the p-adic closures have the same $\mathbb{Z}_p$-rank.) For the sake of completeness we will verify that (ii) is equivalent to (iii), although the argument is in principle the same as in [36].

Put $s = \mathrm{rk}_{\mathbb{Z}_p}\overline{E}$ and $t = [F : \mathbb{Q}] - \mathrm{rk}_{\mathbb{Z}_p}\overline{E}$, so that

$$s + t = r_1 + 2r_2. \tag{16}$$

It suffices to see that there is a constant $c > 0$ such that

$$\theta_n = cp^{tn} \tag{17}$$

for n sufficiently large. Indeed (17) implies that $\log\theta_n \sim (t\log p) \cdot n$, whence (iii) becomes equivalent to $t = r_2 + 1$; but (ii) is equivalent to $s = r_1 + r_2 - 1$, and the equations $t = r_2 + 1$ and $s = r_1 + r_2 - 1$ are equivalent by (16).

To derive (17) we use the fact that $\theta_n = h_F^{\mathrm{nar}}(p^n\mathcal{O}_F)$. It is readily verified that $\varphi_F(p^n\mathcal{O}_F) = p^{n[F:\mathbb{Q}]}\prod_{\mathfrak{p}|p}(1 - (\mathbf{N}\mathfrak{p})^{-1})$, so (14) gives

$$\theta_n = c_1 \cdot p^{n[F:\mathbb{Q}]}/[U_F : U_F^+(p^n)] \tag{18}$$

with $c_1 = 2^{r_1} \cdot h_F \cdot \prod_{\mathfrak{p}|p}(1 - (\mathbf{N}\mathfrak{p})^{-1})$.

On the other hand, recalling the notation (15), we can write

$$[U_F : U_F^+(p^n)] = [U_F : E][E : E_n]$$

for $n \geqslant 2$. As the natural map $E/E_n \to \overline{E}/\overline{E_n}$ is an isomorphism, it follows that

$$[U_F : U_F^+(p^n)] = c_2[\overline{E} : \overline{E_n}] \tag{19}$$

with $c_2 = [U_F : E]$. Now the p-adic logarithm $\log_p$ gives an isomorphism

$$\overline{E}/\overline{E_n} \cong (\log_p \overline{E})/((\log_p \overline{E}) \cap p^n \mathcal{O}_F),$$

so we have

$$[\overline{E} : \overline{E_n}] = [L : L \cap (p^n \mathcal{O}_F)] \tag{20}$$

with $L = \log_p \overline{E}$. Put $m = [F : \mathbb{Q}_p]$. As $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module of rank m and L is a $\mathbb{Z}_p$-submodule of rank s, there exists a basis $e_1, e_2, \ldots, e_m$ for $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ together with integers $\nu_1, \nu_2, \ldots \nu_s \geqslant 0$ such that $p^{\nu_1} e_1, p^{\nu_2} e_2, \ldots, p^{\nu_s} e_s$ is a basis for L. Returning to (20), we see that if $n \geqslant \max(\nu_1, \nu_2, \ldots, \nu_s)$ then

$$[\overline{E} : \overline{E_n}] = c_3 p^{ns} \tag{21}$$

with $c_3 = p^{-(\nu_1+\nu_2+\cdots+\nu_s)}$. Finally, combining (21) with (18) and (19), and setting $c = c_1/(c_2c_3)$, we obtain (17) for n sufficiently large. □

5. Dihedral representations

A finite subgroup G of $\mathrm{GL}_n(\mathbb{C})$ is *irreducible* if the tautological representation $\iota : G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ is irreducible. Similarly, G is *monomial* if ι is monomial, and G is *self-dual* if ι is self-dual. Let D_{2m} denote the dihedral group of order $2m$ ($m \geqslant 3$) and Q_{4m} the quaternion group of order $4m$ ($m \geqslant 2$). The term "quaternion group" is used here as in [27], p. 72, but since it is often reserved for the case $m = 2$, let us recall the standard presentations: D_{2m} has generators a, b with $a^m = 1 = b^2$ and $bab^{-1} = a^{-1}$, while Q_{4m} has generators a, b with $a^{2m} = 1$, $a^m = b^2$, and $bab^{-1} = a^{-1}$. These are the only groups that figure in $\vartheta_{\mathbb{Q},2}^{\mathrm{im,sd}}(x)$:

Proposition 10. *Let G be a finite subgroup of $\mathrm{GL}_2(\mathbb{C})$. If G is irreducible, monomial, and self-dual then either $G \cong D_{2m}$ with $m \geqslant 3$ or $G \cong Q_{4m}$ with $m \geqslant 2$. In the former case G is conjugate to a subgroup of $\mathrm{O}_2(\mathbb{R})$ and in the latter case $G \subset \mathrm{SL}_2(\mathbb{C})$.*

A two-dimensional irreducible monomial self-dual Artin representaton ρ will be called *dihedral* or *quaternionic* according as the image of ρ is isomorphic to D_{2m} ($m \geqslant 3$) or to Q_{4m} ($m \geqslant 2$). We also put $m(\rho) = m$. Since $\mathrm{SL}_2(\mathbb{C})$ and $\mathrm{Sp}_2(\mathbb{C})$ coincide, we see that the orthogonal and symplectic terms in the decomposition

$$\vartheta_{\mathbb{Q},2}^{\mathrm{im,sd}}(x) = \vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(x) + \vartheta_{\mathbb{Q},2}^{\mathrm{im,symp}}(x) \tag{22}$$

count dihedral and quaternionic Artin representations of $\mathbb{Q}$ respectively. In this section we bound the the dihedral term $\vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(x)$.

Proposition 10 is a standard remark, as are Propositions 11 and 12 below, but for want of a suitable reference we supply proofs of all three assertions in an appendix (Section 13). Given a group G, a normal subgroup H, a one-dimensional character χ of H, and an element $g \in G$, write χ^g for the character $h \mapsto \chi(ghg^{-1})$ of H.

Proposition 11. *Let G be a finite group and ρ a faithful irreducible monomial self-dual representation of G of dimension two. Then G has a cyclic subgroup of index two, and if H is any such subgroup then ρ is induced by a faithful one-dimensional character ξ of H of order $\geqslant 3$ satisfying $\xi^g = \xi^{-1}$ for $g \in G \smallsetminus H$. Furthermore, ξ and ξ^{-1} are the only two characters of H inducing ρ.*

Given a finite group G and a subgroup H, write G^{ab} and H^{ab} for their maximal abelian quotients and $\mathrm{tran}_H^G : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ for the transfer. If ξ is a one-dimensional character of H then ξ factors through H^{ab}, whence we can form the composition $\xi \circ \mathrm{tran}_H^G$ and view it as a one-dimensional character of G. We write sign_H^G for the sign of the permutation representation of G on the left cosets of H in G, and we write 1 for the trivial one-dimensional character of any group. Finally, if λ is a representation of H then $\mathrm{ind}_H^G\lambda$ denotes the representation of G induced by λ. Part (a) of the following proposition is a converse to Proposition 11 and part (b) is a refinement of it.

Proposition 12. *Let G be a finite group and H a subgroup of index two, and let ξ be a faithful one-dimensional character of H of order $\geqslant 3$. Put $\rho = \mathrm{ind}_H^G\xi$.*

(a) *If $\xi^g = \xi^{-1}$ for $g \in G \smallsetminus H$ then ρ is faithful, irreducible, and self-dual.*

(b) *The hypothesis of* (a) *holds if and only if $\xi \circ \mathrm{tran}_H^G$ is either* 1 *or sign_H^G, and these two alternatives imply respectively that ρ is orthogonal or symplectic.*

Now let F be a number field. Given a finite extension K of F (always understood to be contained in some fixed algebraic closure $\overline{F}$ of F) and an Artin representation λ of K, we write $\mathrm{ind}_{K/F}\lambda$ for the Artin representation of F induced by λ. We may think of $\mathrm{ind}_{K/F}$ either as induction from $\mathrm{Gal}(\overline{F}/K)$ to $\mathrm{Gal}(\overline{F}/F)$ or as induction from $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(L/K)$, where L is any finite Galois extension of F containing K such that λ factors through $\mathrm{Gal}(L/K)$. Similarly, $\mathrm{tran}_{K/F}$ denotes the transfer from $\mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}}$ to $\mathrm{Gal}(\overline{F}/K)^{\mathrm{ab}}$ or alternatively the transfer from $\mathrm{Gal}(L/F)^{\mathrm{ab}}$ to $\mathrm{Gal}(L/K)^{\mathrm{ab}}$, where L is any finite Galois extension of F containing K. Of course in the case of a topological group like $\mathrm{Gal}(\overline{F}/F)$ the notation G^{ab} refers to the quotient of G by the *closure* of its commutator subgroup.

Proposition 13. *Consider pairs (K, ξ) with $[K : F] = 2$ and ξ a one-dimensional character of $\mathrm{Gal}(\overline{F}/K)$ of order $m \geqslant 3$ such that $\xi \circ \mathrm{tran}_{K/F} = 1$. The formula $\rho = \mathrm{ind}_{K/F}\xi$ defines a two-to-one map from the set of such (K, ξ) onto the set of isomorphism classes of dihedral Artin representations ρ of F with $m(\rho) = m$, the other preimage of the isomorphism class of ρ being the pair (K, ξ^{-1}).*

Proof. Given a dihedral Artin representation ρ of F, let L be the fixed field of $\mathrm{Ker}\,\rho$ and put $G = \mathrm{Gal}(L/F)$. By Proposition 11 and part (b) of Proposition 12, $\rho = \mathrm{ind}_{K/F}\xi$ for some (K, ξ) as above. Conversely, given (K, ξ), we have $\xi^g = \xi^{-1}$ for $g \in \mathrm{Gal}(\overline{F}/F) \smallsetminus \mathrm{Gal}(\overline{F}/K)$ by part (b) of Proposition 12. Hence the fixed field L of $\mathrm{Ker}\,\xi$ is Galois over F, and part (a) of Proposition 12 shows that the representation $\rho = \mathrm{ind}_{K/F}\xi$ is irreducible and orthogonal, as well as faithful as a representation of $\mathrm{Gal}(L/F)$. Hence it follows from Proposition 10 that ρ has image D_{2m}. Since a cyclic subgroup of index two in D_{2m} is unique, ρ determines K uniquely, and the last assertion of Proposition 11 then implies that ξ is unique up to replacement by ξ^{-1}. $\square$

If $\rho = \mathrm{ind}_{K/F}\xi$ then $\mathfrak{q}(\rho) = \mathfrak{d}_{K/F}\,\mathfrak{q}(\xi)$ by the conductor-discriminant formula (cf. [32], p. 104, Proposition 6), whence $q(\rho) = d_{K/F}\,q(\xi)$ on taking absolute norms. Thus Proposition 13 gives

$$\vartheta_{F,2}^{\mathrm{im,orth}}(x) = \frac{1}{2} \sum_{d_{K/F}q(\xi) \leqslant x} 1, \tag{23}$$

where the sum runs over ordered pairs (K, ξ) satisfying the stated inequality.

We now rewrite (23) using class field theory: A one-dimensional character ξ of $\mathrm{Gal}(\overline{F}/K)$ becomes an idele class character of K of finite order, and the condition $\xi \circ \mathrm{tran}_{K/F} = 1$ becomes $\xi | \mathbb{A}_F^\times = 1$, where $\mathbb{A}_F^\times$ is the idele group of F.

Lemma. *There is an ideal* $\mathfrak{q}$ *of* $\mathcal{O}_F$ *such that* $\mathfrak{q}(\xi) = \mathfrak{q}\mathcal{O}_K$.

Proof. This is a straightforward deduction from the fact that $\xi|\mathbb{A}_F^\times = 1$. Only one point deserves comment: If v is a finite place of F which ramifies in K and w is the place of K above v, then the local component ξ_w of ξ has *even* conductor-exponent $a(\xi_w)$. To see this, let $\mathcal{O}_{F,v}$ and $\mathcal{O}_{K,w}$ be the completions of $\mathcal{O}_F$ and $\mathcal{O}_K$, and let π_w be a uniformizer of $\mathcal{O}_{K,w}$. If $a = a(\xi_w)$ is odd then the cosets of $1 + \pi_w^a \mathcal{O}_{K,w}$ in $1 + \pi_w^{a-1}\mathcal{O}_{K,w}$ (or in $\mathcal{O}_{K,w}^\times$, if $a = 1$) are represented by elements of $\mathcal{O}_{F,v}^\times$, whence the nontriviality of ξ_w on the quotient contradicts the triviality of ξ on $\mathbb{A}_F^\times$. □

Given a nonzero integral ideal $\mathfrak{q}$ of F, let $g_{K/F}(\mathfrak{q})$ be the number of idele class characters of K of finite order $\geqslant 3$ which are trivial on $\mathbb{A}_F^\times$ and of conductor $\mathfrak{q}\mathcal{O}_K$. Returning to (23), we see that $\vartheta_{F,2}^{\mathrm{im,orth}}(x) = 1/2 \sum g_{K/F}(\mathfrak{q})$, where the sum runs over pairs $(K, \mathfrak{q})$ with $d_{K/F}(\mathbf{N}\mathfrak{q})^2 \leqslant x$. It follows in particular that

$$\vartheta_{F,2}^{\mathrm{im,orth}}(x) \leqslant \frac{1}{2} \sum_{d_{K/F}(\mathbf{N}\mathfrak{q})^2 \leqslant x} h_{K/F}^{\mathrm{nar}}(\mathfrak{q}), \tag{24}$$

where $h_{K/F}^{\mathrm{nar}}(\mathfrak{q})$ is the number of idele class characters of K of *arbitrary* finite order which are trivial on $\mathbb{A}_F^\times$ and of conductor *dividing* $\mathfrak{q}\mathcal{O}_K$.

Now take $F = \mathbb{Q}$. We write $h_{K/F}^{\mathrm{nar}}(\mathfrak{q})$ simply as $h_{K/\mathbb{Q}}^{\mathrm{nar}}(q)$, where q is the positive integer such that $\mathfrak{q} = q\mathcal{O}_K$. If the quadratic field K is imaginary then $h_{K/\mathbb{Q}}^{\mathrm{nar}}(q)$ may be further abbreviated to $h_{K/\mathbb{Q}}(q)$. Thus (24) becomes

$$\vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(x) \leqslant \frac{1}{2} \sum_{\substack{d_K q^2 \leqslant x \\ K \text{ imaginary}}} h_{K/\mathbb{Q}}(q) + \frac{1}{2} \sum_{\substack{d_K q^2 \leqslant x \\ K \text{ real}}} h_{K/\mathbb{Q}}^{\mathrm{nar}}(q). \tag{25}$$

Siegel [35] proved the asymptotic formulas

$$\sum_{\substack{d_K q^2 \leqslant x \\ K \text{ imaginary}}} h_{K/\mathbb{Q}}(q) \sim \pi x^{3/2}/(18\zeta(3)) \tag{26}$$

and

$$\sum_{\substack{d_K q^2 \leqslant x \\ K \text{ real}}} h_{K/\mathbb{Q}}^{\mathrm{nar}}(q) \log \epsilon_{K,q} \sim \pi^2 x^{3/2}/(18\zeta(3)), \tag{27}$$

where $\epsilon_{K,q}$ is the fundamental totally positive unit of the order $\mathcal{O}_{K,q} = \mathbb{Z} + q\mathcal{O}_K$: In other words, $\epsilon_{K,q}$ is the unique generator > 1 of the group $U_{K,q}^+ = U_K^+ \cap U_{K,q}$, where $U_{K,q} = \mathcal{O}_{K,q}^\times$. Since $\log \epsilon_{K,q} \gg 1$ (indeed $\epsilon_{K,q} > q\sqrt{d}/2 \geqslant \sqrt{5}/2$) we deduce the following bound from (25), (26), and (27).

