SELF-DUAL ARTIN REPRESENTATIONS OF DIMENSION THREE

(WITH AN APPENDIX BY DAVID E. ROHRLICH)

ADITYA KARNATAKI

Abstract. We give an unconditional proof that self-dual Artin representations of $\mathbb{Q}$ of dimension 3 have density 0 among all Artin representations of $\mathbb{Q}$ of dimension 3. Previously this was known under the assumption of Malle's Conjecture.

1. Introduction

It is expected that essentially self-dual motives (i.e. motives that are dual to a Tate twist of themselves) should occur with density 0. This statement has not yet been formulated for motives with weights higher than 0, but for Artin motives of fixed dimension, this is a precise question as shown in [1]. Let F be a number field, and if ρ is an Artin representation of F, let $q(\rho)$ be the absolute norm of the conductor ideal $\mathfrak{q}(\rho)$. We denote by $\vartheta_{F,n}(x)$ the number of isomorphism classes of Artin representations over F of dimension n with $q(\rho) \leq x$ and by $\vartheta^{sd}_{F,n}(x)$ the number of isomorphism classes of self-dual Artin representations over F of dimension n with $q(\rho) \leq x$. Rohrlich proved in [10] that the quotient $\vartheta^{sd}_{\mathbb{Q},2}(x)/\vartheta_{\mathbb{Q},2}(x)$ goes to 0 as x goes to ∞. Thus, our density 0 expectations are true for dimension 2. (The 1-dimensional case is elementary.) He proved the same result for $\mathbb{Q}$ and dimension 3 under a weak form of Malle's Conjecture. In this paper, we remove this condition, viz. we confirm unconditionally,

Theorem 1.

$$\lim_{x\to\infty} \frac{\vartheta^{sd}_{\mathbb{Q},3}(x)}{\vartheta_{\mathbb{Q},3}(x)} = 0.$$

We can replace $\mathbb{Q}$ by any number field and ask a similar question. But that case seems considerably harder. In dimension 1, the density result for a general number field follows from work of Taylor [13].

Before describing our work, we set some notations. For a finite extension K/F of number fields, we denote by $\mathfrak{d}_{K/F}$ the relative discriminant ideal and by $d_{K/F}$ its absolute norm. For $F = \mathbb{Q}$, we simply write $\mathfrak{d}_K$ and d_K. We denote by $\eta_{F,m}(x)$ the number of extensions K/F inside a fixed algebraic closure $\bar{F}$ such that $[K : F] = m$ and $d_{K/F} \leq x$. Also, if T is a transitive subgroup of the symmetric group S_m, we denote by $\eta^T_{F,m}(x)$ the number of extensions K/F for which $Gal(L/F) \cong T$ as permutation groups, where L/F

Key words and phrases. Artin L-function, self-dual Artin representation, conductor, discriminant, distribution of discriminants.

is the normal closure of K over F and $Gal(L/F)$ is viewed as a permutation group via its action on conjugates of a primitive element of K over F.

We now describe the structure of this paper. In section 2, we shall use results from [10] to see that the problem reduces to bounding the number of *irreducible* self-dual Artin representations of $\mathbb{Q}$.

Thus, we wish to count irreducible self-dual Artin representations. Such a representation has to be either orthogonal or symplectic. Since the dimension is odd, we see that we are reduced to the orthogonal case. We are thus reduced to analyzing irreducible orthogonal finite subgroups G of $\mathrm{GL}_3(\mathbb{C})$, where $G = \rho(Gal(K/\mathbb{Q}))$ and K is the fixed field of ker ρ.

Our general strategy is to replace ϑ, which count conductors of representations, by η, which count discriminants of number fields. We then appeal to results of Bhargava ([3], [4]) and Bhargava, Cojocaru, and Thorne [5].

We shall divide our analysis into two cases : (1) Those G which are contained in SO_3 and, (2) those which are not. In section 3, we analyze the subgroups occurring in case (1). Using bounds on ramification of primes, we obtain bounds in this case in terms of $\eta^{A_4}_{\mathbb{Q},4}(x)$, $\eta^{S_4}_{\mathbb{Q},4}(x)$, and $\eta^{A_5}_{\mathbb{Q},5}(x)$.

Having obtained these, we turn our attention to case (2). We further divide this case into two parts. Part 1 is the case where $-1 \notin G$. We analyze this case in section 5. If $-1 \notin G$, then we show that $G \cong S_4$ and ρ is monomial, induced from a quadratic character of a cubic subextension. Therefore, we reduce our problem to counting such extensions and characters, using the interplay between conductors and discriminants, and obtain bounds in terms of $\eta_{\mathbb{Q},3}(x)$.

In section 6, we deal with the case where $-1 \in G$. This implies that G can be written as $H \times \{\pm 1\}$. In this case, in addition to monomial representations with $H \cong A_4$ or S_4, we must also contend with representations coming from a primitive $H \cong A_5$. It is worth noting that the irreducible primitive case corresponds to the dominant term in all our analysis and it is only the power-saving result of Bhargava, Cojocaru and Thorne that helps us establish our result.

Finally, in section 7, we combine results from section 4, 5, 6 to get the main theorem.

2. Acknowledgments

I am deeply grateful to David Rohrlich for directing my attention towards this problem and for providing me with helpful hints. I would also like to thank Shaunak Deo for his indispensable inputs and all the innumerable Mathematics discussions. I am also thankful to the anonymous referee for making valuable comments and suggestions.

3. Reduction To The Irreducible Case

As in [10], we have

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

where

(a) $\vartheta^{ab,sd}_{\mathbb{Q},3}(x)$ is the number of abelian self-dual Artin representations of $\mathbb{Q}$ of dimension 3 with $q(\rho) \leq x$

(b) $\vartheta^{1+2,sd}_{\mathbb{Q},3}(x)$ is the number of isomorphism classes of self-dual Artin representations of $\mathbb{Q}$ of dimension 3 of the form $\rho \cong \rho' \oplus \rho''$ with ρ' one-dimensional, ρ'' irreducible and two-dimensional and $q(\rho')q(\rho'') \leq x$, and

(c) $\vartheta^{irr,sd}_{\mathbb{Q},3}(x)$ is the number of irreducible self-dual Artin representations of $\mathbb{Q}$ of dimension 3 with $q(\rho) \leq x$.

From Theorem 2 of [10], we see that

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

while from equation (80) of the same paper, we see that

$$\vartheta^{1+2,sd}_{\mathbb{Q},3}(x) \ll x^{2-\epsilon}.$$

Since, by Theorem 1 of [10],

$$\vartheta^{ab}_{\mathbb{Q},3}(x) \sim O(x^2(\log x)^2),$$

we see that, if we can prove

$$\vartheta^{irr,sd}_{\mathbb{Q},3}(x) \ll O(x^{2-\epsilon}), \tag{2}$$

then we conclude that the self-dual representations have density zero.