Proposition 14. $\vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(x) = O(x^{3/2})$.

One point deserves clarification. Put $d = \pm d_K q^2$, choosing the sign so that $\pm d_K$ is the discriminant of K. The quantity $h_{K/\mathbb{Q}}^{\mathrm{nar}}(q)$ as we have defined it is *the narrow ring class number of* K *to the modulus* q, whereas the results which we have quoted from [35] pertain to *the narrow class number of primitive binary quadratic forms of discriminant d*. The equality of these two quantities is of course classical and can be established conceptually, but we will take the shortcut of recalling a standard formula for $h^{\mathrm{nar}}_{K/\mathbb{Q}}(q)$, which upon comparison with formulas (10) and (19) of [35] (and an application of Dirichlet's class number formula) will assure us that Siegel's h_d coincides with our $h^{\mathrm{nar}}_{K/\mathbb{Q}}(q)$. Let χ_K be the primitive quadratic Dirichlet character corresponding to K. We write h^{nar}_K for the narrow ideal class number of K (equal to h_K if K is imaginary).

Proposition 15. $h^{\mathrm{nar}}_{K/\mathbb{Q}}(q) = \dfrac{h^{\mathrm{nar}}_K}{[U^+_K : U^+_{K,q}]} \cdot q \prod_{p|q}(1 - \chi_K(p)/p)$.

Proof. The argument is classical (see for example the references to Fueter and Weber on p. 95 of [24], where the analogous formula is proved for wide ring class numbers) but we recall it briefly nonetheless.

Suppose first that K is real. Write $C^{\mathrm{nar}}_{\mathbb{Q}}(q)$ and $C^{\mathrm{nar}}_K(q)$ for the narrow ray class groups of $\mathbb{Q}$ and K to the moduli $q\mathbb{Z}$ and $q\mathcal{O}_K$ respectively, and let ω be the natural map from $C^{\mathrm{nar}}_{\mathbb{Q}}(q)$ to $C^{\mathrm{nar}}_K(q)$. Then $h^{\mathrm{nar}}_{K/\mathbb{Q}}(q)$ is the order of the cokernel of ω. Hence

$$h^{\mathrm{nar}}_{K/\mathbb{Q}}(q) = \frac{h^{\mathrm{nar}}_K(q)}{\varphi(q)} |\mathrm{Ker}\ \omega|. \tag{28}$$

Let $U_{K/\mathbb{Q}}(q)$ be the subgroup of U_K consisting of units u for which there exists $a \in \mathbb{Z}$ with $au \equiv 1$ modulo $\mathfrak{q}\mathcal{O}_K$ and $au > 0$ at both real places of K. Also put $U^+_K(q) = U^+_K(q\mathcal{O}_K)$. One checks that the map sending the ray class of $a\mathbb{Z}$ to the coset of u modulo $\{\pm 1\}U^+_K(q)$ is an isomorphism from $\mathrm{Ker}\,\omega$ onto $U_{K/\mathbb{Q}}(q)/\{\pm 1\}U^+_K(q))$. Hence (28) becomes

$$h^{\mathrm{nar}}_{K/\mathbb{Q}}(q) = \frac{h^{\mathrm{nar}}_K(q)}{\varphi(q)} [U_{K/\mathbb{Q}}(q) : \{\pm 1\}U^+_K(q)]. \tag{29}$$

Replacing F by K in (14) and inserting the result in (29), we deduce that

$$h^{\mathrm{nar}}_{K/\mathbb{Q}}(q) = h_K \cdot q \prod_{p|q}(1 - \chi_K(p)/p) \cdot \frac{2^2}{[U_K : U_{K/\mathbb{Q}}(q)][\{\pm 1\}U^+_K(q) : U^+_K(q)]}. \tag{30}$$

The stated formula follows from (30), because $[\{\pm 1\}U^+_K(q) : U^+_K(q)] = 2$ and $2h_K[U^+_K : U^+_{K,q}] = h^{\mathrm{nar}}_K[U_K : U_{K/\mathbb{Q}}(q)]$. (To verify the latter equation, consider cases according as the fundamental unit of K does or does not have norm -1, and observe that the units in $U_{K/\mathbb{Q}}(q)$ all have norm 1.)

Next suppose that K is imaginary. We take ω to be the natural map of wide ray class groups $C_{\mathbb{Q}}(q) \to C_K(q)$. The order of $C_{\mathbb{Q}}(q)$ is $\varphi(q)/2$ or $\varphi(q)$ according as $q > 2$ or $q \leqslant 2$, hence it equals $\varphi(q)/[\{\pm 1\}U_K(q) : U_K(q)]$ in all cases. Thus we have

$$h_{K/\mathbb{Q}}(q) = \frac{h_K(q)}{\varphi(q)} [U_{K/\mathbb{Q}}(q) : U_K(q)]. \tag{31}$$

in place of (29). Applying (14) as before, we obtain

$$h_{K/\mathbb{Q}}(q) = \frac{h_K}{[U_K : U_{K/\mathbb{Q}}(q)]} \cdot q \prod_{p|q}(1 - \chi_K(p)/p). \tag{32}$$

Now $[U_K : U_{K/\mathbb{Q}}(q)]$ is 1, 2, or 3 according as $d_K > 4$, $d_K = 4$, or $d_K = 3$. The same is true of $[U_K : U_{K,q}]$, so (32) is the stated formula. □

6. Quaternionic representations

Next we will prove an estimate for the quaternionic term in (22):

Proposition 16. *$\vartheta^{\mathrm{im,symp}}_{\mathbb{Q},2}(x) = O(x^{3/2+\varepsilon})$ for every $\varepsilon > 0$, where the implied constant depends on ε.*

Combining Propositions 16 and 14, we will have:

Proposition 17. *$\vartheta^{\mathrm{im,sd}}_{\mathbb{Q},2}(x) = O(x^{3/2+\varepsilon})$ for every $\varepsilon > 0$, where the implied constant depends on ε.*

We begin with a general remark. Given Artin representations ρ and ρ' of a number field F, write $\mathrm{P}\rho$ and $\mathrm{P}\rho'$ for the projective representations of $\mathrm{Gal}(\overline{F}/F)$ determined by ρ and ρ', and call ρ and ρ' *projectively equivalent* if $\mathrm{P}\rho \cong \mathrm{P}\rho'$.

Proposition 18. *Suppose that ρ and ρ' are symplectic of dimension n. Then ρ and ρ' are projectively equivalent if and only if $\rho' \cong \rho \otimes \chi$ for some one-dimensional character χ of $\mathrm{Gal}(\overline{F}/F)$ with $\chi^n = 1$.*

Proof. To say that $\mathrm{P}\rho \cong \mathrm{P}\rho'$ means precisely that $\rho' \cong \rho \otimes \chi$ for some one-dimensional character χ of $\mathrm{Gal}(\overline{F}/F)$. Taking determinants of both sides, we find that $\chi^n = 1$, because symplectic representations have trivial determinant. □

Next we state an analogue for quaternionic Artin representations of an earlier assertion about dihedral Artin representations (Proposition 13). Given a quadratic extension K of F (understood to lie in some fixed algebraic closure $\overline{F}$ of F), write $\mathrm{sign}_{K/F}$ for the quadratic character of $\mathrm{Gal}(\overline{F}/F)$ with kernel $\mathrm{Gal}(\overline{F}/K)$.

Proposition 19. *Consider pairs (K, ξ) with $[K : F] = 2$ and ξ a one-dimensional character of $\mathrm{Gal}(\overline{F}/K)$ of even order $2m \geqslant 6$ such that $\xi \circ \mathrm{tran}_{K/F} = \mathrm{sign}_{K/F}$. The formula $\rho = \mathrm{ind}_{K/F}\xi$ defines a two-to-one map from the set of such (K, ξ) onto the set of isomorphism classes of quaternionic Artin representations ρ of F with $m(\rho) = m$, the other preimage of the isomorphism class of ρ being the pair (K, ξ^{-1}).*

This is simply Proposition 13 with three changes: the word "dihedral" is replaced by "quaternionic" and the conditions "order $m \geqslant 3$" and "$\xi \circ \mathrm{tran}_{K/F} = 1$" by "even order $2m \geqslant 6$" and "$\xi \circ \mathrm{tran}_{K/F} = \mathrm{sign}_{K/F}$." (Acutally the requirement that ξ have *even* order is superfluous; it follows from the condition $\xi \circ \mathrm{tran}_{K/F} = \mathrm{sign}_{K/F}$). The proof of Proposition 19 is likewise identical to that of Proposition 13, apart from the obvious changes. Note in particular that in terms of the presentation of Q_{4m} given in Section 5, the elements $a^j b$ and $a^j b^3$ have order four, whence for $m \geqslant 3$ a cyclic subgroup of index two in Q_{4m} is unique, just as it is in D_{2m}. By contrast, Q_8 has three cyclic subgroups of index two, and as a result the analogue of Proposition 19 for $m(\rho) = 2$ is as follows:

Proposition 20. *Consider pairs (K, ξ) with $[K : F] = 2$ and ξ a one-dimensional character of $\mathrm{Gal}(\overline{F}/K)$ of order 4 such that $\xi \circ \mathrm{tran}_{K/F} = \mathrm{sign}_{K/F}$. The formula $\rho = \mathrm{ind}_{K/F}\xi$ defines a six-to-one map from the set of such (K, ξ) onto the set of isomorphism classes of quaternionic Artin representations ρ of F with $m(\rho) = 2$. If L is the fixed field of $\mathrm{Ker}\,\rho$ and K_1, K_2 and K_3 are the three quadratic extensions of F contained in L then the six preimages of the isomorphism class of ρ have the form $(K_j, \xi_j^{\pm 1})$ with $1 \leqslant j \leqslant 3$ and one-dimensional characters ξ_j of $\mathrm{Gal}(\overline{F}/K_j)$.*

Our strategy for bounding the quaternionic term in (22) rests on a simple remark: Given a quaternionic Artin representation ρ of F with $m(\rho) \geqslant 3$, we can define a dihedral Artin representation $\hat{\rho}$ of F by writing $\rho \cong \mathrm{ind}_{K/F}\xi$ as in Proposition 19 and setting $\hat{\rho} = \mathrm{ind}_{K/F}\xi^2$. That the isomorphism class of $\hat{\rho}$ is well defined follows from Proposition 13, which also gives

$$m(\rho) = m(\hat{\rho}). \tag{33}$$

Using Proposition 20, we can define $\hat{\rho}$ in the same way when $m(\rho) = 2$, but because of the nonuniqueness of K in Proposition 20 we must make an arbitrary but fixed choice of a quadratic extension K of F inside every biquadratic extension of F. Note that $\hat{\rho}$ is now reducible; in fact if L is the fixed field of Ker ρ then $\hat{\rho} \cong \chi \oplus \chi'$, where χ and χ' are the two quadratic characters of $\mathrm{Gal}(L/F)$ which do not factor through $\mathrm{Gal}(K/F)$. Thus $\hat{\rho}$ is no longer "dihedral," but we still set $m(\hat{\rho}) = 2$, so that (33) holds in all cases. Another formula which holds in all cases is

$$q(\rho) \geqslant q(\hat{\rho}), \tag{34}$$

because $q(\rho) = d_{K/F}\, q(\xi)$ and $q(\hat{\rho}) = d_{K/F}\, q(\xi^2)$ by the conductor-discriminant formula, and $q(\xi) \geqslant q(\xi^2)$. Finally, it follows from Proposition 10 that if ρ is a quaternionic Artin representation of F and χ is a one-dimensional character of $\mathrm{Gal}(\overline{F}/F)$ with $\chi^2 = 1$ then $\rho \otimes \chi$ is again a quaternionic Artin representation of F. Now if ρ is replaced by $\rho \otimes \chi$ then ξ is multiplied by $\mathrm{res}_{K/F}(\chi)$, the restriction of χ to $\mathrm{Gal}(\overline{F}/K)$. But as $\chi^2 = 1$ the character ξ^2 is unchanged, and hence $\hat{\rho}$ is unchanged up to isomorphism. Referring to Proposition 18, we deduce that the isomorphism class $\langle\hat{\rho}\rangle$ of $\hat{\rho}$ depends only on the projective equivalence class $[\rho]$ of ρ, so we obtain a map $[\rho] \mapsto \langle\hat{\rho}\rangle$.

Proposition 21. *The map $[\rho] \mapsto \langle\hat{\rho}\rangle$ is injective.*

Proof. In view of (33), it suffices to verify injectivity on the subset of projective equivalence classes $[\rho]$ for which $m(\rho)$ has a fixed value m. To begin with we take $m \geqslant 3$. So suppose that we are given quaternionic Artin representations ρ and ρ' of F with $m(\rho) = m(\rho') = m \geqslant 3$. Write $\rho \cong \mathrm{ind}_{K/F}\xi$ and $\rho' \cong \mathrm{ind}_{K'/F}\xi'$ with pairs (K, ξ) and (K', ξ') as in Proposition 19. We assume that

$$\mathrm{ind}_{K/F}\xi^2 \cong \mathrm{ind}_{K'/F}(\xi')^2 \tag{35}$$

and must deduce that $\mathrm{P}\rho \cong \mathrm{P}\rho'$.

Since $m \geqslant 3$, the representations $\mathrm{ind}_{K/F}\xi^2$ and $\mathrm{ind}_{K/F}(\xi')^2$ are dihedral. Hence in view of (35), we have $K = K'$ and $(\xi')^2 = \xi^{\pm 2}$ by Proposition 13. After replacing the pair (K, ξ) by (K, ξ^{-1}) if necessary, we may assume that $(\xi')^2 = \xi^2$, and then $\xi' = \xi\phi$ for some character ϕ of $\mathrm{Gal}(\overline{F}/K)$ with $\phi^2 = 1$. Since $\xi \circ \mathrm{tran}_{K/F}$ and $\xi' \circ \mathrm{tran}_{K/F}$ both coincide with $\mathrm{sign}_{K/F}$, it follows that $\phi \circ \mathrm{tran}_{K/F} = 1$. Let us now view ϕ as an idele class character of K. Then the condition $\phi \circ \mathrm{tran}_{K/F} = 1$ becomes $\phi|\mathbb{A}_F^\times = 1$. In particular, $\phi \circ N_{K/F} = 1$, where $N_{K/F}$ is the idelic norm from $\mathbb{A}_K^\times$ to $\mathbb{A}_F^\times$. Write σ for the nontrivial element of $\mathrm{Gal}(K/F)$, and view σ as an automorphism of $\mathbb{A}_K^\times$. Then $\phi(x^{\sigma+1}) = 1$ for all $x \in \mathbb{A}_K^\times$, and as $\phi^2 = 1$ we deduce that $\phi(x^{\sigma-1}) = 1$ also. Hilbert's Theorem 90 now implies that ϕ factors through $N_{K/F}$, so that $\phi = \chi \circ N_{K/F}$ for some one-dimensional character χ of $\mathbb{A}_F^\times$. Returning to the Galois setting, we see that $\phi = \mathrm{res}_{K/F}(\chi)$ when ϕ and χ are viewed as one-dimensional characters of $\mathrm{Gal}(\overline{F}/K)$ and $\mathrm{Gal}(\overline{F}/F)$ respectively.

To recapitulate, we have $\rho \cong \mathrm{ind}_{K/F}\xi$, $\rho' \cong \mathrm{ind}_{K'/F}\xi'$, $K = K'$, $\xi' = \xi\phi$, and $\phi = \mathrm{res}_{K/F}(\chi)$. It follows that $\rho' \cong \rho \otimes \chi$, whence $\mathrm{P}\rho \cong \mathrm{P}\rho'$.

The case $m = 2$ is contained in Theorem 4 on p. 146 of [12], at least for $F = \mathbb{Q}$. However for the sake of completing the present argument, we first observe that if χ and χ' are distinct quadratic characters of $\mathrm{Gal}(\overline{F}/F)$, then there is a unique pair (K, ζ) consisting of a quadratic extension K of F and a quadratic character ζ of $\mathrm{Gal}(\overline{F}/K)$ such that $\mathrm{ind}_{K/F}(\zeta) \cong \chi \oplus \chi'$. Indeed if M and M' are the fixed fields of the kernels of χ and χ' respectively then K is the third quadratic extension of F contained in MM', and ζ is the unique quadratic character of $\mathrm{Gal}(\overline{F}/K)$ which factors through $\mathrm{Gal}(MM'/K)$. It follows that in the case $m = 2$, the isomorphism (35) still implies that $K = K'$ and $\xi^2 = (\xi')^2$. The proof is now completed as in the case $m \geqslant 3$. □

Now take $F = \mathbb{Q}$, and let X be the set of one-dimensional characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfying $\chi^2 = 1$. The arguments to be given next will be needed again when we deal with primitive representations, so it is efficient to suspend our focus on quaternionic Artin representations in favor of a more general setting. Thus $\mathcal{A}$ will denote any class of two-dimensional Artin representations of $\mathbb{Q}$ which is *symplectic* and *closed under quadratic twists* in the sense that the following conditions hold:

- If $\rho \in \mathcal{A}$ then $\det \rho = 1$.
- If $\rho \in \mathcal{A}$ and $\chi \in X$ then $\rho \otimes \chi \in \mathcal{A}$.
- If $\rho \in \mathcal{A}$ and $\rho' \cong \rho$ then $\rho' \in \mathcal{A}$.

The third condition is an inessential nicety intended only to eliminate ambiguities. We write $\vartheta_{\mathcal{A}}(x)$ for the number of isomorphism classes of representations $\rho \in \mathcal{A}$ such that $q(\rho) \leqslant x$.

Let $\mathcal{E}$ denote the set of projective equivalence classes of $\mathcal{A}$, and write $[\rho]$ as before for the projective equivalence class of ρ. Proposition 18 implies that

$$\vartheta_{\mathcal{A}}(x) \leqslant \sum_{[\rho]\in\mathcal{E}} \sum_{\substack{\chi\in X \\ q(\rho\otimes\chi)\leqslant x}} 1, \tag{36}$$

the inner sum being independent of the choice of representative ρ of $[\rho]$. The reason for inequality rather than equality in (36) is that sometimes $\rho \otimes \chi \cong \rho$ with $\chi \neq 1$.

In order to bound the right-hand side of (36) it is convenient to introduce the notion of the "ρ-conductor" $q_\rho(\chi)$ of a character $\chi \in X$. Let ord_p denote the p-adic valuation of $\mathbb{Z}$. We define $q_\rho(\chi)$ by deleting from $q(\chi)$ the contributions of the primes dividing $q(\rho)$:

$$q_\rho(\chi) = \prod_{p \nmid q(\rho)} p^{\mathrm{ord}_p q(\chi)}. \tag{37}$$

Then we have the following elementary remark:

Proposition 22. *Each projective equivalence class $E \in \mathcal{E}$ has a representative ρ such that $q(\rho \otimes \chi) \geqslant q(\rho) q_\rho(\chi)^2$ for all $\chi \in X$.*

Proof. Write $E = [\lambda]$ with $\lambda \in \mathcal{A}$. We must exhibit a character $\phi \in X$ such that the representation $\rho = \lambda \otimes \phi$ satisfies the stated inequality for all $\chi \in X$.

Given a prime p, let $X_p \subset X$ be the subset of characters $\chi \in X$ which are unramified outside p and infinity. Thus $|X_2| = 4$, and if p is odd then $|X_p| = 2$. In particular, X_p is finite, so for each p dividing $q(\lambda)$ we can choose $\phi_p \in X_p$ minimizing

$\mathrm{ord}_p\, q(\lambda \otimes \phi_p)$. We put $\phi = \prod_{p|q(\lambda)} \phi_p$, and as already indicated, $\rho = \lambda \otimes \phi$. By construction, every prime p dividing $q(\rho)$ divides $q(\lambda)$, and for every such p and every $\chi \in X$ we have

$$\mathrm{ord}_p\, q(\rho \otimes \chi) \geqslant \mathrm{ord}_p\, q(\rho) \qquad (p|q(\rho)). \tag{38}$$

On the other hand, if $p \nmid q(\rho)$ then the restriction of ρ to an inertia subgroup at p is the two-dimensional trivial representation, whence the restriction of $\rho \otimes \chi$ coincides with that of $\chi \oplus \chi$. Therefore

$$\mathrm{ord}_p\, q(\rho \otimes \chi) = 2\, \mathrm{ord}_p\, q(\chi) \qquad (p \nmid q(\rho)). \tag{39}$$

The stated inequality follows from (38) and (39). □

Henceforth we assume that in the sum in (36) over equivalence classes $[\rho] \in \mathcal{E}$, the representative ρ is chosen as in Proposition 22. Then

$$\vartheta_{\mathcal{A}}(x) \leqslant \sum_{[\rho]\in\mathcal{E}} \sum_{\substack{\chi\in X \\ q_\rho(\chi)\leqslant(x/q(\rho))^{1/2}}} 1, \tag{40}$$

because the summation in (36) runs over a subset of the set of summation in (40). The next step eliminates the inner sum in (40):

Proposition 23. *For every $\varepsilon > 0$,*

$$\vartheta_{\mathcal{A}}(x) \ll x^{1/2} \sum_{\substack{[\rho]\in\mathcal{E} \\ q(\rho)\leqslant x}} q(\rho)^{-1/2+\varepsilon},$$

where the implicit constant depends on ε.

Proof. Given $[\rho] \in \mathcal{E}$, we define a map $\chi \mapsto \chi_\rho$ from X to itself as follows: Write $\chi = \prod_{p|q(\chi)} \chi_p$ with $\chi_p \in X$ and χ_p unramified outside p and infinity; then

$$\chi_\rho = \prod_{\substack{p|q(\chi) \\ p\nmid q(\rho)}} \chi_p.$$

Recalling the definition (37) of $q_\rho(\chi)$, we see that

$$q_\rho(\chi) = q(\chi_\rho). \tag{41}$$

for all $\chi \in X$. Furthermore an element $\lambda \in X$ has at most $2\tau(q(\rho))$ preimages under the map $\chi \mapsto \chi_\rho$, where $\tau(q)$ denotes the number of positive divisors of q. Hence on making the substitution (41) in (40) and setting $\lambda = \chi_\rho$, we obtain

$$\vartheta^{\mathrm{ip,sd}}_{\mathbb{Q},2}(x) \leqslant 2 \sum_{[\rho]\in\mathcal{E}} \sum_{\substack{\lambda\in X \\ q(\lambda)\leqslant(x/q(\rho))^{1/2}}} \tau(q(\rho)). \tag{42}$$

The inner sum in (42) equals $\tau(q(\rho)) \cdot \vartheta^{\mathrm{sd}}_{\mathbb{Q},1}((x/q(\rho))^{1/2})$ if $q(\rho) \leqslant x$ and 0 otherwise. Furthermore $\tau(q) = O(q^\varepsilon)$ for every $\varepsilon > 0$. Hence the stated estimate for $\vartheta_{\mathcal{A}}(x)$ follows from the corollary to Proposition 3. □

We now specialize to the case where $\mathcal{A}$ is the class of quaternionic Artin representations of $\mathbb{Q}$ and $\mathcal{E}$ is the set of projective equivalence classes of such representations. Combining (34) with Proposition 23, we find that

$$\vartheta_{\mathbb{Q},2}^{\mathrm{im,symp}}(x) \ll x^{1/2} \sum_{\substack{[\rho]\in\mathcal{E} \\ q(\hat{\rho})\leqslant x}} q(\hat{\rho})^{-1/2+\varepsilon} \tag{43}$$

provided $\varepsilon < 1/2$. In view of Proposition 21 we deduce that

$$\vartheta_{\mathbb{Q},2}^{\mathrm{im,symp}}(x) \ll x^{1/2} \sum_{\substack{\langle\varrho\rangle \text{ im, orth} \\ q(\varrho)\leqslant x}} q(\varrho)^{-1/2+\varepsilon} + x^{1/2} \sum_{\substack{\langle\varrho\rangle \text{ ab, sd} \\ q(\varrho)\leqslant x}} q(\varrho)^{-1/2+\varepsilon}, \tag{44}$$

where in the first sum $\langle\varrho\rangle$ denotes an *arbitrary* isomorphism class of dihedral Artin representations of $\mathbb{Q}$ (not just one of the form $\langle\hat{\rho}\rangle$) and in the second sum $\langle\varrho\rangle$ denotes an *arbitrary* isomorphism class of two-dimensional abelian self-dual Artin representations of $\mathbb{Q}$ (not just one of the form $\langle\chi\oplus\chi'\rangle$ with distinct quadratic characters χ and χ' of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$). Let us apply Abel summation to the first sum:

$$\sum_{\substack{\langle\varrho\rangle \text{ im, orth} \\ q(\varrho)\leqslant x}} q(\varrho)^{-1/2+\varepsilon} = \vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(x)x^{-1/2+\varepsilon} + (1/2-\varepsilon)\int_1^x \frac{\vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(t)}{t^{3/2-\varepsilon}}\,dt.$$

Since $\vartheta_{\mathbb{Q},2}^{\mathrm{im,orth}}(x) = O(x^{3/2})$ by Proposition 14, we deduce that

$$\sum_{\substack{\langle\varrho\rangle \text{ im, orth} \\ q(\varrho)\leqslant x}} q(\varrho)^{1+\varepsilon} = O(x^{3/2+\varepsilon}). \tag{45}$$

The second sum in (44) can be handled similarly:

$$\sum_{\substack{\langle\varrho\rangle \text{ ab, sd} \\ q(\varrho)\leqslant x}} q(\varrho)^{-1/2+\varepsilon} = \vartheta_{\mathbb{Q},2}^{\mathrm{ab,sd}}(x)x^{-1/2+\varepsilon} + (1/2-\varepsilon)\int_1^x \frac{\vartheta_{\mathbb{Q},2}^{\mathrm{ab,sd}}(t)}{t^{3/2-\varepsilon}}\,dt.$$

Theorem 2 gives $\vartheta_{\mathbb{Q},2}^{\mathrm{ab,sd}}(x) = O(x\log x)$, so we find that

$$\sum_{\substack{\langle\varrho\rangle \text{ ab, sd} \\ q(\varrho)\leqslant x}} q(\varrho)^{-1/2+\varepsilon} = O(x^{1+2\varepsilon}). \tag{46}$$

Inserting (45) and (46) in (44), we obtain Proposition 16.

7. Schur covers

As before, if G is a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ then we attribute properties of the tautological representation $\iota : G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ to G itself. Thus G is *irreducible* or *self-dual* or *primitive* if these adjectives are applicable to ι. We denote the image of G in $\mathrm{PGL}_n(\mathbb{C})$ by $\mathrm{P}G$, and we write S_n and A_n for the symmetric and alternating groups on n letters. The following result is classical (cf. [37], Section 68).

Proposition 24. *Let G be a finite subgroup of $\mathrm{GL}_2(\mathbb{C})$. If G is irreducible and primitive then $\mathrm{P}G \cong A_4$, S_4, or A_5.*

Note that it is $\mathrm{P}G$ and not G itself which is isomorphic to A_4, S_4, or A_5. In fact A_4, S_4, and A_5 do not have faithful two-dimensional representations over $\mathbb{C}$, so none of them is isomorphic to G. But if G is self-dual then there is an analogous tripartition for G itself (cf. [38], p. 131, Lemma 1). To state it, put $\widetilde{A}_4 = \mathrm{SL}_2(\mathbb{F}_3)$ and $\widetilde{A}_5 = \mathrm{SL}_2(\mathbb{F}_5)$, and let $\widetilde{S}_4$ be the subgroup of $\mathrm{SL}_2(\mathbb{F}_9)$ generated by $\mathrm{SL}_2(\mathbb{F}_3)$ and $i\eta$, where $i \in \mathbb{F}_9$ is a fixed square root of -1 and

$$\eta = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Since η normalizes $\mathrm{SL}_2(\mathbb{F}_3)$ and $(i\eta)^2 = -1$ we have $\widetilde{S}_4 = \mathrm{SL}_2(\mathbb{F}_3) \cup (i\eta)\mathrm{SL}_2(\mathbb{F}_3)$. We denote the center of a group G by $Z(G)$.

Proposition 25. *Let G be a finite subgroup of* $\mathrm{GL}_2(\mathbb{C})$. *If G is irreducible, primitive, and self-dual then $G \cong \widetilde{A}_4$, $\widetilde{S}_4$, or $\widetilde{A}_5$. Furthermore $G \subset \mathrm{SL}_2(\mathbb{C})$ and $Z(G) = \{\pm 1\}$.*

Conversely, these three groups do all have faithful two-dimensional irreducible primitive self-dual representations over $\mathbb{C}$. In fact up to isomorphism $\widetilde{A}_4$ has exactly one such representation, while $\widetilde{S}_4$ and $\widetilde{A}_5$ have exactly two. These facts can all be read from a character table (see for example [15], p. 44 or [16], p. 89 in the case of $\widetilde{A}_4$; [15], p. 43 in the case of $\widetilde{S}_4$; and [16], p. 140 in the case of $\widetilde{A}_5$). On the other hand, to derive Proposition 25 from Proposition 24, we will use the theory of Schur covers, a few elements of which will now be recalled. All of the results about Schur covers to be quoted here can be found in [17], and some of them are also usefully summarized in [15]. Given a group G we denote its commutator subgroup by G', and we say that G is *perfect* if $G = G'$.