4. Finite Irreducible Orthogonal Subgroups of $\mathrm{GL}_3(\mathbb{C})$

We are interested in irreducible self-dual Artin representations. By definition of self-dual representations, these have to be either orthogonal or symplectic, i.e. their image is contained either in $O_n(\mathbb{R})$ or $Sp_{2n}(\mathbb{C})$. (In particular the trace has to be real for these representations.) But since the dimension is odd, these have to be in O_3, where O_3 is the orthogonal group of real $3x3$ matrices. We shall first concentrate on finite subgroups of SO_3. Referring to [2], chapter 5, we see that every finite subgroup G of SO_3 is one of the following :

(1) C_k : The cyclic group of rotations by multiples of $2\pi/k$ about a line
(2) D_k : The dihedral group of symmetries of a regular k-gon
(3) A_4 : The alternating group on 4 variables
(4) S_4 : The symmetric group on 4 variables
(5) A_5 : The alternating group on 5 variables

The cyclic groups and dihedral groups do not possess irreducible 3-dimensional representations. The last three groups do have irreducible 3-dimensional representations. Note that S_4 has two irreducible 3-dimensional representations, but the image of only one of them is contained in SO_3. We call a subgroup G of $\mathrm{GL}_n(\mathbb{C})$ *irreducible* if the inclusion $i : G \to \mathrm{GL}_n(\mathbb{C})$ is an irreducible representation of G.

5. A Bound on Discriminants for finite subgroups of SO_3

In this section, ρ is an irreducible self-dual Artin representation and K denotes the fixed field of kerρ. We know that $\rho(Gal(K/\mathbb{Q}))$ is a finite irreducible subgroup of O_3. We divide our analysis into two cases, depending upon whether $\rho(Gal(K/\mathbb{Q}))$ is a subgroup of SO_3 or not. Thus, we write :

$$\vartheta^{irr,sd}_{\mathbb{Q},3}(x) = \vartheta_1(x) + \vartheta_2(x), \tag{3}$$

where

$$\vartheta_1(x) = \sum_{\substack{\rho \\ \rho(Gal(K/\mathbb{Q}))\subset SO(3) \\ q(\rho)\leq x}} 1$$

and

$$\vartheta_2(x) = \sum_{\substack{\rho \\ \rho(Gal(K/\mathbb{Q}))\not\subset SO(3) \\ q(\rho)\leq x}} 1.$$

For the rest of the section, we focus on bounding $\vartheta_1(x)$. From here on, we identify $Gal(K/\mathbb{Q})$ with its image under ρ. Thus, we assume $Gal(K/\mathbb{Q}) \subset SO_3$. We have seen in the previous section that this implies that $Gal(K/\mathbb{Q})$ is isomorphic to A_4, S_4, or A_5, and we write m for the degree of the permutation group in question. Thus, $m = 4$ in the first two cases and $m = 5$ for the third. In all that follows, M is any subfield of K with $[M : \mathbb{Q}] = m$. The choice of M is arbitrary, but the normal closure of M is K for every one of them.

Proposition 1. *If $Gal(K/\mathbb{Q}) \cong A_4$,*

$$d_M \leq cq(\rho)^{3/2}$$

with an absolute constant $c > 1$.

Proof. We quote a standard bound (*cf.* [12], p. 127, Proposition 2), which is

$$d_M \leq c \prod_{\substack{p|d_M \\ p>m}} p^3 \tag{4}$$

with $c = 2^{11}3^7$.

Now, if $p > 4$ and $p|d_M$, then ρ restricted to the inertia group I for any prime $\mathfrak{p}$ above p factors through its tame quotient (since 2 or 3 are the only wildly ramified primes for im $\rho \cong A_4$) and hence, by the formula for (local) Artin conductor,

$$ord_p(q(\rho)) = dim(V/V^I) \tag{5}$$

where V is the space of ρ and V^I is the subspace of inertial invariants.

Case 1: I is a cyclic subgroup of order 2. Since all elements of order 2 are conjugate to each other in A_4, only one computation will suffice for all the three subgroups of order 2. We see from a character table (see e.g. [9]) and Frobenius Reciprocity that

$$\text{Multiplicity of trivial character in } \rho|_I = \frac{3(1) + (-1)(1)}{2} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Alternatively, we can also argue without referring to a character table as follows : We see that since the determinant of ρ is 1, the image under ρ of a non-trivial element is conjugate to

$$\begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$$

from which it is immediate that $dim(V^I) = 1$. We record this method here, since it is this method that will be useful in the latter sections.

Case 2: I is a cyclic subgroup of order 3. There are two conjugacy classes, each containing 4 elements of order 3, which cover all the elements of order 3 in A_4. The character of our 3-dimensional representation is valued 0 on both of these classes. Hence, for restriction to any subgroup of order 3, we see that

$$\text{Multiplicity of trivial character} = \frac{3(1) + 0(1) + 0(1)}{3} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Therefore, by (5), we see that

$$q(\rho) \geq \prod_{\substack{p|q(\rho) \\ p>m}} p^2$$

and combined with (4), it completes the proof.

Again, we can argue without using a character table : Since the determinant of ρ is 1, the image under ρ of a non-trivial element is conjugate to

$$\begin{pmatrix} 1 & & \\ & \zeta & \\ & & \zeta^2 \end{pmatrix}$$

where ζ is a primary cube root of unity. Thus, it is immediate that $dim(V^I) = 1$.

□

Proposition 2. *If $Gal(K/\mathbb{Q}) \cong S_4$,*

$$d_M \leq cq(\rho)^{3/2}$$

with an absolute constant $c > 1$.

Proof. We use a strategy similar to the one we used earlier. Note that the representation ρ of S_4 is the twist of the standard representation by the alternating character. This can be seen from the character table of S_4 since ρ is irreducible and of trivial determinant. At the referee's suggestion, we direct the reader to [9], page 18, for information about the standard representation of S_4.