Let G and J be finite groups. We say that G is a *representation group* of J if there is a subgroup $C \subset Z(G) \cap G'$ such that $C \cong H^2(J, \mathbb{C}^\times)$ and $G/C \cong J$. The group $H^2(J, \mathbb{C}^\times)$ is the *Schur multiplier* of J, and a representation group of J is also called a *Schur cover* of J. Every finite group has at least one Schur cover, and up to isomorphism it has only finitely many. Furthermore, if the orders of $H^2(J, \mathbb{C}^\times)$ and J/J' are relatively prime – in particular, if J is perfect – then the isomorphism class of a Schur cover of J is unique.

In keeping with tradition we have referred to G itself as a Schur cover of J, but it is also convenient to apply the term to any epimorphism $\varphi : G \to J$ with kernel C. In practice G and φ are largely interchangeable, for if $Z(J)$ is trivial (as it will be in the cases of primary interest to us) then G determines C: In fact $C = Z(G)$, because $Z(G)$ has trivial image in J and is therefore contained in C. Furthermore, the fundamental property of a "representation group" (and the property which explains the terminology itself) is that projective representations of J lift to genuine representations of G, and we claim that the validity of this property is unaffected by the choice of φ. To justify the claim, let us state the property at issue more precisely: If π is a projective representation of J then there exists a representation ρ of G such that $\mathrm{P}\rho \cong \pi \circ \varphi$, where $\mathrm{P}\rho$ denotes the projective representation determined by ρ. Now if $\psi : G \to J$ is another epimorphism with kernel $Z(G)$ then $\psi = \alpha \circ \varphi$ for some automorphism α of J, and as $\pi \circ \alpha$ is a projective representation of J there exists a representation ρ' of G such that $\mathrm{P}\rho' = (\pi \circ \alpha) \circ \varphi$. Then $\mathrm{P}\rho' = \pi \circ \psi$.

While the lifting property will be used in Section 8, our immediate concern is simply to identify the Schur covers of A_4, S_4, and A_5. It is actually more instructive to consider A_n and S_n for arbitrary n. First A_n: It is known that $H^2(A_n, \mathbb{C}^\times)$ is trivial if $n \leqslant 3$, cyclic of order six if $n = 6$ or 7, and cyclic of order two otherwise. Furthermore A_n is perfect for $n \geqslant 5$, while for $n = 4$ we have $|A_4/A_4'| = 3$. It follows that for all $n \geqslant 1$ the groups $H^2(A_n, \mathbb{C}^\times)$ and A_n/A_n' are of relatively prime order, whence a Schur cover of A_n is unique up to isomorphism. If $n \geqslant 4$ and $n \neq 6, 7$ then a Schur cover of A_n is typically denoted $\widetilde{A}_n$ or $\widehat{A}_n$. Granted, if $n = 4$ or 5 then $\widetilde{A}_n$ has already been assigned a meaning, but we will check in a moment that $\mathrm{SL}_2(\mathbb{F}_3)$ and $\mathrm{SL}_2(\mathbb{F}_5)$ are indeed Schur covers of A_4 and A_5.

The situation for S_n is as follows: $H^2(S_n, \mathbb{C}^\times)$ is trivial for $n \leqslant 3$ but cyclic of order two for all $n \geqslant 4$ without exception. Furthermore, if $n \geqslant 4$ and $n \neq 6$ then up to isomorphism there are exactly *two* Schur covers of S_n. In the literature, the two Schur covers are variously denoted $\widetilde{S}_n$ and $\widehat{S}_n$ (cf. [15], p. 23), or S_n^* and S_n^{**} (cf. [17], p. 523), or 2^+S_n and 2^-S_n (cf. [8], p. xxiii), the second member of each pair being characterized by the fact that the preimages of the transpositions of S_n are involutions. (Warning: Although we follow [15] in distinguishing between $\widetilde{S}_n$ and $\widehat{S}_n$, the opposite convention is also in use; see e. g. the characterization of $\widetilde{S}_4$ in [22], p. 199 and of $\widetilde{S}_n$ in [34], p. 97.) If $n \geqslant 4$ and $n \neq 6, 7$ then the respective inverse images of A_n under $\widetilde{S}_n \to S_n$ and $\widehat{S}_n \to S_n$ are Schur covers of A_n and are therefore isomorphic, whence we obtain the notations $\widetilde{A}_n$ and $\widehat{A}_n$ already mentioned.

The next proposition will justify our original definition of $\widetilde{A}_4$, $\widetilde{S}_4$, and $\widetilde{A}_5$ and will show in addition that we may take $\widehat{S}_4 = \mathrm{GL}_2(\mathbb{F}_3)$. By an *involution* in a group we mean as usual an element of order two (which of course is central if unique).

Lemma. *Let G and J be finite groups. Assume:*

(i) *$H^2(J, \mathbb{C}^\times)$ has order two, and J' has even order.*
(ii) *G has a unique involution, and if C is the subgroup generated by the involution then $G/C \cong J$.*

Then G is a Schur cover of J.

Proof. The only point to be checked is that $C \subset G'$. As C is the unique subgroup of order two in G it is contained in every subgroup of even order, and G' is of even order because its quotient J' is. $\square$

Proposition 26. *In each of the following cases, G is a Schur cover of J, and $J \cong G/C$ with $C = Z(G) = \{\pm 1\}$:*

- *$J = A_4$ and $G = \mathrm{SL}_2(\mathbb{F}_3)$.*
- *$J = A_5$ and $G = \mathrm{SL}_2(\mathbb{F}_5)$.*
- *$J = S_4$ and $G = \mathrm{SL}_2(\mathbb{F}_3) \cup (i\eta)\mathrm{SL}_2(\mathbb{F}_3)$.*
- *$J = S_4$ and $G = \mathrm{GL}_2(\mathbb{F}_3)$.*

Furthermore, -1 is the unique involution in G in the first three cases, but every transposition in S_4 lifts to an involution in $\mathrm{GL}_2(\mathbb{F}_3)$.

Proof. Over any field F the scalar matrix -1 is the unique involution in $\mathrm{SL}_2(F)$, and we have identifications $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$ and $A_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$ ($\cong \mathrm{PSL}_2(\mathbb{F}_5)$) by virtue of the transitive action of $\mathrm{PGL}_2(F)$ on the projective line $\mathbf{P}^1(F)$. The first two cases of the proposition now follow from the lemma.

To justify the fourth case we note that the identification $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$ is again a reflection of the action of $\mathrm{PGL}_2(F)$ on $\mathbf{P}^1(F)$. Since the subgroup $C = \{\pm 1\}$ of $\mathrm{GL}_2(\mathbb{F}_3)$ is both central and contained in $\mathrm{GL}_2(\mathbb{F}_3)' = \mathrm{SL}_2(\mathbb{F}_3)$, we conclude directly from the definition that $\mathrm{GL}_2(\mathbb{F}_3)$ is a Schur cover of S_4. Now when we identify $\mathrm{PGL}_2(\mathbb{F}_3)$ with S_4 via its action on $\mathbf{P}^1(F)$, the image of the matrix η in $\mathrm{PGL}_2(\mathbb{F}_3)$ maps to the transposition in S_4 interchanging the points $[1:1]$ and $[-1:1]$ of $\mathbf{P}^1(\mathbb{F}_3)$. Since the transpositions form a conjugacy class of S_4, we deduce that *every* transposition in S_4 lifts to an involution in $\mathrm{GL}_2(\mathbb{F}_3)$.

Finally, in the third case $G \subset \mathrm{SL}_2(\mathbb{F}_9)$, and consequently -1 is the unique involution in G. Hence to conclude from the lemma that G is a Schur cover of S_4 it suffice to see that $G/C \cong S_4$, or equivalently that $G/C \cong \mathrm{PGL}_2(\mathbb{F}_3)$. But $\mathrm{GL}_2(\mathbb{F}_3) = \mathrm{SL}(2, \mathbb{F}_3) \cup \eta\mathrm{SL}_2(\mathbb{F}_3)$, and η and $i\eta$ have the same image in $\mathrm{PGL}_2(\mathbb{F}_9)$. Thus the identity embedding of $\mathrm{PGL}_2(\mathbb{F}_3)$ into $\mathrm{PGL}_2(\mathbb{F}_9)$ is an isomorphism of $\mathrm{PGL}_2(\mathbb{F}_3)$ onto G/C. $\square$

Proof of Proposition 25. By Proposition 24, $\mathrm{P}G$ is A_4, S_4, or A_5. As already noted, none of these groups has a faithful irreducible two-dimensional representation, so G intersects the group of scalar matrices in $\mathrm{GL}_2(\mathbb{C})$ nontrivially. On the other hand, G is self-dual, so the only scalar matrices which can belong to G are ± 1. It follows that $-1 \in G$, that the group $C = \{\pm 1\}$ coincides with $Z(G)$ (by Schur's lemma), and that $G/C \cong \mathrm{P}G$. Now G is symplectic, for otherwise it is orthogonal, and a two-dimensional irreducible orthogonal representation is monomial (because $\mathrm{O}_2(\mathbb{R})$ contains the abelian subgroup $\mathrm{SO}_2(\mathbb{R})$ with index two). Thus $G \subset \mathrm{SL}_2(\mathbb{C})$. As -1 is the only involution in $\mathrm{SL}_2(\mathbb{C})$ and *a fortiori* the only involution in G, the lemma shows that G is a Schur cover of $\mathrm{P}G$. Proposition 25 now follows from Proposition 26 and the fact that a Schur cover of A_4 or A_5 is unique up to isomorphism, as is a Schur cover of S_4 with only one involution. $\square$

8. Primitive representations

As already mentioned, some of the arguments used to bound the quaternionic term in Section 6 will now find application in the primitive case. We take the class $\mathcal{A}$ of Section 6 to be the collection of two-dimensional irreducible self-dual primitive Artin representations of $\mathbb{Q}$. That $\mathcal{A}$ is symplectic and closed under quadratic twists follows from Proposition 25. Hence Proposition 23 gives

$$\vartheta^{\mathrm{ip,sd}}_{\mathbb{Q},2}(x) \ll x^{1/2} \sum_{\substack{[\rho]\in\mathcal{E} \\ q(\rho)\leqslant x}} q(\rho)^{-1/2+\varepsilon}, \tag{47}$$

where $\mathcal{E}$ is the set of projective equivalence classes of $\mathcal{A}$. Although the validity of (47) depends on the choice of a particular representative ρ for the equivalence class $[\rho]$, in the arguments that follow no further use will be made of this choice. Our goal is the following bound:

Proposition 27. *Fix $\gamma < 1/60$. Then $\vartheta^{\mathrm{ip,sd}}_{\mathbb{Q},2}(x) = O(x^{2-\gamma})$, where the implicit constant depends on γ.*

Our strategy for proving Proposition 27 is to replace conductors by discriminants in (47) and then to appeal to the results of Bhargava and of Bhargava, Cojocaru and Thorne. Consider the fixed field L of the kernel of $\mathrm{P}\rho$. By Proposition 24, $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to one of A_4, S_4, and A_5, and we write m for the degree of the permutation group in question: thus $m = 4$ in the first two cases and $m = 5$ in the third. In the following proposition K is any subfield of L with $[K : \mathbb{Q}] = m$. While the choice of K is arbitrary, L is the normal closure of K over $\mathbb{Q}$ for every possible choice.

Proposition 28. *$d_K \leqslant cq(\rho)^{(m-1)/2}$ with an absolute constant $c > 1$.*

Proof. A standard bound for wild ramification (cf. [33], p. 127, Proposition 2) gives

$$d_K \leqslant c \prod_{\substack{p \mid d_K \\ p > m}} p^{m-1}. \tag{48}$$

with $c = 2^{11}3^7$ if $m = 4$ and $c = 2^{14}3^9 5^9$ if $m = 5$. (Thus we may take $c = 2^{14}3^9 5^9$ in all cases.) On the other hand, let M be the fixed field of the kernel of ρ itself. Then Proposition 25 implies that $\mathrm{Gal}(M/\mathbb{Q})$ is $\widetilde{A}_4$, $\widetilde{S}_4$, or $\widetilde{A}_5$ according as $\mathrm{Gal}(L/\mathbb{Q})$ is A_4, S_4, or A_5. Thus if $p > m$ then p does not divide the order of the image of ρ, and consequently the restriction of ρ to an inertia group I at p factors through the tame quotient of I. Hence $\mathrm{ord}_p\, q(\rho)$ is $\dim(V/V^I)$, where V is the space of ρ and V^I the subspace of inertial invariants. Now if $p \mid q(\rho)$ then V/V^I has dimension 1 or 2, but if the dimension is 1 then V is the direct sum of a line on which I acts trivially and a line on which it acts nontrivially, contradicting the fact that $\det \rho = 1$ (Proposition 25 again). Therefore

$$q(\rho) \geqslant \prod_{\substack{p \mid q(\rho) \\ p > m}} p^2, \tag{49}$$

Since L is the normal closure of K, every prime dividing d_K divides $q(\rho)$, whence the proposition follows from (48) and (49). □

Remarks. 1) The inequalities (48) and (49) are both deduced from the fact that one side of the inequality is *divisible* by the other.

2) Using the fact that A_4 has no elements of order > 3, one finds that $d_K \leqslant cq(\rho)$ when $\mathrm{Gal}(L/\mathbb{Q}) \cong A_4$. However this improvement in Proposition 28 does not lead to an improvement in Proposition 27, because the latter combines all three cases.

Proposition 29. *Let L be a finite Galois extension of $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to A_4, S_4, or A_5. Then the number of elements $[\rho] \in \mathcal{E}$ such that L is the fixed field of $\mathrm{Ker}\,(\mathrm{P}\rho)$ is bounded by an absolute constant.*

Proof. Put $J = \mathrm{Gal}(L/\mathbb{Q})$. We may assume that there is a quadratic extension M of L, Galois over $\mathbb{Q}$, such that the group $G = \mathrm{Gal}(M/\mathbb{Q})$ is isomorphic to $\widetilde{A}_4$, $\widetilde{S}_4$, or $\widetilde{A}_5$ according as J is isomorphic to A_4, S_4, or A_5. Indeed if there exists $[\rho] \in \mathcal{E}$ such that L is the fixed field of $\mathrm{Ker}\,(\mathrm{P}\rho)$ then we may take M to be the fixed field of $\mathrm{Ker}\,(\rho)$, and if no such $[\rho]$ exists then there is nothing to prove. Now up to isomorphism, there are exactly three two-dimensional irreducible representations φ of G if $G \cong \widetilde{A}_4$ or $\widetilde{S}_4$ and exactly two if $G \cong \widetilde{A}_5$. (Note that we are not requiring φ to be faithful or self-dual or primitive.) Let us declare φ and φ' to be equivalent if $\varphi' \cong \varphi \otimes \chi$ for some one-dimensional character χ of G. Then there is exactly one equivalence class if $G \cong \widetilde{A}_4$ and there are exactly two if $G \cong \widetilde{S}_4$ or $\widetilde{A}_5$. So the proposition will follow (with the absolute constant equal to 2) if we define an injective map $[\rho] \mapsto [\varphi]$ from the set of $[\rho] \in \mathcal{E}$ such that L is the fixed field of $\mathrm{Ker}\,(\mathrm{P}\rho)$ to the set of equivalence clases $[\varphi]$ as above.