Case 1: I is a cyclic subgroup of order 2. There are two conjugacy classes, one containing 6 elements of order 2 and one containing 3 elements of order 2, which cover all the elements of order 2 in S_4. The character of our 3-dimensional representation is valued -1 on both these classes. Hence, for restriction to any subgroup of order 2, we see that

$$\text{Multiplicity of trivial character} = \frac{3(1) + (-1)(1)}{2} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Case 2: I is a cyclic subgroup of order 3. The character is valued 0 on the unique conjugacy class of elements of order 3. Hence, for restriction to any subgroup of order 3, we see that

$$\text{Multiplicity of trivial character} = \frac{3(1) + 0(1) + 0(1)}{3} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Case 3: I is a cyclic subgroup of order 4. Any subgroup of order 4 contains, apart from the identity, two elements of order 4 and one element of order 2. Our character is valued 1 on elements of order 4 and -1 on elements of order 2. (Elements of order 4 all belong to the same conjugacy class and the class does not matter for elements of order 2 as our character is valued the same on both of them as mentioned above.) Hence, for restriction to any subgroup of order 4, we see that

$$\text{Multiplicity of trivial character} = \frac{3(1) + 1(1) + (-1)(1) + 1(1)}{4} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Therefore, by (5), we see that

$$q(\rho) \geq \prod_{\substack{p|q(\rho)\\ p>m}} p^2$$

and combined with (4), it completes the proof.

We remark that we can follow the alternate method mentioned in the previous proposition here as well.

□

Proposition 3. *If $Gal(K/\mathbb{Q}) \cong A_5$,*

$$d_M \leq cq(\rho)^2$$

with an absolute constant $c > 1$.

Proof. Since m is now 5 rather than 4, we have a different bound

$$d_M \leq c \prod_{\substack{p|d_K\\ p>5}} p^4 \tag{6}$$

with $c = 2^{14}3^9 5^9$ from the same reference [12].

Now, we again consider cases of cyclic subgroups. Note that, in this case, we have two 3-dimensional representations.

Case 1: I is a cyclic subgroup of order 2. All the elements of order 2 in A_5 are conjugate to each other. Both our characters are valued -1 on this class. Hence, for restriction of either of the representations to any cyclic subgroup of order 2, we see that

$$\text{Multiplicity of trivial character} = \frac{3(1) + (-1)(1)}{2} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Case 2: I is a cyclic subgroup of order 3. All the elements of order 3 in A_5 are conjugate to each other. Both our characters are valued 0 on this class. Hence, for restriction of either of the representations to any cyclic subgroup of order 3, we see that

$$\text{Multiplicity of trivial character} = \frac{3(1)+0(1)+0(1)}{3} = 1.$$

Hence, $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Case 2: I is a cyclic subgroup of order 5. There are two conjugacy classes in A_5, each containing 12 elements of order 5, which cover all the elements of order 5. As before, we can compute $codim V^I$ using a character table. But, in this case, it is more efficient to use the alternate method. We just note that since the determinant of ρ is 1, the image under ρ of a non-trivial element of I is conjugate to

$$\begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix}$$

where ω is a primary 5th root of unity. Thus, it is immediate that $dim(V^I) = 1$. So that $dim(V/V^I) = 2$.

Therefore, by (5), we see that

$$q(\rho) \geq \prod_{\substack{p|q(\rho) \\ p>m}} p^2$$

and combined with (6), it completes the proof.

□

Finally, we have

$$\vartheta_1(x) = \sum_{\substack{Gal(K/\mathbb{Q})\subset SO(3) \\ Gal(K/\mathbb{Q})\cong A_4 \\ q(\rho)\leq x}} 1 + \sum_{\substack{Gal(K/\mathbb{Q})\subset SO(3) \\ Gal(K/\mathbb{Q})\cong S_4 \\ q(\rho)\leq x}} 1 + \sum_{\substack{Gal(K/\mathbb{Q})\subset SO(3) \\ Gal(K/\mathbb{Q})\cong A_5 \\ q(\rho)\leq x}} 1,$$

which translates using propositions 1, 2, 3 to

$$\vartheta_1(x) \leq \sum_{\substack{Gal(K/\mathbb{Q})\cong A_4 \\ d_M\leq cx^{\frac{3}{2}}}} 1 + \sum_{\substack{Gal(K/\mathbb{Q})\cong S_4 \\ d_M\leq cx^{\frac{3}{2}}}} 1 + \sum_{\substack{Gal(K/\mathbb{Q})\cong A_5 \\ d_M\leq cx^2}} 1.$$

Since [3], [4] and [5] show that

$$\eta^{A_4}_{\mathbb{Q},4}(x) = O(x),\ \eta^{S_4}_{\mathbb{Q},4}(x) = O(x),\ \eta^{A_5}_{\mathbb{Q},5}(x) = O(x^{1-\beta}),$$

where β is any positive constant less than 1/120, we see that the above implies

$$\vartheta_1(x) = O(x^{2-2\beta+\epsilon}). \tag{7}$$

This yields the required estimate for $\vartheta_1(x)$.

6. Finite Subgroups of $O(3)$ that are not contained in $SO(3)$ - Part 1

In this section and the next, we focus on bounding $\vartheta_2(x)$.

We deal with this case in two parts, depending upon whether -1, the negative of the identity matrix in 3 dimensions, is in the image of $Gal(K/\mathbb{Q})$. Part 1 is devoted to the case :

$$Gal(K/\mathbb{Q}) \not\subset SO(3), -1 \notin Gal(K/\mathbb{Q}).$$

In this case, we prove a lemma which straightaway tells us what $Gal(K/\mathbb{Q})$ is.

Lemma 1. *Let G be a finite irreducible subgroup of $O(3)$ which is not contained in $SO(3)$. Assume further that $-1 \notin G$. Then $G \cong S_4$.*

Proof. Let

$$H = G \cap SO(3).$$

Then we can write

$$G = H \cup \kappa H,$$

where $det(\kappa) = -1$.

Then we can define

$$H^* = H \cup (-\kappa)H,$$

so that $H^* \subset SO(3)$. Note that G and H^* are "isoclinic", i.e. they only possibly differ by scalars. (Refer to [7], page xxiii, for more details on isoclinism.) Therefore, H^* is an irreducible subgroup of SO_3. As a result, we see that $H^* \cong A_4, S_4$ or A_5. But, A_4 or A_5 do not possess index 2 subgroups. Hence,

$$H^* \cong S_4.$$

Then, we can give an explicit isomorphism from G to H^* using the index 2 subgroup H, viz. send $h \to h$ and $\kappa h \to (-\kappa)h$. It is easily seen that this is an isomorphism, and thus $G \cong S_4$.

□

Indeed we see that S_4 has a faithful 3-dimensional representation which satisfies our hypotheses. Our earlier method of comparing conductors and discriminants yields weaker bounds than what are needed for our purpose, because we cannot rule out the possibility that $\det \rho$ is nontrivial on I. If I is of order 2, then the matrix corresponding to the non-trivial element of inertia would then be conjugate to

$$\begin{pmatrix} -1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

which yields a weaker lower bound for $q(\rho)$ and thus allows for a larger number of ρ. This does not happen, but we need to take a different path to prove this, which we describe below.

The standard representation (i.e. the 3-dimensional irreducible representation with non-trivial determinant) of S_4 is monomial. This means that there exists a subfield M of K such that $[M : \mathbb{Q}] = 3$, $Gal(K/M) = D_8$, together with a quadratic 1-dimensional character χ of $Gal(K/M)$ such that

$\rho = Ind_{M/\mathbb{Q}}(\chi)$, where $Ind_{M/\mathbb{Q}}$ denotes induction of representation from the subgroup $Gal(K/M)$ to the group $Gal(K/\mathbb{Q})$. Thus, we can try to count pairs (M, χ). We have classical results by Davenport and Heilbronn ([8]) on counting cubic number fields by discriminants. Since we are only concerned about the main term here, we do not need the error improvement by Bhargava, Shankar and Tsimerman ([6]). Note that for each such pair (M, χ), we have two more pairs (M', χ') and (M'', χ''), corresponding to conjugate copies of $D_8 \subset S_4$ that will give us the same representation, but that will only affect the constant term in our bounds.

We begin by denoting our counting function :

$$\Theta(x) := \sum_{\substack{\rho \\ Gal(K/\mathbb{Q}) \not\subset SO_3 \\ -1 \notin Gal(K/\mathbb{Q}) \\ q(\rho) \leq x}} 1.$$

The Conductor-Discriminant formula gives

$$q(\rho) = d_M q(\chi), \tag{8}$$

where d_M is the discriminant of the field M and $q(\chi)$ is the absolute norm of the conductor of the character χ.

Thus, we see that

$$\Theta(x) = \sum_{\substack{\rho \\ Gal(K/\mathbb{Q}) \not\subset SO_3 \\ Gal(K/\mathbb{Q}) \cong S_4 \\ q(\rho) \leq x}} 1 \ \leq \sum_{\substack{(M,\chi) \\ [M:\mathbb{Q}]=3 \\ \chi^2=1 \\ q(\chi) d_M \leq x}} 1, \tag{9}$$

where the first equality is due to the lemma.

We need to count the extensions M as well as characters χ. We write $\theta_{M,2}(x)$ for the number of characters χ of M with $\chi^2 = 1$ and $q(\chi) \leq x$. We shall use upper bounds for $\theta_{M,2}(x)$ from the appendix of this paper. These bounds are slightly weaker than the actual asymptotic if we work with a field M that is fixed, but since we are working with varying fields M at the same time, these bounds, which are uniform as long as the degree $[M : \mathbb{Q}]$ is fixed (which is true in our case), will work better, and the only expense incurred is a power of logarithm. It can be seen from the final proposition of this section below, that this increased power does not affect our result. We note that the asymptotic is an interesting result in itself, which follows from computing the residue of an appropriate Zeta Function and knowledge of bounds on the class number and the regulator of a number field.

From the corollary to Proposition 2 in the appendix to this paper, we see that

$$\theta_{M,2}(x) \ll \sqrt{d_M} (\log\, d_M)^2 x (\log\, x)^2, \tag{10}$$

where the implied constant is independent of M, since c and m are now fixed.

We now prove our main result of this section.

Proposition 4. *Let ρ, K be as before. Then*

$$\Theta(x) = O(x^{\frac{3}{2}+\epsilon}).$$

Proof. By (9), it is sufficient to prove

$$\sum_{\substack{(M,\chi)\\ [M:\mathbb{Q}]=3\\ q(\chi)d_M\leq x}} 1 = O(x^{\frac{3}{2}+\epsilon}), \tag{11}$$

where χ is a quadratic character of M. That is, we wish to prove

$$\sum_{\substack{M\\ [M:\mathbb{Q}]=3\\ d_M\leq x}} \sum_{\substack{\chi\\ q(\chi)\leq x/d_M}} 1 = O(x^{\frac{3}{2}+\epsilon}). \tag{12}$$

From (10), we see that

$$\sum_{\substack{M\\ [M:\mathbb{Q}]=3\\ d_M\leq x}} \sum_{\substack{\chi\\ q(\chi)\leq x/d_M}} 1 \ll \sum_{\substack{[M:\mathbb{Q}]=3\\ d_M\leq x}} \sqrt{d_M}(\log d_M)^2(\log \frac{x}{d_M})^2\frac{x}{d_M}. \tag{13}$$

The implied constant is uniform. Hence, we get

$$\sum_{\substack{M\\ [M:\mathbb{Q}]=3\\ d_M\leq x}} \sum_{\substack{\chi\\ q(\chi)\leq x/d_M}} 1 = x(\log x)^2 O\left(\sum_{\substack{M\\ [M:\mathbb{Q}]=3\\ d_M\leq x}} \frac{(\log d_M)^2}{\sqrt{d_M}}\right). \tag{14}$$

Using the fact from [8] that

$$\sum_{\substack{M\\ [M:\mathbb{Q}]=3\\ d_M\leq x}} 1 \sim cx, \tag{15}$$

where c is an absolute constant, we see that the above sum can be estimated as

$$\left(\sum_{\substack{M\\ [M:\mathbb{Q}]=3\\ d_M\leq x}} \frac{(\log d_M)^2}{\sqrt{d_M}}\right) = O(x^{\frac{1}{2}+\epsilon}), \tag{16}$$

which proves (12). Thus, the proposition follows. □

7. Finite Subgroups of $O(3)$ that are not contained in $SO(3)$ - Part 2

We deal with the remaining cases in this section. These cases are characterized by :

$$Gal(K/\mathbb{Q}) \not\subset SO(3), -1 \in Gal(K/\mathbb{Q}).$$

Put $H = Gal(K/\mathbb{Q}) \cap SO(3)$. Then we see that $Gal(K/\mathbb{Q}) \cong H \times \{\pm 1\}$. The Artin representation ρ we are considering can be written as $\rho \cong \sigma \bigotimes \epsilon$, where σ is the irreducible three-dimensional representation of H given by the inclusion $H \subset SO(3)$ and ϵ is a quadratic character of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus, we can hope to estimate the number of pairs (σ, ϵ) and obtain the bounds that we need.

We shall first do this in the case where $H \cong A_5$. Let us denote the corresponding A_5-subextension of K by L. In this case, the representation σ of A_5 is a primitive representation since A_5 has no index three subgroups. In fact, there are two representations of A_5 possible, and both of them are primitive. As before, let M be a subfield of L such that $[M : \mathbb{Q}] = 5$. The normal closure of M is L for any choice of M.

We wish to estimate

$$\Psi(x) := \sum_{\substack{\rho \\ q(\rho)\leq x \\ \rho\cong\sigma \bigotimes \epsilon}} 1,$$

where σ is a faithful irreducible representation of $A_5 \cong Gal(L/\mathbb{Q})$, considered as an Artin representation of $\mathbb{Q}$, and ϵ is a quadratic character of $\mathbb{Q}$.