Given $[\rho]$, view $P\rho$ as a projective representation of J. Since G is a Schur cover of J we can lift $P\rho$ to a genuine representation φ of G. It is immediately verified that the equivalence class $[\varphi]$ of φ is uniquely determined by $[\rho]$ and that the map $[\rho] \mapsto [\varphi]$ is injective. $\square$

Reviewing the preceding paragraphs, we see that we have defined a function $[\rho] \mapsto K$: Given $[\rho] \in \mathcal{E}$, we let L be the fixed field of Ker $(\mathrm{P}\rho)$ and then we choose a subfield $K \subset L$ with $[K : \mathbb{Q}] = m$. Since L is determined by K (indeed L is the normal closure of K) Proposition 29 shows that the number of preimages $[\rho]$ of K is bounded by an absolute constant. Thus Proposition 28 gives

$$\sum_{\substack{[\rho]\in\mathcal{E}\\ q(\rho)\leqslant x}} q(\rho)^{-1/2+\varepsilon} \ll \sum_{\substack{[K:\mathbb{Q}]=4\\ d_K\leqslant cx^{3/2}}} d_K^{-1/3+\varepsilon/3} + \sum_{\substack{[K:\mathbb{Q}]=5\\ \mathrm{Gal}(L/\mathbb{Q})\cong A_5\\ d_K\leqslant cx^2}} d_K^{-1/4+\varepsilon/2} \tag{50}$$

for $0 < \varepsilon < 1/2$, where the first sum on the right-hand side runs over number fields K with $[K : \mathbb{Q}] = 4$ and $d_K \leqslant cx^{3/2}$, and the second sum runs over K with $[K : \mathbb{Q}] = 5$, $d_K \leqslant cx^2$, and $\mathrm{Gal}(L/\mathbb{Q}) \cong A_5$, L being the normal closure of K. Of course the first sum could be confined to K such that $\mathrm{Gal}(L/\mathbb{Q}) \cong A_4$ or $\mathrm{Gal}(L/\mathbb{Q}) \cong S_4$, but (50) will suffice as it stands.

We now apply Abel summation to the first sum on the right-hand side of (50):

$$\sum_{\substack{[K:\mathbb{Q}]=4\\ d_K\leqslant cx^{3/2}}} d_K^{-1/3+\varepsilon/3} = \eta_{\mathbb{Q},4}(cx^{3/2})(cx^{3/2})^{-1/3+\varepsilon/3} + (1/3-\varepsilon/3)\int_1^{cx^{3/2}} \frac{\eta_{\mathbb{Q},4}(t)}{t^{4/3-\varepsilon/3}}\,dt.$$

Since $\eta_{\mathbb{Q},4}(x) = O(x)$ by [3], we deduce that

$$\sum_{\substack{[K:\mathbb{Q}]=4\\ d_K\leqslant cx^{3/2}}} d_K^{-1/3+\varepsilon/3} = O(x^{1+\varepsilon}). \tag{51}$$

The second sum on the right-hand side of (50) can be treated in the same way:

$$\sum_{\substack{[K:\mathbb{Q}]=5\\ \mathrm{Gal}(L/\mathbb{Q})\cong A_5\\ d_K\leqslant cx^2}} d_K^{-1/4+\varepsilon/2} = \eta_{\mathbb{Q},5}^{A_5}(cx^2)(cx^2)^{-1/4+\varepsilon/2} + (1/4-\varepsilon/2)\int_1^{cx^2} \frac{\eta_{\mathbb{Q},5}^{A_5}(t)}{t^{5/4-\varepsilon/2}}\,dt.$$

By [5] we have $\eta_{\mathbb{Q},5}^{A_5}(x) = O(x^{1-\beta})$ for any $\beta < 1/120$, so we obtain

$$\sum_{\substack{[K:\mathbb{Q}]=5\\ \mathrm{Gal}(L/\mathbb{Q})\cong A_5\\ d_K\leqslant cx^2}} d_K^{-1/4+\varepsilon/2} \ll O(x^{3/2-2\beta+\varepsilon}). \tag{52}$$

Inserting (51) and (52) in (50) and then concatenating the result with (47), we obtain Proposition 27.

9. Monomial representations revisited

Assembling our estimates for the three terms on the right-hand side of (1), we see that Theorem 2, Proposition 17, and Proposition 27 together imply the upper bound for $\vartheta^{\mathrm{sd}}_{\mathbb{Q},2}(x)$ claimed in (3). On the other hand, Theorem 1 gives the lower bound for $\vartheta^{\mathrm{ab}}_{\mathbb{Q},2}(x)$ in (4), so we conclude that indeed $\lim_{x\to\infty} \vartheta^{\mathrm{sd}}(x)/\vartheta(x) = 0$ for

$F = \mathbb{Q}$ and $n = 2$, as asserted in the introduction. We will now show that the limit of $\vartheta^{\mathrm{sd}}(x)/\vartheta^{\mathrm{irr}}(x)$ and *a fortiori* of $\vartheta^{\mathrm{irr,sd}}(x)/\vartheta^{\mathrm{irr}}(x)$ is 0 also. Since $\vartheta^{\mathrm{irr}}(x) \geqslant \vartheta^{\mathrm{im}}(x)$ it will suffice to show that

$$\vartheta^{\mathrm{im}}_{\mathbb{Q},2}(x) \gg x^2. \tag{53}$$

I do not know how to replace (53) by an asymptotic equality.

To prove (53), fix an imaginary quadratic field K, and let $\vartheta^{K}_{\mathbb{Q},2}(x)$ be the number of isomorphism classes of two-dimensional monomial Artin representations of $\mathbb{Q}$ which are induced from K and of absolute conductor $\leqslant x$. Write $\vartheta^{\mathrm{im},K}_{\mathbb{Q},2}(x)$ and $\vartheta^{\mathrm{ab},K}_{\mathbb{Q},2}(x)$ for the number of such classes of irreducible representations and abelian representations respectively. Then

$$\vartheta^{\mathrm{im},K}_{\mathbb{Q},2}(x) = \vartheta^{K}_{\mathbb{Q},2}(x) - \vartheta^{\mathrm{ab},K}_{\mathbb{Q},2}(x). \tag{54}$$

We shall prove that

$$\vartheta^{\mathrm{ab},K}_{\mathbb{Q},2}(x) \sim 18x/(d_K\pi^4) \tag{55}$$

and that

$$\vartheta^{K}_{\mathbb{Q},2}(x) \sim cx^2 \tag{56}$$

with a constant $c > 0$ depending on K, whence also $\vartheta^{\mathrm{im},K}_{\mathbb{Q},2}(x) \sim cx^2$ by (54). Since $\vartheta^{\mathrm{im}}_{\mathbb{Q},2}(x) \geqslant \vartheta^{\mathrm{im},K}_{\mathbb{Q},2}(x)$ the lower bound (53) will then follow. In principle we would get a better result in (53) if instead of fixing K we were to sum (56) over all K, taking account of any duplications. However even after summing over K we would not be able to replace (53) by an asymptotic formula, because we do not have the analogue of (56) for real quadratic fields.

To prove (55), we observe that the two-dimensional abelian Artin representations of $\mathbb{Q}$ induced from K are precisely the representations $\rho \cong \chi \oplus \chi \cdot \mathrm{sign}_{K/\mathbb{Q}}$, where χ is an arbitrary one-dimensional character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\mathrm{sign}_{K/\mathbb{Q}}$ is the character with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. As $q(\rho) = q(\chi)^2 d_K$ we have

$$\vartheta^{\mathrm{ab},K}_{Q,2}(x) = \sum_{q(\chi)^2 \leqslant x/d_K} 1,$$

where the sum runs over all χ satisfying the stated inequality. Recognizing this sum as $\vartheta_{\mathbb{Q},1}(\sqrt{x/d_K})$, we obtain (55) from the corollary to Proposition 2.

It remains to prove (56). The Artin representations of $\mathbb{Q}$ counted by $\vartheta^{K}_{\mathbb{Q},2}(x)$ are precisely the representations of the form $\rho \cong \mathrm{ind}_{K/\mathbb{Q}}\xi$, where ξ runs over one-dimensional characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ such that $d_K q(\xi) \leqslant x$. Furthermore the map sending the isomorphism class of ρ to ξ is two-to-one, for it follows from Frobenius reciprocity that if G is a finite group, H a subgroup of index two, and ξ a one-dimensional character of H, then there is exactly one character ξ' of H such that $\xi' \neq \xi$ and $\mathrm{ind}^G_H\xi' \cong \mathrm{ind}^G_H\xi$. Therefore

$$\vartheta^{K}_{\mathbb{Q},2}(x) = (1/2)\vartheta_{K,1}(x/d_K). \tag{57}$$

Now put

$$c = (\pi/(2d_K^{5/2})) \cdot (h_K/(w_K\zeta_K(2)))^2, \tag{58}$$

where $\zeta_K(s)$, h_K, and w_K are as usual the Dedekind zeta function, class number, and number of roots of unity in K. We obtain (56) with c as in (58) by combining (57) with the following assertion:

Theorem 4. $\vartheta_{K,1}(x) \sim (\pi/\sqrt{d_K})(h_K x/(w_K\zeta_K(2)))^2$.

Proof. Given a nonzero integral ideal $\mathfrak{q}$ of K, put $\varphi_K(\mathfrak{q}) = |(\mathcal{O}_K/\mathfrak{q})^\times|$ as before, and set $\mu_K(\mathfrak{q}) = (-1)^t$ if $\mathfrak{q}$ is the product of exactly t distinct prime ideals of K and $\mu_K(\mathfrak{q}) = 0$ otherwise. Also write $h_K^*(\mathfrak{q})$ for the number of primitive ray class characters of K of conductor $\mathfrak{q}$, so that

$$\vartheta_{K,1}(x) = \sum_{\mathbf{N}\mathfrak{q}\leqslant x} h_K^*(\mathfrak{q}) \tag{59}$$

and

$$h_K^*(\mathfrak{q}) = \sum_{\mathfrak{q}'|\mathfrak{q}} \mu_K(\mathfrak{q}/\mathfrak{q}')h_K(\mathfrak{q}'). \tag{60}$$

Let $w_K(\mathfrak{q})$ the number of roots of unity in K which are congruent to 1 modulo $\mathfrak{q}$. Since K has no real embeddings, the narrow ray class number $h_K^{\mathrm{nar}}(\mathfrak{q})$ is indistinguishable from the wide ray class number $h_K(\mathfrak{q})$, and consequently

$$h_K(\mathfrak{q}) = h_K \cdot \varphi_K(\mathfrak{q}) \cdot (w_K(\mathfrak{q})/w_K) \tag{61}$$

by (14). Combining (60) and (61), we have

$$h_K^*(\mathfrak{q}) = (h_K/w_K)\sum_{\mathfrak{q}'|\mathfrak{q}} \mu_K(\mathfrak{q}/\mathfrak{q}')\varphi_K(\mathfrak{q}')w_K(\mathfrak{q}'). \tag{62}$$

Put $\psi_K(\mathfrak{q}) = \sum_{\mathfrak{q}'|\mathfrak{q}} \mu_K(\mathfrak{q}/\mathfrak{q}')\varphi_K(\mathfrak{q}')$. It is convenient to rewrite (62) in the form

$$h_K^*(\mathfrak{q}) = (h_K/w_K)\psi_K(\mathfrak{q}) + O(1) \tag{63}$$

with $O(1) = (h_K/w_K)\sum_{\mathfrak{q}'|\mathfrak{q}} \mu_K(\mathfrak{q}/\mathfrak{q}')\varphi_K(\mathfrak{q}')(w_K(\mathfrak{q}') - 1)$.

The expression which we have denoted $O(1)$ is indeed bounded by a constant depending only on K, because $w_K(\mathfrak{q}') = 1$ unless $\mathfrak{q}'|6\mathcal{O}_K$. Hence by substituting (63) in (59) we obtain

$$\vartheta_{K,1}(x) = (h_K/w_K)\sum_{\mathbf{N}\mathfrak{q}\leqslant x} \psi_K(\mathfrak{q}) + O(\sum_{\mathbf{N}\mathfrak{q}\leqslant x} 1). \tag{64}$$

Denote the first and second sums on the right-hand side of (64) by Σ_1 and Σ_2:

$$\vartheta_{K,1}(x) = (h_K/w_K)\Sigma_1 + O(\Sigma_2). \tag{65}$$

Then Σ_2 is the summatory function of $\zeta_K(s)$, and consequently Proposition 1 gives $\Sigma_1 \sim \lambda_K x$, where λ_K is the residue of $\zeta_K(s)$ at $s = 1$. In particular, $\Sigma_1 = O(x)$. On the other hand, if we redo the proof of Proposition 2 with φ and ψ replaced by φ_K and ψ_K and with the rational prime p replaced by a prime ideal $\mathfrak{p}$ of K or by $\mathbf{N}\mathfrak{p}$, as appropriate, then we find that Σ_1 is the summatory function of $\zeta_K(s-1)/\zeta_K(s)^2$. Hence another appeal to Proposition 1 gives

$$\Sigma_1 \sim \lambda_K/(2\zeta_K(2)^2) \cdot x^2. \tag{66}$$

Since $\Sigma_2 = O(x)$, it follows from (64) and (66) that

$$\vartheta_{K,1}(x) \sim \lambda_K h_k x^2/(2w_K\zeta_K(2)^2).$$

Substituting $\lambda_K = (2\pi)h_K/(w_K\sqrt{d_K})$, we obtain the stated asymptotic formula. □

10. Malle's conjecture

Only a weak form of Malle's conjecture will be needed here, but for the sake of completeness we first state the conjecture in its original form: Given a number field F, an integer $m \geqslant 2$, and a transitive subgroup G of S_m, there are constants a, b, and c satisfying $0 < a \leqslant 1$, $b \geqslant 1$, and $c > 0$ such that

$$\eta^G_{F,m} \sim cx^a(\log x)^{b-1}. \tag{67}$$

What distinguishes Malle's conjecture from previous hypotheses of this type (cf. Cohen [6]) is that explicit values are proposed for a and b, as we now describe.