For a fixed σ we look at $q(\sigma \otimes \epsilon)$ and $q(\sigma)$. Let

$$q_{tame}(\sigma) = \prod_{p\in X} p^{e_p}$$

be the tame conductor of σ, where X is the set of tamely ramified primes in L. By a computation done previously, each $e_p = 2$. Thus,

$$q_{tame}(\sigma) = \prod_{p\in X} p^2. \tag{17}$$

Let $X = A \cup B \cup C$, where A, B, and C are the sets of tamely ramified primes with inertia subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/5\mathbb{Z}$ respectively.

Let us write the conductor of ϵ as

$$q(\epsilon) = 2^{\alpha} \prod_{j=1}^{s} q_j, \tag{18}$$

where $\alpha = 0, 2$, or 3, and q_j are distinct odd primes. We can write $\epsilon = \chi\chi'$ where χ and χ' are quadratic characters of $\mathbb{Q}$ such that

$$p|q(\chi) \iff p = 2, 3, 5 \text{ or } p \in X.$$

Thus, primes that divide $q(\chi')$ are primes that are unramified in L which divide the conductor of ϵ.

Proposition 5. *Let $\sigma, \epsilon, \chi, \chi'$ be as above. Then*

$$q(\sigma \otimes \epsilon) = q(\sigma \otimes \chi\chi') = q(\sigma \otimes \chi)q(\chi')^3.$$

Proof. This follows from a well-known local computation for each prime dividing $q(\sigma \otimes \chi)$ and $q(\chi')$. At the referee's suggestion, we include the reference of Serre's book on Local Fields [11], Corollary 1′, page 100 from which the result follows. ☐

Thus, we see that the condition

$$q(\rho) = q(\sigma \otimes \epsilon) \leq x$$

translates to the condition

$$q(\sigma \otimes \chi) \leq x \text{ and } q(\chi') \leq \left(\frac{x}{q(\sigma \otimes \chi)}\right)^{\frac{1}{3}}. \tag{19}$$

Hence, we get

$$\Psi(x) \leq \sum_{q(\sigma\otimes\chi)\leq x} \sum_{q(\chi')\leq\left(\frac{x}{q(\sigma\otimes\chi)}\right)^{\frac{1}{3}}} 1. \tag{20}$$

The number of quadratic characters of $\mathbb{Q}$ with conductor $\leq x$ is $O(x)$. So (20) yields

$$\Psi(x) \ll \sum_{q(\sigma\otimes\chi)\leq x} \left(\frac{x^{\frac{1}{3}}}{q(\sigma \otimes \chi)^{\frac{1}{3}}}\right),$$

which gives the following proposition.

Proposition 6.

$$\Psi(x) \ll x^{\frac{1}{3}} \sum_{q(\sigma\otimes\chi)\leq x} \frac{1}{q(\sigma \otimes \chi)^{\frac{1}{3}}}. \tag{21}$$

Now, let

$$\Theta(x) = \sum_{q(\sigma\otimes\chi)\leq x} 1,$$

where σ and χ are as above.

Proposition 7. *We have*

$$\Theta(x) = O(x^{2-2\beta}),$$

where β is any positive constant less than $\frac{1}{120}$.

Proof. We shall convert the problem of estimating $\Theta(x)$ into a problem of counting A_5-extensions of $\mathbb{Q}$ and quadratic characters of $\mathbb{Q}$. For this, we look at the conductors and discriminants.

Since we only let $2, 3, 5$ or primes that are tamely ramified in L remain in the conductor of χ, we see that

$$q(\chi) = 2^\alpha 3^\beta 5^\gamma \prod_{p\in Y} p$$

for some $Y \subset X$ and $\beta, \gamma \in \{0, 1\}$.

Let $A' = A\cap Y, B' = B\cap Y, C' = C\cap Y$ and $A'' = A\setminus A', B'' = B\setminus B', C'' = C \setminus C'$.

We can compute the effect of twisting by χ at each prime locally by looking at image under ρ of I, *cf.* proof of Proposition 1. We see using equations (17) and (18) that the tame conductor of $\sigma \otimes \chi$ is given by

$$q_{tame}(\sigma \otimes \chi) = \left(\prod_{p\in A'} p \prod_{p\in A''} p^2\right)\left(\prod_{p\in B'} p^3 \prod_{p\in B''} p^2\right)\left(\prod_{p\in C'} p^3 \prod_{p\in C''} p^2\right). \tag{22}$$

On the other hand, by a computation involving ramification degrees, we obtain a bound on the tame discriminant of M :

$$d_M^{tame} \leq \prod_{p\in A} p^2 \prod_{p\in B} p^2 \prod_{p\in C} p^4. \tag{23}$$

Comparing the above expressions, we see that

$$d_M^{tame} \leq q_{tame}(\sigma\otimes\chi)^2. \tag{24}$$

This is the inequality which helps us translate the bound on the conductor to a bound on the discriminants. We have not yet dealt with the primes $2, 3, 5$ which might be wild primes. But we have a uniform bound for them as we have seen before, cf. [12]. Letting $c = 2^{14}3^9 5^9$, we see from *loc. cit.* and (19) that

$$d_M \leq c d_M^{tame} \leq c q_{tame}(\sigma\otimes\chi)^2 \leq c q(\sigma\otimes\chi)^2 \leq cx^2. \tag{25}$$

Equipped with these results, we now obtain our result. We have

$$\Theta(x) \leq \sum_{\sigma}\sum_{\chi} 1$$

where σ and χ are as above and the sum runs only over pairs such that $q(\sigma\otimes\chi) \leq x$. Thus, we get

$$\Theta(x) \ll \sum_{\substack{M \\ d_M \leq cx^2}} \sum_{\substack{\chi \\ \chi^2=1 \\ q(\chi)|8d_M}} 1. \tag{26}$$

The inner sum is over quadratic characters χ and is thus $O(x^\epsilon)$ once σ is fixed, because the number of divisors of d_M is d_M^ϵ. Hence, we get

$$\Theta(x) \ll x^\epsilon \sum_{\substack{M \\ d_M \leq cx^2}} 1. \tag{27}$$

We then appeal to [5] as before, to obtain

$$\Theta(x) \ll x^\epsilon \left(x^2\right)^{1-\beta} \tag{28}$$

where β is a positive constant less than $1/120$, which finishes our proof. □

Using this proposition, we obtain our main result :

Proposition 8.

$$\Psi(x) = O(x^{2-2\beta}) \tag{29}$$

where β is as before.