The value of a depends only on G, not on F; Malle denotes it $a(G)$. To define $a(G)$ we recall that the *index* of an element $g \in G$ is the quantity

$$\mathrm{ind}(g) = m - \mathrm{cyc}(g),$$

where $\mathrm{cyc}(g)$ is the number of cycles in the exhaustive disjoint cycle decomposition of g. Here "exhaustive" means that cycles of length 1 are included; for example if $g = 1$ then we write $g = (1)(2)\cdots(m)$ and find that $\mathrm{cyc}(g) = m$ and $\mathrm{ind}(g) = 0$, while if $g \neq 1$ then $\mathrm{ind}(g) > 0$. We put

$$\mathrm{ind}(G) = \min_{\substack{g \in G\\ g \neq 1}} \mathrm{ind}(g)$$

and $a(G) = \mathrm{ind}(G)^{-1}$.

The quantity b depends on F as well as G. The function $g \mapsto \mathrm{ind}(g)$ is constant on conjugacy classes of G, so we can speak of the index of a conjugacy class, and we let $\mathcal{C}$ be the set consisting of all conjugacy classes C such that $\mathrm{ind}(C) = \mathrm{ind}(G)$. We define an action of $\mathrm{Gal}(\overline{F}/F)$ on $\mathcal{C}$ by setting $\sigma \cdot C = C^{\omega(\sigma)}$ for $\sigma \in \mathrm{Gal}(\overline{F}/F)$ and $C \in \mathcal{C}$, where $\omega : \mathrm{Gal}(\overline{F}/F) \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character ($\widehat{\mathbb{Z}}$ being the ring of adelic integers) and $C^{\omega(\sigma)}$ is the conjugacy class consisting of the elements $g^{\omega(\sigma)}$ with $g \in C$. If one prefers one can take ω to be the mod-e cyclotomic character $\mathrm{Gal}(\overline{F}/F) \to \mathbb{Z}/e\mathbb{Z}^\times$ for any positive integer e divisible by the order of every element of G. In any case, b is the number of orbits of $\mathrm{Gal}(\overline{F}/F)$ on $\mathcal{C}$.

A counterexample of Klüners [21] shows that with these definitions Malle's original conjecture (67) is false: If $F = \mathbb{Q}$, $n = 6$, and

$$G = ((\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

(embedded in S_6 by identifying the first factor of $\mathbb{Z}/3\mathbb{Z}$ with $\langle(123)\rangle$, the second with $\langle(456)\rangle$, and $\mathbb{Z}/2\mathbb{Z}$ with $\langle(14)(25)(36)\rangle$) then $a = 1/2$ and $b = 1$, but Klüners shows that the left-hand side of (67) is $\gg x^{1/2}\log x$. However if we state Malle's conjecture in the weaker form

$$\eta^G_{F,m}(x) \ll x^{a(G)+\varepsilon} \tag{68}$$

for all $\varepsilon > 0$, where the implicit constant depends on F, G, and ε, then the conjecture has so far proved unassailable, and henceforth it is (68) to which reference will be made. We shall call (68) *the weak form of Malle's conjecture.*

At this juncture we change perspective slightly by viewing G as an *abstract* group of order $m \geqslant 2$. If we wish to regard G as a permutation group then we do so via the regular representation, so that the associated embedding $G \hookrightarrow S_m$ is uniquely determined up to conjugacy in S_m. Now fix an integer $n \geqslant 2$ and let $\vartheta^G_{F,n}(x)$ be the number of isomorphism classes of n-dimensional irreducible Artin representations ρ

of F with image isomorphic to G and $q(\rho) \leqslant x$. We would like to compare $\vartheta_{F,n}^{G}(x)$ with $\eta_{F,m}^{G}(x)$. In Section 11 we will prove the inequality

$$d_{L/F} \leqslant q(\rho)^{|G|-n(n-1)}, \tag{69}$$

where L is the fixed field of the kernel of ρ and ρ is as before an n-dimensional irreducible Artin representation of F with image isomorphic to G. Granting (69), and making the trivial remark that if $q(\rho) \leqslant x$ then $q(\rho)^{|G|-n(n-1)} \leqslant x^{|G|-n(n-1)}$, we see that

$$\vartheta_{F,n}^{G}(x) \leqslant \mathrm{i}_n(G) \cdot \eta_{F,m}^{G}(x^{|G|-n(n-1)}), \tag{70}$$

where $\mathrm{i}_n(G)$ is the number of isomorphism classes of faithful n-dimensional irreducible complex representations of G.

Proposition 30. *Let p be the smallest prime divisor of $|G|$, and fix*

$$\gamma < pn(n-1)/((p-1)|G|).$$

If the weak form of Malle's conjecture holds then

$$\vartheta_{F,n}^{G}(x) \ll x^{p/(p-1)\,-\,\gamma},$$

where the implied constant depends on F, G, n, and γ.

Proof. Since G is a permutation group via the regular representation, we have $\mathrm{cyc}(g) = |G|/|g|$ for $g \in G$, where $|g|$ is the order of g. Thus $\mathrm{ind}(G) = |G| - |G|/p$ and $a(G) = p/((p-1)|G|)$. Inserting this value in (68) and then combining (68) with (70) gives the stated estimate. □

Next we recall a theorem of Jordan: If G is a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ then G has an abelian normal subgroup of index bounded by a constant depending only on n. We denote the optimal choice of this constant $j(n)$. The value $j(2) = 60$ is classical, and the value of $j(n)$ for arbitrary n was determined by Collins [7]. For example if $n \geqslant 71$ then $j(n) = (n+1)!$.

Proposition 31. *Let G be a finite irreducible self-dual subgroup of* $\mathrm{GL}_n(\mathbb{C})$*. If G is primitive then $|G| \leqslant 2j(n)$.*

Proof. Let $\iota : G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ be the tautological representation and A an abelian normal subgroup of G of index $\leqslant j(n)$. Then $\iota|A$ is a direct sum of one-dimensional characters of A. Let χ be a one-dimensional character of A occurring in $\iota|A$. If the multiplicity of χ in $\iota|A$ is $< n$ then the subgroup of G stabilizing χ is a proper subgroup from which ι is induced, contradicting the primitivity of ι. Hence $\iota|A = \chi^{\oplus n}$, and therefore

$$|G| = [G:A]|\mathrm{Ker}\ \chi|.$$

But ι is self-dual, hence so is $\iota|A$. Thus $\chi^2 = 1$ and consequently $|\mathrm{Ker}\ \chi| \leqslant 2$. □

Finally we deduce a conditional bound on $\vartheta_{F,n}^{\mathrm{ip,sd}}(x)$:

Proposition 32. *Fix $\gamma < n(n-1)/j(n)$. If the weak form of Malle's conjecture holds then*

$$\vartheta_{F,n}^{\mathrm{ip,sd}}(x) \ll x^{2-\gamma},$$

where the implied constant depends on F, n, and γ.

Proof. The only irreducible self-dual representation of a group of odd order is the one-dimensional trivial representation. Hence it follows from Proposition 31 that

$$\vartheta^{\mathrm{ip,sd}}_{F,n}(x) \leqslant \sum_{\substack{|G|\leqslant 2j(n)\\ |G| \text{ even}}} \vartheta^{G}_{F,n}(x), \tag{71}$$

where the sum on the right-hand side runs over a set of representatives for the distinct isomorphism classes of groups of even order $\leqslant 2j(n)$. Taking $p = 2$ in Proposition 30, we obtain the stated estimate. □

11. Lower bounds for the conductor

We must still prove (69), the inequality between conductors and discriminants. Fix a number field F and a finite Galois extension L of F, and put $G = \mathrm{Gal}(L/F)$.

Lemma. *Let ρ and λ be finite-dimensional complex representations of G, with ρ faithful. Then $\mathfrak{q}(\lambda)$ divides $\mathfrak{q}(\rho)^{\dim(\lambda)}$.*

Proof. Fix a prime ideal $\mathfrak{p}$ of F, and let $a(\rho)$ and $a(\lambda)$ be the exponent of $\mathfrak{p}$ in $\mathfrak{q}(\rho)$ and $\mathfrak{q}(\lambda)$ respetively. It suffices to see that

$$a(\lambda) \leqslant \dim(\lambda)a(\rho). \tag{72}$$

Let $I \subset G$ be the inertia subgroup of some fixed prime ideal of L above $\mathfrak{p}$. If $I = \{1\}$ then both sides of (72) are 0 and there is nothing to prove. Hence we may assume that $I \neq \{1\}$.

Let $G_0 = I \supseteq G_1 \supseteq G_2 \supseteq \ldots$ be the higher ramification subgroups of I in the lower numbering (cf. [32], p. 62). Since I is nontrivial there exists an integer $n \geqslant 1$ such that $G_i \neq \{1\}$ for $0 \leqslant i \leqslant n$ and $G_i = \{1\}$ for $i \geqslant n+1$. Writing V for the space of ρ and V^{G_i} for the subspace of vectors fixed by G_i, we have

$$a(\rho) = \sum_{i=0}^{n} \frac{|G_i|}{|G_0|}\dim(V/V^{G_i}) \tag{73}$$

(cf. [32], p. 100). Similarly,

$$a(\lambda) = \sum_{i=0}^{n} \frac{|G_i|}{|G_0|}\dim(W/W^{G_i}), \tag{74}$$

where W is the space of λ. Now as ρ is faithful we have $V^{G_i} \neq V$ for $1 \leqslant i \leqslant n$ and hence $\dim(V/V^{G_i}) \geqslant 1$. Thus

$$\dim(W/W^{G_i}) \leqslant \dim(W) = \dim(\lambda) \leqslant \dim(\lambda)\dim(V/V^{G_i}).$$

Substituting this inequality in (74) and comparing the result with (73), we obtain (72). □

The inequality (69) is an immediate consequence of the following proposition:

Proposition 33. *Let ρ be a faithful irreducible complex representation of G. Then $\mathfrak{d}_{L/F}$ divides $\mathfrak{q}(\rho)^{|G|-(n^2-n)}$, where $n = \dim(\rho)$.*

Proof. We apply the lemma to a set of representatives λ for the distinct isomorphism classes of irreducible representations of G. Raising both ideals in the divisibility of the lemma to the power $\dim\lambda$ and then taking the product over $\lambda \not\cong \rho$, we see that

$$\prod_{\lambda\not\cong\rho} \mathfrak{q}(\lambda)^{\dim\lambda} \ \text{ divides } \ q(\rho)^{\sum_{\lambda\not\cong\rho}(\dim\lambda)^2}. \tag{75}$$

Let reg_G denote the regular representation of G, and multiply the divisor and dividend in (75) by the same ideal $\mathfrak{q}(\rho)^n$. Since $\mathrm{reg}_G \cong \oplus_\lambda \lambda^{\oplus\dim\lambda}$, we obtain

$$\mathfrak{q}(\mathrm{reg}_G) \ \text{ divides } \ \mathfrak{q}(\rho)^{(\sum_\lambda(\dim\lambda)^2)-n^2+n}.$$

Now $\mathfrak{q}(\mathrm{reg}_G) = \mathfrak{d}_{L/F}$ by Artin's conductor-discriminant formula (cf. [32], p. 104). Since $|G| = \sum_\lambda(\dim\lambda)^2$, the proposition follows. □

12. A conditional result in dimension three

To evaluate $\lim_{x\to\infty}\vartheta^{\mathrm{sd}}(x)/\vartheta(x)$ conditionally when $F=\mathbb{Q}$ and $n=3$, we must bound each of the three terms on the right-hand side of (2). The first term is easily dealt with:

$$\vartheta^{\mathrm{ab,sd}}_{\mathbb{Q},3}(x) = O(x(\log x)^2). \tag{76}$$

by Theorem 2.

To bound $\vartheta^{1+2,\mathrm{sd}}_{\mathbb{Q},3}(x)$, we observe that if a self-dual representation is a direct sum of a one-dimensional and an irreducible two-dimensional representation then the one-dimensional and two-dimensional representations are self-dual. Thus

$$\vartheta^{1+2,\mathrm{sd}}_{\mathbb{Q},3}(x) = \sum_{q\leqslant x}\psi^{\mathrm{sd}}(q)\vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},2}(x/q), \tag{77}$$

where $\psi^{\mathrm{sd}}(q)$ is the number of primitive Dirichlet characters χ of conductor q satisfying $\chi^2=1$, as in Section 2. But (3) gives

$$\vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},2}(x/q) \leqslant \vartheta^{\mathrm{sd}}_{\mathbb{Q},2}(x/q) \ll (x/q)^{2-\varepsilon}$$

for any $\varepsilon < 1/60$, so (77) becomes

$$\vartheta^{1+2,\mathrm{sd}}_{\mathbb{Q},3}(x) \ll x^{2-\varepsilon}\sum_{q\leqslant x}\frac{\psi^{\mathrm{sd}}(q)}{q^{2-\varepsilon}}. \tag{78}$$

Now apply Abel summation:

$$\sum_{q\leqslant x}\frac{\psi^{\mathrm{sd}}(q)}{q^{2-\varepsilon}} = \frac{\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(x)}{x^{2-\varepsilon}} + (2-\varepsilon)\int_1^x \frac{\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(t)}{t^{3-\varepsilon}}\,dt. \tag{79}$$

Since $\vartheta^{\mathrm{sd}}_{\mathbb{Q},1}(t) \ll t$ by the corollary to Proposition 3, we see that the right-hand side of (79) is bounded by a constant, whence

$$\vartheta^{1+2,\mathrm{sd}}_{\mathbb{Q},3}(x) \ll x^{2-\varepsilon} \tag{80}$$

after substitution in (78).

It remains to bound $\vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},3}(x)$. We will use a variant of Proposition 31:

Proposition 34. *Let G be a finite irreducible self-dual subgroup of $\mathrm{GL}_n(\mathbb{C})$. If n is odd then $|G| \leqslant 2^n j(n)$.*

Proof. The proof is similar to the proof of Proposition 31. If A is an abelian normal subgroup of G of index $\leqslant j(n)$ and $\iota : G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ is the tautological representation then $\iota|A$ is a direct sum of one-dimensional characters of A, and it follows from the self-duality of $\iota|A$ that the multiplicity of any character χ occurring in $\iota|A$ equals the multiplicity of χ^{-1}. Furthermore, since A is normal in G and ι is irreducible, all of the one-dimensional characters χ of A occurring in $\iota|A$ are conjugate under the action of G and thus have the same order w. If $w \geqslant 3$ then $\chi \neq \chi^{-1}$, whence $\iota|A$ is a direct sum of two-dimensional representations of the form $\chi \oplus \chi^{-1}$, contradicting the assumption that n is odd. Thus $w = 2$. Since A is abelian we may assume after a conjugation in $\mathrm{GL}_n(\mathbb{C})$ that A is contained in the group of diagonal matrices, hence in the group of diagonal matrices of order $\leqslant 2$. Thus $|A| \leqslant 2^n$ and $|G| = [G : A]|A| \leqslant j(n)2^n$. $\square$

We apply the proposition with $n = 3$. Using the value $j(3) = 360$ [7], and recalling once again that a group of odd order does not have nontrivial irreducible self-dual representations, we see that

$$\vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},3}(x) \leqslant \sum_{\substack{|G|\leqslant 2880\\ |G| \text{ even}}} \vartheta^{G}_{\mathbb{Q},3}(x), \tag{81}$$

where the sum on the right-hand side runs over a set of representatives for the distinct isomorphism classes of groups of even order $\leqslant 2880$. Applying Proposition 30 with $p = 2$, we obtain:

Proposition 35. *Fix $\gamma < 1/240$. If the weak form of Malle's conjecture holds then*

$$\vartheta^{\mathrm{irr,sd}}_{\mathbb{Q},3}(x) \ll x^{2-\gamma},$$

where the implied constant depends on γ.

Using the proposition together with (76) and (80) on the right-hand side of (2), we obtain the conditional bound $\vartheta^{\mathrm{sd}}_{\mathbb{Q},3}(x) = O(x^{2-\gamma})$ for every $\gamma < 1/240$. Since $\vartheta^{\mathrm{ab}}_{\mathbb{Q},3}(x) \gg (x \log x)^2$ by Theorem 1, we conclude under Malle's conjecture that $\lim_{x\to\infty} \vartheta^{\mathrm{sd}}(x)/\vartheta(x) = 0$ for $F = \mathbb{Q}$ and $n = 3$.

13. Appendix: Proof of Propositions 10, 11, and 12

We shall prove the propositions in reverse order.

Proof of Proposition 12. (a) The irreducibility of ρ follows from Mackey's criterion, because the assumption that χ has order $\geqslant 3$ means that $\chi \neq \chi^{-1}$ and hence that $\chi \neq \chi^g$ for $g \in G \smallsetminus H$. The self-duality of ρ follows from the calculation

$$\rho^\vee = (\mathrm{ind}_H^G \chi)^\vee \cong \mathrm{ind}_H^G \chi^{-1} \cong \mathrm{ind}_H^G \chi^g \cong \rho.$$

Finally, induction preserves faithfulness.

(b) A straightforward calculation shows that if $g \in G \smallsetminus H$ and $h \in H$ then $\mathrm{tran}_H^G(h) = hghg^{-1}$. Consequently $\chi \circ \mathrm{tran}_H^G|H = \chi\chi^g$, whence $\chi^g = \chi^{-1}$ if and only if $\chi \circ \mathrm{tran}_H^G|H = 1$. Since sign_H^G and 1 are precisely the characters of G trivial on H we obtain the first half of (b). Now an irreducible self-dual representation is either orthogonal or symplectic, and we have just observed that if $\chi^g = \chi^{-1}$ then $\chi \circ \mathrm{tran}_H^G$ is either 1 or sign_H^G. Thus to prove the second half of (b) it suffices to see that $\chi \circ \mathrm{tran}_H^G = \mathrm{sign}_H^G$ if and only if ρ is symplectic, or equivalently (since $\mathrm{Sp}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})$) if and only if $\det \rho = 1$. We now appeal to the formula for the determinant of an induced representation (cf. [13] or [10], p. 508, Proposition 1.2), which takes the form $\det\rho = (\mathrm{sign}_H^G)(\chi \circ \mathrm{tran}_H^G)$ in the case at hand. □

Proof of Proposition 11. Since ρ is monomial, there exists a subgroup H of index two in G and a one-dimensional character χ of H such that ρ is induced by χ. Since ρ is irreducible, $\chi \neq \chi^g$ for $g \in G \smallsetminus H$, and $\rho|H = \chi \oplus \chi^g$. Thus by Frobenius reciprocity χ and χ^g are precisely the two characters of H inducing ρ. But ρ is self-dual, so χ^{-1} also induces ρ. Hence either $\chi^{-1} = \chi^g$ and χ is of order $\geqslant 3$ or else $\chi^{-1} = \chi$ and χ is quadratic. In the latter case ρ is realizable over $\mathbb{R}$, hence orthogonal. Viewing G as a subgroup of $\mathrm{O}_2(\mathbb{R})$, we can replace H by $\mathrm{SO}_2(\mathbb{R}) \cap G$ to get a *cyclic* subgroup of index two in G. On the other hand, if $\chi^{-1} = \chi^g$ then $\rho|H \cong \chi \oplus \chi^{-1}$. Since ρ is faithful, so is χ, whence H is cyclic.

Thus G has a cyclic subgroup of index two. If H is any such subgroup then $\rho|H \cong \chi \oplus \chi'$ with one-dimensional characters χ and χ' of H, and $\chi \neq \chi'$ because ρ is irreducible (if H is central then G is abelian). The irreducibility also gives $\chi' = \chi^g$ for $g \in G \smallsetminus H$, whence $\rho \cong \mathrm{ind}_H^G \chi$. We are now in the situation of the previous paragraph, but this time H is cyclic and so has at most one quadratic character. Thus if χ is quadratic then χ^g, which is consequently also quadratic, coincides with χ, a contradiction. Hence χ has order $\geqslant 3$ and χ^{-1}, which induces ρ and thus coincides with one of χ and χ^g, coincides with χ^g. □

Proof of Proposition 10. Applying Proposition 11 to the tautological representation $\iota : G \to \mathrm{GL}_2(\mathbb{C})$, we see that $\iota = \mathrm{ind}_H^G \chi$ for some cyclic subgroup H of index two in G and some character χ of H as in the proposition. Let a be a generator of H and choose $b \in G \smallsetminus H$. Then $\chi^b = \chi^{-1}$, and since χ is faithful we get $bab^{-1} = a^{-1}$. Also $b^2 \in H$ as $[G : H] = 2$. If $b^2 = 1$ then $G \cong D_{2m}$ with $m \geqslant 3$. Otherwise b^2 is a nontrivial element of the center of G, whence b^2 $(= \iota(b^2))$ is a scalar $\neq 1$ (Schur's lemma). Since ι is self-dual we get $b^2 = -1$. But $b^2 \in H$, so H has even order. Write $|H| = 2m$; then $a^m = b^2$ and $G \cong H_{4m}$.

The second assertion of the proposition follows from Proposition 12, because $\mathrm{tran}_H^G(b) = 1$ or -1 according as $G \cong D_{2m}$ or H_{4m}.

□

14. Appendix: Proof of Theorem 3

As we have already remarked, it suffices to prove (12). View $1 + \eta_{F,2}(x)$ as the summatory function associated to the Dirichlet series

$$\mathcal{D}(s) = \sum_{K \in \mathcal{K}} d_{K/F}^{-s}, \tag{82}$$

where $\mathcal{K}$ is the set of extensions K of F inside $\overline{F}$ with $[K : F] \leqslant 2$. We will show that this series converges for $\Re(s) > 1$, that it extends to a meromorphic function in the region $\Re(s) > 1/2$, and that it is holomorphic in the latter region except for a simple pole at $s = 1$. The theorem will then follow from Proposition 1.

We begin by establishing a partition of $\mathcal{K}$ of the form

$$\mathcal{K} = \bigcup_{\mathfrak{b} \in \mathfrak{B}} \bigcup_{c \in C} \bigcup_{r \in R(\mathfrak{b})} \bigcup_{\mathfrak{a} \in \mathfrak{A}(\mathfrak{b}, c, r)} \mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r} \tag{83}$$

with index sets $\mathfrak{B}$, C, $R(\mathfrak{b})$, and $\mathfrak{A}(\mathfrak{b}, c, r)$ still to be defined. In fact C is simply the ideal class group of F, and $\mathfrak{B}$ is the set consisting of all products of distinct prime ideals of F above 2. Note that the empty product is by convention $\mathcal{O}_F$, whence $\mathcal{O}_F \in \mathfrak{B}$. To define $R(\mathfrak{b})$ for $\mathfrak{b} \in \mathfrak{B}$ we first introduce an ideal $\hat{\mathfrak{b}}$ of $\mathcal{O}_F$ determined by $\mathfrak{b}$. Given any prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, let $e(\mathfrak{p})$ be the ramification index of $\mathfrak{p}$ over $\mathbb{Q}$. Then

$$\hat{\mathfrak{b}} = \prod_{\substack{\mathfrak{p}|2 \\ \mathfrak{p}\nmid\mathfrak{b}}} \mathfrak{p}^{2e(\mathfrak{p})+1}. \tag{84}$$

Let $C(\hat{\mathfrak{b}})$ be the wide ray class group of F to the modulus $\hat{\mathfrak{b}}$, and let $P(\hat{\mathfrak{b}})$ be the subgroup consisting of all ray classes represented by principal fractional ideals. Also write $P(\hat{\mathfrak{b}})^2$ for the subgroup consisting of all squares of elements of $P(\hat{\mathfrak{b}})$. We put

$$T(\mathfrak{b}) = C(\hat{\mathfrak{b}})/P(\hat{\mathfrak{b}})^2$$

and

$$R(\mathfrak{b}) = P(\hat{\mathfrak{b}})/P(\hat{\mathfrak{b}})^2,$$

and given a nonzero fractional ideal $\mathfrak{c}$ of F relatively prime to $\hat{\mathfrak{b}}$, we let $t(\mathfrak{c}) \in T(\mathfrak{b})$ be the coset represented by the ray class of $\mathfrak{c}$ modulo $\hat{\mathfrak{b}}$. Thus if $\mathfrak{c}'$ is another fractional ideal of F relatively prime to $\hat{\mathfrak{b}}$, then $t(\mathfrak{c}) = t(\mathfrak{c}')$ if and only if $\mathfrak{c}' = \alpha\beta^2\mathfrak{c}$ for some $\alpha, \beta \in F^\times$ relatively prime to $\hat{\mathfrak{b}}$ with $\alpha \equiv 1 \bmod^* \hat{\mathfrak{b}}$.

Before defining $\mathfrak{A}(\mathfrak{b}, c, r)$, we note that if $\mathfrak{c}$ and $\mathfrak{c}'$ are nonzero fractional ideals of F relatively prime to $\hat{\mathfrak{b}}$ and belonging to the same ideal class c then $t(\mathfrak{c}^2) = t((\mathfrak{c}')^2)$. Indeed $\mathfrak{c}' = \alpha\mathfrak{c}$ for some with $\alpha \in F^\times$ relatively prime to $\hat{\mathfrak{b}}$, and $t(\alpha^2\mathcal{O}_F) = 1$. We define $\mathfrak{A}(\mathfrak{b}, c, r)$ to be the set of ideals $\mathfrak{a}$ of $\mathcal{O}_F$ which are products of distinct prime ideals of F of odd residue characteristic and satisfy

$$t(\mathfrak{a}\mathfrak{b}\mathfrak{c}^2) = r \tag{85}$$

for some (hence any) fractional ideal $\mathfrak{c} \in c$ relatively prime to $\hat{\mathfrak{b}}$.

We can now define the sets $\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$: Given $\mathfrak{a}$, $\mathfrak{b}$, c, and r as in (83), choose an ideal $\mathfrak{c} \in c$ relatively prime to $\hat{\mathfrak{b}}$. We define $\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ to be the set of extensions of F inside $\overline{F}$ of the form $K = F(\sqrt{\delta})$, where δ runs over all generators of the principal fractional ideal $\mathfrak{a}\mathfrak{b}\mathfrak{c}^2$. Note that the set of such extensions is independent of the choice of $\mathfrak{c} \in c$. If we fix a generator δ of $\mathfrak{a}\mathfrak{b}\mathfrak{c}^2$ then the other generators have the form $u\delta$ with $u \in \mathcal{O}_F^\times$, so the elements of $\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ are the fields $K(\sqrt{u\delta})$ with u running over a set of representatives for the distinct cosets of $\mathcal{O}_F^{\times 2}$ in $\mathcal{O}_F^\times$. Thus

$$|\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}| = 2^{r_1+r_2}. \tag{86}$$

In particular, $\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ is finite.

Next we check that (83) holds. Given $K \in \mathcal{K}$, write $K = F(\sqrt{\delta})$ with $\delta \in F^\times$. Let $\mathfrak{g}$ be the product of the distinct prime ideals at which δ has odd valuation. Then $\delta\mathcal{O}_F = \mathfrak{g}\mathfrak{c}^2$ for some fractional ideal $\mathfrak{c}$ of F. Let $\mathfrak{a}$ be the product of the prime ideals dividing $\mathfrak{g}$ which are of odd residue characteristic and $\mathfrak{b}$ the product of those of residue characteristic 2. If $\mathfrak{p}$ is a prime ideal dividing $\hat{\mathfrak{b}}$ then the valuation of δ at $\mathfrak{p}$ is even, so after replacing δ by $\alpha^2\delta$ and $\mathfrak{c}$ by $\alpha\mathfrak{c}$ for an appropriate $\alpha \in F^\times$ we may assume that δ and $\mathfrak{c}$ are relatively prime to $\hat{\mathfrak{b}}$. Let c be the ideal class of $\mathfrak{c}$ and put $r = t(\delta\mathcal{O}_F)$. Then $K \in \mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$.

To see that (83) is actually a partition of $\mathcal{K}$ we must still check that the sets $\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ do not overlap nontrivially, or in other words that if $K \in \mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ then

$(\mathfrak{a}, \mathfrak{b}, c, r)$ can be recovered from K. In fact by (85) it suffices to see that $(\mathfrak{a}, \mathfrak{b}, c)$ can be recovered from K. Now $K = F(\sqrt{\delta})$ with

$$\delta\mathcal{O}_F = \mathfrak{a}\mathfrak{b}\mathfrak{c}^2 \tag{87}$$

and $\mathfrak{c} \in c$ relatively prime to $\hat{\mathfrak{b}}$. Thus $\mathfrak{a}\mathfrak{b}$ is the product of the distinct prime ideals of K which occur in $\mathfrak{d}_{K/F}$ with odd multiplicity. In particular, $\mathfrak{a}\mathfrak{b}$ is uniquely determined by K. Since $\mathfrak{a}$ is the product of the prime ideals dividing $\mathfrak{a}\mathfrak{b}$ which have odd residue characteristic it follows that $\mathfrak{a}$ and $\mathfrak{b}$ are uniquely determined by K as well. As for c, if $K = F(\sqrt{\delta'})$ with $\delta' \in F^\times$ then $\delta' = \alpha^2\delta$ for some $\alpha \in F^\times$. If we replace δ by δ' on the left-hand side of (87) then $\mathfrak{c}$ is replaced by $\alpha\mathfrak{c}$, so c is unchanged.

Thus (83) is a partition. It follows that the Dirichlet series (82) can be written

$$\mathcal{D}(s) = \sum_{\mathfrak{b}\in\mathfrak{B}} \sum_{c\in C} \sum_{r\in R(\mathfrak{b})} \sum_{\mathfrak{a}\in\mathfrak{A}(\mathfrak{b},c,r)} \sum_{K\in\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}} d_{K/F}^{-s}. \tag{88}$$

The innermost sum on the right-hand side is a finite Dirichlet series by (86), and we claim that it has the form

$$\sum_{K\in\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}} d_{K/F}^{-s} = (\mathbf{N}\mathfrak{a})^{-s}\Phi_{\mathfrak{b},r}(s), \tag{89}$$

where $\Phi_{\mathfrak{b},r}(s)$ is also a finite Dirichlet series and depends only on $\mathfrak{b}$ and r, not on $\mathfrak{a}$ and c. Granting this claim for the moment, we substitute (89) in (88), obtaining

$$\mathcal{D}(s) = \sum_{\mathfrak{b}\in\mathfrak{B}} \sum_{c\in C} \sum_{r\in R(\mathfrak{b})} \Phi_{\mathfrak{b},r}(s) \sum_{\mathfrak{a}\in\mathfrak{A}(\mathfrak{b},c,r)} (\mathbf{N}\mathfrak{a})^{-s} \tag{90}$$

Let us complete the proof of the theorem, granting the claim.