Proof. This follows from combining the previous propositions 6 and 7 using Abel partial summation. □

We move on to the remaining cases. Recall that $Gal(K/\mathbb{Q}) \cong H \times \{\pm 1\}$, where H is an irreducible finite subgroup of $SO(3)$. We have dealt with the case $H \cong A_5$. We deal with the cases $H \cong A_4$, $H \cong S_4$ below. Let $L/\mathbb{Q}$ be a subextension such that $Gal(L/\mathbb{Q}) \cong H$.

In these cases, the representations ρ can be again written as $\sigma\otimes\epsilon$, where σ is an irreducible 3-dimensional representation of A_4 or S_4 with trivial determinant. Such representations σ are necessarily monomial, say induced from a cubic subextension $M/\mathbb{Q}$ of L. (As before, this follows from looking at the character table of respective groups.) ϵ is a quadratic character of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ as before. Note that $\epsilon = \det \rho$.

Proposition 9. *Let K, M, H be as before where $H \cong A_4$ or S_4. Define*

$$\Phi(x) := \sum_{\substack{\rho \\ q(\rho)\leq x \\ \rho\cong\sigma\otimes\epsilon}} 1$$

where ρ, σ, ϵ are also as before.

Then,

$$\Phi(x) = O(x^{\frac{3}{2}+\epsilon'}) \tag{30}$$

where ϵ' is arbitrarily small.

Proof. We prove the result for $H \cong S_4$. The case $H \cong A_4$ is completely analogous. Let $Ind_{M/\mathbb{Q}}$ and $res_{M/\mathbb{Q}}$ denote the induction and restriction functors for the group $Gal(L/\mathbb{Q})$ and subgroup $Gal(L/M)$. If $\sigma = Ind_{M/\mathbb{Q}}(\chi)$ for some χ, we see, by adjoint property of induction and restriction (Frobenius reciprocity), that

$$\rho \cong Ind_{M/\mathbb{Q}}(\chi \otimes res_{M/\mathbb{Q}}\epsilon).$$

Here, M determines σ which in turn fixes ϵ. Moreover, both χ and ϵ are quadratic characters. We denote the quadratic character $\chi \otimes \text{res}\ \epsilon$ by χ'.

This is analogous to our methods in section 5, where we counted pairs (M, χ') where M is a cubic extension of $\mathbb{Q}$ and χ' is a quadratic character of M. We again write :

$$q(\rho) = d_M q(\chi').$$

Then, using the same method, from corollary to Proposition 2 in the appendix, we have :

$$\theta_{M,2}(x) \ll \sqrt{d_M}(\log\, d_M)^2 x (\log\, x)^2.$$

And thus, we get

$$\Phi(x) \ll \sum_{\substack{[M:\mathbb{Q}]=3 \\ d_M\leq x}} \sqrt{d_M}(\log\, d_M)^2 (\log\, \frac{x}{d_M})^2 \frac{x}{d_M},$$

from which we get the required result.

□

8. Proof of Theorem 1

By Propositions 4, 8, 9, we see that

$$\vartheta_2(x) = O(x^{2-2\beta}) \tag{31}$$

which coupled with equations (3) and (7) finishes the proof.

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] M. Artin, *Algebra, Second Edition,* Pearson, 2 edition (August 13, 2010).

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

[4] M. Bhargava, *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] M. Bhargava, A. Shankar, J. Tsimerman, *On the Davenport-Heilbronn theorems and second order terms,* Invent. Math. 193(2) (2013), 439 – 499.

[7] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups,* Oxford, England: Clarendon Press, (1985).

[8] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II,* Proc. Roy. Soc. London Ser. A 322 (1971), no. 1551, 405 – 420.

[9] W. Fulton, J. Harris, *Representation Theory : A First Course (Readings in Mathematics),* Springer, Corrected edition (October 22, 1991).

[10] D. Rohrlich, *Self-dual Artin representations,* Automorphic Representation and L-functions, D. Prasad, C.S. Rajan, A. Sankaranarayanan, J. Sengupta, eds., Tata Institute of Fundamental Research Studies in Mathematics Vol. 22 (2013), 455 – 499.

[11] J.-P. Serre, *Local Fields : Graduate Texts in Mathematics* **67***,* Springer, Second corrected edition (1995).

[12] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev,* Publ. Math. IHES 54 (1981), 123 - 201. (=*Oeuvres* vol. III, no. 125.)

[13] M. J. Taylor, *On the equidistribution of Frobenius in cyclic extensions of a number field,* J. London Math. Soc. 29 (1984), 211-213.

Appendix:
Ray class characters of bounded order and bounded conductor

David E. Rohrlich

We introduce a partial order on the set of formal Dirichlet series with non-negative real coefficients. Given two such series $A(s) = \sum_{q\geqslant 1} a(q)q^{-s}$ and $B(s) = \sum_{q\geqslant 1} b(q)q^{-s}$, write $A(s) \preccurlyeq B(s)$ to mean that $a(q) \leqslant b(q)$ for all $q \geqslant 1$. It is readily verified that if $A(s) \preccurlyeq B(s)$ and $C(s) \preccurlyeq D(s)$ then $A(s)C(s) \preccurlyeq B(s)D(s)$. Furthermore the implication holds at the level of Euler products: if $A(s) = \prod_p A_p(s)$ and $B(s) = \prod_p B_p(s)$ with $A_p(s) \preccurlyeq B_p(s)$ for all p then $A(s) \preccurlyeq B(s)$.

By way of illustration, let M be a number field, $\mathcal{O}_M$ its ring of integers, and $\zeta_M(s)$ the associated Dedekind zeta function. Then it is a standard remark that

$$\zeta_M(s) \preccurlyeq \zeta(s)^m, \tag{1}$$

where $m = [M : \mathbb{Q}]$. Indeed let p be a rational prime and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_M$ above p, say of residue class degree f. The Euler factor of $\zeta_M(s)$ at $\mathfrak{p}$ satisfies

$$(1 - (\mathbf{N}\mathfrak{p})^{-s})^{-1} = \sum_{\nu\geqslant 0} p^{-\nu f s} \preccurlyeq \sum_{\nu\geqslant 0} p^{-\nu s} = (1 - p^{-s})^{-1}.$$

Hence if there are exactly r prime ideals $\mathfrak{p}$ above p then

$$\prod_{\mathfrak{p}|p} (1 - (\mathbf{N}\mathfrak{p})^{-s})^{-1} \preccurlyeq (1 - p^{-s})^{-r} \preccurlyeq (1 - p^{-s})^{-m}.$$

Passing to Euler products we obtain (1).

It follows from the definitions that if $A(s) \preccurlyeq B(s)$ then the associated summatory functions $\vartheta_A(x) = \sum_{n\leqslant x} a(n)$ and $\vartheta_B(x) = \sum_{n\leqslant x} b(n)$ satisfy $\vartheta_A(x) \leqslant \vartheta_B(x)$ for all x. For example, let $A(s)$ and $B(s)$ be the two sides of (1): Using Theorem 7.7 on p. 154 of [1] to estimate the summatory function of $\zeta(s)^m$, we obtain

$$\sum_{\mathbf{N}\mathfrak{q}\leqslant x} 1 \ll x(\log x)^{m-1} \qquad (x \geqslant 2), \tag{2}$$

where $\mathfrak{q}$ denotes a nonzero ideal of $\mathcal{O}_M$ and the implicit constant depends only on m, not on M.

To illustrate the use of (2), let us deduce a standard bound for the class number h_M of M. Let r_1 and r_2 be the number of real embeddings and half the number of complex embeddings of M, so that $r_1 + 2r_2 = m$. Thus the Minkowski constant $(4/\pi)^{r_2} m!/m^m$ is bounded above by

$$\mu = (4/\pi)^{m/2} \frac{m!}{m^m},$$

and therefore Minkowski's theorem gives

$$h_M \leqslant \sum_{\mathbf{N}\mathfrak{q}\leqslant \mu\sqrt{d_M}} 1, \tag{3}$$

where d_M is the absolute value of the discriminant of M (cf. [2], pp. 119-120). Combining (3) with (2), we recover the well-known bound

$$h_M \ll \sqrt{d_M}(\log d_M)^{m-1} \qquad (\mu\sqrt{d_M} \geqslant 2), \tag{4}$$

where the implicit constant depends only on m. We shall regard m as a fixed integer $\geqslant 2$, and thus the condition $\mu\sqrt{d_M} \geqslant 2$ is satisfied for all but finitely many

d_M with $[M:\mathbb{Q}]=m$. Furthermore, since $m \geqslant 2$, we have $d_M \geqslant 2$. Therefore we can remove the condition $\mu\sqrt{d_M} \geqslant 2$ from (4) and still assert that the implicit constant in (4) depends only on m. Actually it is more useful to state (4) for h_M^{nar}, the narrow ray class number of M. Since $h_M^{\mathrm{nar}} \leqslant 2^{r_1} h_M$, we have

$$h_M^{\mathrm{nar}} \ll \sqrt{d_M}(\log d_M)^{m-1}, \tag{5}$$

where the implicit constant depends only on m.

It is convenient to refine the relation $\preccurlyeq$ slightly. Suppose that $A(s)$ and $B(s)$ are Dirichlet series over M in the sense that they are presented to us in the form $A(s)=\sum_{\mathfrak{q}} a(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s}$ and $B(s)=\sum_{\mathfrak{q}} b(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s}$, where $\mathfrak{q}$ denotes as before a nonzero ideal of $\mathcal{O}_M$. We write $A(s) \preccurlyeq_M B(s)$ to mean that $a(\mathfrak{q}) \leqslant b(\mathfrak{q})$ for all $\mathfrak{q}$. Thus $\preccurlyeq$ coincides with $\preccurlyeq_{\mathbb{Q}}$. Of course every Dirichlet series is a Dirichlet series over $\mathbb{Q}$, and one readily verifies that if $A(s) \preccurlyeq_M B(s)$ then $A(s) \preccurlyeq B(s)$.

Given a rational integer $c \geqslant 2$, let

$$R_{M,c}(s)=\sum_{\mathfrak{q}} h^*_{M,c}(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s}$$

where $h^*_{M,c}(\mathfrak{q})$ is the number of idele class characters χ of M of conductor $\mathfrak{q}$ such that $\chi^c=1$. Also put

$$E_{M,c}(s)=\prod_{p|c}\prod_{\mathfrak{p}|p}\Big(\sum_{\nu=0}^{e(\mathfrak{p})(v_p(c)+1)}(\mathbf{N}\mathfrak{p})^{\nu(1-s)}\Big),$$

where $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$ over p and $v_p(c)$ the p-adic valuation of c.

Proposition 1. $R_{M,c}(s) \preccurlyeq_M h_M^{\mathrm{nar}} \cdot (\zeta_M(s)/\zeta_M(2s))^{c-1} \cdot E_{M,c}(s)$.

Define

$$E_{m,c}=\prod_{p|c}\prod_{e=1}^{m}\prod_{f=1}^{m}\Big(\sum_{\nu=0}^{e(v_p(c)+1)} p^{f\nu(1-s)}\Big)^m,$$

The following variant of Proposition 1 is weaker but actually more useful:

Proposition 2. $R_{M,c}(s) \preccurlyeq h_M^{\mathrm{nar}} \cdot \zeta(s)^{m(c-1)} \cdot E_{m,c}(s)$.

Proof. By inspection, $E_{M,c}(s) \preccurlyeq E_{m,c}(s)$. Also

$$\zeta_M(s)/\zeta_M(2s)=\prod_{\mathfrak{p}}(1+(\mathbf{N}\mathfrak{p})^{-s}) \preccurlyeq \prod_p\Big(\sum_{\nu\geqslant 0} p^{-\nu s}\Big)^m=\zeta(s)^m,$$

where $\mathfrak{p}$ runs over all nonzero prime ideals of $\mathcal{O}_M$. □

Let $\vartheta_{M,c}(x)$ and $\vartheta_{m,c}(x)$ denote the summatory function associated to $R_{M,c}(s)$ and $\zeta(s)^{m(c-1)} \cdot E_{m,c}(s)$ respectively. Then Proposition 2 gives

$$\vartheta_{M,c}(x) \leqslant h_M^{\mathrm{nar}}\vartheta_{m,c}(x),$$

which in conjunction with (5) becomes

$$\vartheta_{M,c}(x) \ll \sqrt{d_M}(\log d_M)^{m-1}\vartheta_{m,c}(x). \tag{6}$$

Here the implicit constant depends only on m. Since $E_{m,c}(s)$ is entire while $\zeta(s)$ has a simple pole at $s=1$, we obtain (cf. [1], *loc. cit.*):

Corollary. $\vartheta_{M,c}(x) \ll \sqrt{d_M}(\log d_M)^{m-1}x(\log x)^{m(c-1)-1}$, *the implicit constant depending only on c and $m=[M:\mathbb{Q}]$.*

We turn to the proof of Proposition 1. Put

$$\varphi_M(\mathfrak{q}) = |(\mathcal{O}_M/\mathfrak{q})^\times|,$$

and let $\mathbb{A}_M^\times$ be the group of ideles of M. As usual, we think of $\mathbb{A}_M^\times$ as the restricted direct product $\prod'_v M_v^\times$, where v runs over the places of M and M_v is the completion of M at v, and we identify $M^\times$ with its image in $\mathbb{A}_M^\times$ under the diagonal embedding. We also put

$$\widehat{\mathcal{O}}_M = \prod_{v\nmid\infty} \mathcal{O}_v, \tag{7}$$

where v runs over the finite places of M and $\mathcal{O}_v$ is the ring of integers of M_v. By appending the coordinate 1 at the infinite places, we may view $\widehat{\mathcal{O}}_M^\times$ as a subgroup of $\mathbb{A}_M^\times$. Similarly, the product $M_\infty^\times = \prod_{v|\infty} M_v^\times$ and its identity component $(M_\infty^\times)^0$ are subgroups of $\mathbb{A}_M^\times$ with coordinate 1 at the finite places. With these conventions,

$$h_M^{\mathrm{nar}} = |\mathbb{A}_M^\times/(M^\times \cdot \widehat{\mathcal{O}}_M^\times \cdot (M_\infty^\times)^0)|$$

(cf. [2], pp. 146-147). As idele class characters are trivial on the principal ideles and idele class characters of finite order are trivial on the identity component at infinity, we deduce that there are at most h_M^{nar} extensions of a given character of $\widehat{\mathcal{O}}_M^\times$ to a finite-order idele class character of M. Let us write $\varphi^*_{M,c}(\mathfrak{q})$ for the number of characters χ of $\widehat{\mathcal{O}}_M^\times$ of order dividing c and conductor $\mathfrak{q}$, the conductor of a character of $\widehat{\mathcal{O}}_M^\times$ being defined in the same way as for idele class characters. Then the preceding discussion gives

$$h^*_{M,c}(\mathfrak{q}) \leqslant h_M^{\mathrm{nar}} \varphi^*_{M,c}(\mathfrak{q}).$$

Now $\varphi^*_{M,c}$ is multiplicative because $\widehat{\mathcal{O}}_M^\times = \prod_{v\nmid\infty} \mathcal{O}_v^\times$ by (7). Thus

$$\sum_{\mathfrak{q}} h^*_{M,c}(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s} \preccurlyeq_M h_M^{\mathrm{nar}} \prod_{\mathfrak{p}} (\sum_{\nu\geqslant 0} \varphi^*_{M,c}(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s}), \tag{8}$$

where $\mathfrak{p}$ runs over the nonzero prime ideals of $\mathcal{O}_M$.

We now focus on the Euler factor in (8) corresponding to a particular prime ideal $\mathfrak{p}$. Let v be the corresponding place of M and p the residue characteristic of $\mathfrak{p}$. We consider cases according as $p|c$ or $p \nmid c$. In both cases we use the fact that if $\nu \geqslant 2$ then $\varphi^*_{K,c}(\mathfrak{p}^\nu)$ is the number of characters of $\mathcal{O}_v^\times$ of order dividing c which factor through $\mathcal{O}_v^\times/(1+\mathfrak{p}^\nu\mathcal{O}_v)$ but not through $\mathcal{O}_v^\times/(1+\mathfrak{p}^{\nu-1}\mathcal{O}_v)$.

Suppose first that $p \nmid c$. Then any character of $\mathcal{O}_v^\times$ of order dividing c is trivial on the pro-p-group $1+\mathfrak{p}\mathcal{O}_v$. Hence if $\nu \geqslant 2$ then $\varphi^*_{M,c}(\mathfrak{p}^\nu) = 0$. Furthermore

$$\varphi^*_{M,c}(\mathfrak{p}) = \gcd(c, \mathbf{N}\mathfrak{p} - 1) - 1$$

because $\mathcal{O}_v^\times/(1+\mathfrak{p}\mathcal{O}_v)$ is cyclic and the trivial character of $\mathcal{O}_v^\times$ does not have conductor $\mathfrak{p}$. In particular we have $\varphi^*_{M,c}(\mathfrak{p}) \leqslant c-1$, whence

$$\sum_{\nu\geqslant 0} \varphi^*_{M,c}(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s} \preccurlyeq_M 1 + (c-1)(\mathbf{N}\mathfrak{p})^{-s}.$$

Therefore

$$\sum_{\nu\geqslant 0} \varphi^*_{M,c}(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s} \preccurlyeq_M (1 + (\mathbf{N}\mathfrak{p})^{-s})^{c-1} \tag{9}$$

by the binomial theorem.

Next suppose that $p|c$. If $k \geqslant e(\mathfrak{p})/(p-1)+1$ then every element of $1+c\mathfrak{p}^k\mathcal{O}_v$ is a cth power (cf. [2], p. 186). In particular, every element of $1+c\mathfrak{p}^{e(\mathfrak{p})+1}\mathcal{O}_v$ is a cth power. It follows that $\varphi^*_{M,c}(\mathfrak{p}^\nu\mathcal{O}_v)=0$ for $\nu \geqslant e(\mathfrak{p})(v_p(c)+1)+1$. Now for $1 \leqslant \nu \leqslant e(\mathfrak{p})(v_p(c)+1)$ we apply the trivial estimate

$$\varphi^*_{M,c}(\mathfrak{p}^\nu) \leqslant |\mathcal{O}_v^\times/(1+\mathfrak{p}^\nu\mathcal{O}_v)|.$$

Since $|\mathcal{O}_v^\times/(1+\mathfrak{p}^\nu\mathcal{O}_v)| = (\mathbf{N}\mathfrak{p})^{\nu-1}(\mathbf{N}\mathfrak{p}-1) \leqslant (\mathbf{N}\mathfrak{p})^\nu$, we obtain

$$\sum_{\nu\geqslant 0}\varphi^*_{M,c}(\mathfrak{p}^\nu)(\mathbf{N}\mathfrak{p})^{-\nu s} \preccurlyeq_M \sum_{\nu=0}^{e(\mathfrak{p})(v_p(c)+1)} (\mathbf{N}\mathfrak{p})^{\nu(1-s)}. \tag{10}$$

This completes our discussion of the individual Euler factors in (8).

Now combine (8), (9), and (10). We obtain

$$\sum_{\mathfrak{q}} h^*_{M,c}(\mathfrak{q})(\mathbf{N}\mathfrak{q})^{-s} \preccurlyeq_M h_M^{\mathrm{nar}} \cdot \prod_{p\nmid c}\prod_{\mathfrak{p}|p}(1+(\mathbf{N}\mathfrak{p})^{-s})^{c-1}\cdot E_{M,c}(s) \tag{11}$$

We may weaken the estimate in (11) by extending the product over $p \nmid c$ to a product over all p, and then we use the identity

$$\zeta_M(s)/\zeta_M(2s) = \prod_{\mathfrak{p}}(1+(\mathbf{N}\mathfrak{p})^{-s}).$$

Making this substitution in (11), we obtain Proposition 1.

References

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

[2] S. Lang, *Algebraic Number Theory*