Let $X(\mathfrak{b})$ be the set of characters of $T(\mathfrak{b})$. An element $\chi \in X(\mathfrak{b})$ can be viewed as a character of $C(\hat{\mathfrak{b}})$ trivial on $P(\hat{\mathfrak{b}})^2$ and hence in particular as a ray class character of F to the modulus $\hat{\mathfrak{b}}$. When χ is so viewed it is in general imprimitive. However, consider the equation

$$\frac{L(s,\chi)}{L(2s,\chi)} \cdot \prod_{\mathfrak{p}|2} \frac{(1-\chi(\mathfrak{p})(\mathbf{N}\mathfrak{p})^{-\mathbf{s}})}{(1-\chi(\mathfrak{p})(\mathbf{N}\mathfrak{p})^{-\mathbf{2s}})} = \sum_{\mathfrak{a}} \chi(\mathfrak{a})(\mathbf{N}\mathfrak{a})^{-\mathbf{s}}, \tag{91}$$

where $\mathfrak{a}$ runs over all products of distinct prime ideals of F of odd residue characteristic. Since we have removed the Euler factors at all prime ideals dividing 2 and hence in particular at all prime ideals dividing $\hat{\mathfrak{b}}$, the two sides of (91) are unchanged if χ is replaced by the corresponding primitive character. In particular, the left-hand side is holomorphic for $\Re(s) > 1/2$ if $\chi \neq 1$ and meromorphic with a simple pole at $s = 1$ and no other poles for $\Re(s) > 1/2$ if $\chi = 1$. Furthermore, if $\chi = 1$ then the residue at $s = 1$ is the quantity

$$l_F = \frac{\lambda_F}{\zeta_F(2)} \cdot \prod_{\mathfrak{p}|2} \frac{\mathbf{N}\mathfrak{p}}{1+\mathbf{N}\mathfrak{p}}, \tag{92}$$

where $\zeta_F(s)$ is the Dedekind zeta function of F and λ_F its residue at $s = 1$. Of course λ_F can be given explicitly:

$$\lambda_F = \frac{2^{r_1(F)}(2\pi)^{r_2(F)}h_F\mathrm{R}eg_F}{w_F\sqrt{d_F}}, \tag{93}$$

where $\mathrm{R}eg_F$ is the regulator of F. It is immediate from (92) that $l_F > 0$.

We now return to (90) and consider the sum over $\mathfrak{a}$: the sum runs over $\mathfrak{a} \in \mathfrak{A}(\mathfrak{b}, c, r)$, whereas in (91), $\mathfrak{a}$ runs over all products of distinct prime ideals of odd residue characteristics. To bridge the difference we follow Dirichlet:

(94)
$$\mathcal{D}(s) = \sum_{\mathfrak{b}\in\mathfrak{B}} \sum_{c\in C} \sum_{r\in R(\mathfrak{b})} \frac{|R(\mathfrak{b})|}{|T(\mathfrak{b})|} \Phi_{\mathfrak{b},r}(s) \sum_{\chi\in X(\mathfrak{b})} \overline{\chi}(r) \frac{L(s,\chi)}{L(2s,\chi)} \prod_{\mathfrak{p}|2} \frac{(1-\chi(\mathfrak{p})(\mathbf{N}\mathfrak{p})^{-\mathbf{s}})}{(1-\chi(\mathfrak{p})(\mathbf{N}\mathfrak{p})^{-\mathbf{2s}})}.$$

where $\overline{\chi}(r)$ is understood to mean $\overline{\chi}(\mathfrak{g})$ for any nonzero fractional ideal g of F relatively prime to $\hat{\mathfrak{b}}$. Inspecting (94) and recalling the properties of Hecke L-functions just reviewed, we find that $\mathcal{D}(s)$ is holomorphic in the region $\Re(s) > 1/2$ except for a simple pole at $s = 1$ with residue

$$\kappa = l_F h_F \sum_{\mathfrak{b}\in\mathfrak{B}} \frac{|R(\mathfrak{b})|}{|T(\mathfrak{b})|} \sum_{r\in R(\mathfrak{b})} \Phi_{\mathfrak{b},r}(1).$$

Furthermore we have seen that $l_F > 0$, and since the left-hand side of (86) is a nonempty sum of terms of the form $d_{K/F}^{-s}$, it is immediate from (86) that $\Phi_{\mathfrak{b},r}(1) > 0$ also. Hence $\kappa > 0$, and an appeal to Proposition 1 completes the proof.

It remains to justify the claim. We have already deduced from (87) that if $K \in \mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ then $\mathfrak{ab}$ is the product of the distinct prime ideals of K which occur in $\mathfrak{d}_{K/F}$ with odd multiplicity. Now it is a standard fact about quadratic extensions that if $\mathfrak{p}$ is a prime ideal of F which occurs in $\mathfrak{d}_{K/F}$ with odd multiplicity then its multiplicity is 1 or $2e(\mathfrak{p})+1$ according as the residue characteristic of $\mathfrak{p}$ is odd or 2. Furthermore if $\mathfrak{p}$ occurs in $\mathfrak{d}_{K/F}$ with positive even multiplicity then $\mathfrak{p}|2$. It follows that if $K \in K_{\mathfrak{a},\mathfrak{b},c,r}$ then

$$d_{K/F} = (\mathbf{N}\mathfrak{a}) \cdot (\prod_{\mathfrak{p}|\mathfrak{b}} (\mathbf{N}\mathfrak{p})^{2e(\mathfrak{p})+1}) \cdot (\prod_{\mathfrak{p}|\hat{\mathfrak{b}}} (\mathbf{N}\mathfrak{p})^{\nu_\mathfrak{p}(K)}) \tag{95}$$

with even integers $\nu_\mathfrak{p}(K) \geqslant 0$ (in case $\mathfrak{b}$ or $\hat{\mathfrak{b}}$ is $\mathcal{O}_F$ we follow the usual convention that an empty product is 1). We would like to show that the finite Dirichlet series

$$\Psi_{\mathfrak{b},r}(s) = \sum_{K\in K_{\mathfrak{a},\mathfrak{b},c,r}} (\prod_{\mathfrak{p}|\hat{\mathfrak{b}}} (\mathbf{N}\mathfrak{p})^{\nu_\mathfrak{p}(K)})^{-s} \tag{96}$$

really does depend only on $\mathfrak{b}$ and r, as the notation implies, for then the finite Dirichlet series

$$\Phi_{\mathfrak{b},r}(s) = \Psi_{\mathfrak{b},r}(s) \prod_{\mathfrak{p}|\mathfrak{b}} (\mathbf{N}\mathfrak{p})^{-(2e(\mathfrak{p})+1)s}, \tag{97}$$

will likewise depend only on $\mathfrak{b}$ and r, and (89) will be satisfied.

Given a prime ideal $\mathfrak{p}$ of F dividing $\hat{\mathfrak{b}}$, let $F_\mathfrak{p}$ denote the completion of F at $\mathfrak{p}$, and let $K_\mathfrak{p}$ denote the compositum $KF_\mathfrak{p}$ inside some fixed algebraic closure of $F_\mathfrak{p}$ containing $\overline{F}$. Then $\nu_\mathfrak{p}(K)$ depends only on $K_\mathfrak{p}$. Thus it suffices to see that if K varies over the elements of $\mathcal{K}_{\mathfrak{a},\mathfrak{b},c,r}$ then the completions $K_\mathfrak{p}$ and the multiplicities with which they occur depend only on $\mathfrak{b}$ and r, not on $\mathfrak{a}$ and c.

To verify this, suppose that $c' \in C$ and that $\mathfrak{a}' \in \mathfrak{A}(\mathfrak{b}, c', r)$. Choose $\mathfrak{c}' \in c'$ relatively prime to $\hat{\mathfrak{b}}$. Then (85) holds with $\mathfrak{a}$ and $\mathfrak{c}$ replaced by $\mathfrak{a}'$ and $\mathfrak{c}'$. Let δ' be a fixed generator of the fractional ideal $\mathfrak{a}'\mathfrak{b}(\mathfrak{c}')^2$, and let δ be a fixed generator of the fractional ideal $\mathfrak{abc}^2$, as in (87). Since

$$t(\delta\mathcal{O}_F) = r = t(\delta'\mathcal{O}_F),$$

there exist elements $\alpha, \beta \in F^\times$, relatively prime to $\hat{\mathfrak{b}}$ and with $\alpha \equiv 1 \bmod^* \hat{\mathfrak{b}}$, such that

$$\delta' \mathcal{O}_F = \alpha\beta^2\delta\mathcal{O}_F.$$

Thus

$$\delta' = u_0\alpha\beta^2\delta \tag{98}$$

for some $u_0 \in \mathcal{O}_F^\times$. Thus the elements of $\mathcal{K}_{\mathfrak{a}',\mathfrak{b},c',r}$ are the fields $K' = F(\sqrt{uu_0\alpha\delta})$, where u runs over a set of representatives for the distinct cosets of $\mathcal{O}_F^{\times 2}$ in $\mathcal{O}_F^\times$. Furthermore, if $\mathfrak{p}|\hat{\mathfrak{b}}$ then α is a square in $F_\mathfrak{p}$, because $\alpha \equiv 1 \bmod^* \mathfrak{p}^{2e(\mathfrak{p})+1}$. Hence the list of completions $K'_\mathfrak{p} = F_\mathfrak{p}(\sqrt{uu_0\alpha\delta})$ coincides up to a permutation of the coset representatives u with the list of completions $K_\mathfrak{p} = F_\mathfrak{p}(\sqrt{u\delta})$.

References

[1] G. Anderson, D. Blasius, R. Coleman, and G. Zettler, *On representations of the Weil group with bounded conductor*, Forum Math. 6 (1994), 537 – 545.

[2] P. T. Bateman and H. G. Diamond, *Analytic Number Theory: An Introductory Course*. World Scientific (2004).

[3] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. Math. 162 (2005), 1031 – 1063.

[4] M. Barghava, *The density of discriminants of quintic rings and fields*, Ann. Math. 172 (2010), 1559 – 1591.

[5] M. Bhargava, A. Cojocaru, and F. Thorne, *The square sieve and the number of A_5-quintic extensions of bounded discriminant*, to appear.

[6] H. Cohen, *Advanced topics in computational number theory*. Grad. Texts in Math. 193, Springer (2000).

[7] M. J. Collins, *On Jordan's theorem for complex linear groups*, J. Group Theory 10 (2007), 411 – 423.

[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups.* Clarendon Press, 1985.

[9] G. Cooke and P. J. Weinberger, *On the construction of division chains in algebraic number fields, with applications to SL_2*, Commun. Algebra 3 (1975), 481-524.

[10] P. Deligne, *Les constantes des équations fonctionelles des fonctions L*. In: *Modular Functions of One Variable, II*, Lect. Notes in Math. 349, Springer (1973), 501–595.

[11] W. Duke, *The dimension of the space of cusp forms of weight one*, Internat. Math. Research Notices (1995), 99 – 109.

[12] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. 17 (1972), 143 – 166.

[13] P. X. Gallagher, *Determinants of representations of finite groups*, Abh. Math. Sem. Univ. Hamburg 28 (1965), 162–167.

[14] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, 5th ed.*, Clarendon, Oxford (1979).

[15] P. N. Hoffman and J. F. Humphreys, *Projective Representations of the Symmetric Groups: Q-Functions and Shifted Tableaux*, Oxford Mathematical Monographs, Clarendon Press, Oxford (1992).

[16] B. Huppert, *Character Theory of Finite Groups*, de Gruyter (1998).

[17] G. Karpilovsky, *Group Representations* vol. 2, North-Holland Mathematics Studies 177, (1993).

[18] N. Kataoka, *The distribution of prime ideals in a real quadratic field with units having a given index in the residue class field*, J. Number Theory 101 (2003), 349 – 375.

[19] Y. Kitaoka, *Distribution of units of a cubic field with negative discriminant*, J. Number Theory 91 (2001), 318 – 355.

[20] Y. Kitaoka, *Distribution of units of an algebraic number field*. In: *Galois Theory and Modular Forms,* edited by K. Hashimoto, K. Miyake, and H. Nakamura, Kluwer Academic Publishers (2003).

[21] J. Klüners, *A counter example to malle's conjecture on the asymptotics of discriminants*, C. R. Acad. Sci. Paris, Ser. I 340 (2005), 411-414.
[22] S. Lang, *Introduction to Modular Forms*, Springer, Grundlehren der math. Wissen. 222, (1976). Appendix by W. Feit: *Exceptional subgroups of GL_2*.
[23] S. Lang, *Algebraic Number Theory*, 2nd. ed., Springer GTM 110 (1994).
[24] S. Lang, *Elliptic Functions*, Springer, GTM 112 (1987).
[25] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Inventiones math. 42 (1977), 201 – 224.
[26] G. Malle, *On the distribution of Galois groups, II*, Experimental Math. 13 (2004), 129 – 135.
[27] J. Martinet, *Character theory and Artin L-functions*, In: *Algebraic Number Fields, Proceedings of the Durham Symposium*, A. Fröhlich ed. Academic Press (1977), 1 – 87
[28] P. Michel and A. Venkatesh, *On the dimension of the space of cusp forms associated to 2-dimensional complex Galois representations*, Internat. Math. Research Notices (2002), 2021 – 2027.
[29] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer 10 (1988), 59 – 67.
[30] H. Roskam, *A quadratic analogue of Artin's conjecture on primitve roots*, J. Number Theory 81 (2000), 93 – 109.
[31] J.-P. Serre, *Modular forms of weight one and Galois representations* In: *Algebraic Number Fields, Proceedings of the Durham Symposium*, A. Fröhlich ed. Academic Press (1977), 193 – 268. (=*Oeuvres* vol. III, no. 110.)
[32] J.-P. Serre, *Local Fields*, translated from the French by M. J. Greenberg, Springer GTM 67 (1979).
[33] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), 123 – 201. (=*Oeuvres* vol. III, no. 125.)
[34] J.-P. Serre, *Topics in Galois Theory*, Notes written by H. Darmon, Jones and Bartlett Publishers, Research Notes in Mathematics 1 (1992).
[35] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Ann. of Math. 45 (1944), 667 - 685.
[36] L. C. Washington, *Introduction to cyclotomic fields.* Springer GTM 83 (1982).
[37] H. Weber,*Lehrbuch der Algebra, Bd. II (zweite Auflage).* Braunschweig (1899).
[38] S. Wong, *Automorphic forms on GL(2) and the rank of class groups*, J. reine angew. Math. 515 (1999), 125 – 153.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu