Almost abelian Artin representations of Q

ALMOST ABELIAN ARTIN REPRESENTATIONS OF $\mathbb{Q}$

DAVID E. ROHRLICH

Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. All number fields considered here are understood to be subfields of $\overline{\mathbb{Q}}$. We write $\mathbb{Q}^{\mathrm{ab}}$ for the maximal abelian extension of $\mathbb{Q}$ and $\mathbb{Q}^{\mathrm{aa}}$ for the maximal almost abelian extension, the latter being defined as the compositum of all finite Galois extensions K of $\mathbb{Q}$ such that the commutator subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ is central of exponent dividing 2. Note that $\mathbb{Q}^{\mathrm{ab}} \subset \mathbb{Q}^{\mathrm{aa}}$. Anderson [1] has proved the following beautiful complement to the Kronecker-Weber theorem:

$$\mathbb{Q}^{\mathrm{aa}} = \mathbb{Q}^{\mathrm{ab}}(\{\sqrt[4]{\ell} : \ell \text{ prime}\} \cup \{\sqrt{t_{p,q}} : p, q \text{ prime},\ p < q\}), \tag{1}$$

where if p is odd then $t_{p,q} = s_{p,q}/s_{q,p}$ with

$$s_{p,q} = \prod_{j=1}^{(p-1)/2} \left(\frac{\sin(\pi j/p)}{\prod_{k=0}^{(q-1)/2} \sin(\pi(j+pk)/(pq))} \right)$$

while if $p = 2$ then

$$t_{p,q}^{-1} = 2^{q/2} \left(\prod_{k=0}^{(q-1)/2} \sin(\pi \frac{1+4k}{4q}) \right) \left(\prod_{j=1}^{(q-1)/2} \frac{\sin(\pi j/q)\sin(\pi(2j-1)/(2q))}{\sin(\pi j/(2q))\sin(\pi(2j-1)/(4q))} \right).$$

Although we have departed from Anderson's notation slightly, our $t_{p,q}$ nonetheless coincides with Anderson's $\sin \mathbf{a}_{pq}$.

In this note we use Anderson's work to establish a connection between *almost abelian Artin representations* of $\mathbb{Q}$ – in other words, Artin representations of $\mathbb{Q}$ which factor through $\mathrm{Gal}(\mathbb{Q}^{\mathrm{aa}}/\mathbb{Q})$ – and *Hecke-Shintani representations.* The latter term refers to two-dimensional irreducible monomial Artin representations of $\mathbb{Q}$ which can be induced from more than one quadratic field. The intended allusion is to Shintani's work [12] on Stark's conjecture, which rests on the fact that certain irreducible two-dimensional Artin representations of $\mathbb{Q}$ induced from real quadratic fields can also be induced from imaginary quadratic fields, making it possible to deduce Stark's conjecture in such cases from the Kronecker limit formula. But Shintani himself credits Hecke ([12], p. 158): "A coincidence of an L-series of a real quadratic field with an L-series of an imaginary quadratic field was first observed by Hecke." In any case, we shall see that Hecke-Shintani representations are precisely the *two-dimensional* irreducible almost abelian Artin representations of $\mathbb{Q}$. The connection is in fact somewhat broader:

Theorem 1. *Every irreducible almost abelian Artin representation of* $\mathbb{Q}$ *occurs in a tensor product of Hecke-Shintani representations.*

Here we regard an individual Hecke-Shintani representation as a tensor product with one factor. Our main result is actually a bit more precise than Theorem 1 and includes a uniqueness statement (Theorem 2 in Section 5), but the more precise version depends on the notion of an *AHS representation*: Roughly speaking, an AHS representation is a Hecke-Shintani representation directly tied to Anderson's description (1) of $\mathbb{Q}^{\mathrm{aa}}$. The definition will be given in Section 5, but the point to emphasize here is that the class of AHS representations has been thoroughly studied by Bae, Hu, and Yin [2], who not only construct such representations explicitly but also compute their Artin conductors and characters in some cases. (See also Yin and C. Zhang [13] and Yin and Q. Z. Zhang [14] for the algebraic number theory underlying the constructions in [2].) In principle, the proof of the key technical result of the present work (Proposition 12 in Section 4) could be replaced by an appeal to [2], but for the reader's convenience we have included a simple self-contained argument proving just what we need.

Returning to Theorem 1 itself, we would like to emphasize that even as it stands, it is not a purely group-theoretic assertion: The analogous statement for abstract groups is false. That said, much of the proof does amount to elementary group theory of a sort that is well known in principle, at least in the context of Heisenberg groups. This material occupies the first three sections of the paper. Then in Sections 4 and 5 we deduce our main theorem from Anderson's results. We also give a criterion for a tensor product of Hecke-Shintani representations to be irreducible.

Section 6 consists of two remarks. The first concerns Rankin-Selberg convolutions: If ρ is a Hecke-Shintani representation and $\rho^\vee$ the dual representation, then

$$L(s,\rho\otimes\rho^\vee)=\zeta(s)L(s,\chi)L(s,\chi')L(s,\chi''), \tag{2}$$

where χ, χ', and χ'' are certain primitive quadratic Dirichlet characters associated to ρ. While (2) is just a simple group-theoretic observation, it has the following amusing consequence: If f is the primitive cusp form of weight 1 attached to a Hecke-Shintani representation of odd determinant then the Petersson norm of f can be calculated explicitly via the Dirichlet class number formula. We shall see that (2) actually characterizes Hecke-Shintani representations among all two-dimensional irreducible Artin representations of $\mathbb{Q}$.

Our second remark is a footnote to Serre's results on lacunarity [11]. Fix an Artin representation ρ of $\mathbb{Q}$ such that 0 is a value of the character of ρ, and write $L(s,\rho)=\sum_{n\geqslant 1}a_n n^{-s}$. Let $\vartheta(x)$ be the number of $n\leqslant x$ such that $a_n\neq 0$. Serre proves that

$$\vartheta(x)\sim cx/\log^\alpha x \tag{3}$$

with $c,\alpha>0$ ([11], p. 237, Théorème 3.4). In fact he proves something much stronger, namely that (3) can be replaced by an asymptotic expansion involving arbitrarily high powers of $1/\log x$. But the focus here will be on (3), and specifically on the exponent α. Serre observes that if the image of ρ is the dihedral group of order 8 then $\alpha=3/4$. (See [11], pp. 240 – 241, where the discussion involves the modular form $\Delta^{1/12}(12z)$ – note that Serre refers to the same paper of Hecke [7] cited by Shintani.) The footnote to be added here is that $\alpha=3/4$ for all Hecke-Shintani representations and that they are again characterized by this property among two-dimensional irreducible Artin representations of $\mathbb{Q}$.

In the final section of the paper we classify the finite groups G which can arise as $\mathrm{Gal}(L/\mathbb{Q})$, where L is the fixed field of the kernel of a Hecke-Shintani representation. It turns out that up to a cyclic direct factor of odd order, G is either the dihedral or quaternion group of order 8 or else belongs to one of two infinite families which can be described explicitly. This classification could probably also be deduced from [2], where generators and relations are given for some closely related Galois groups.

It is a great pleasure to thank the referee for a careful reading of the paper, for several thoughtful comments, and especially for drawing my attention to [2], of which I had not been aware. I am also grateful to Henri Darmon for pointing out to me that Hecke-Shintani representations appear (although not by that name) in work of Darmon, Rotger, and Zhao (see [4], Proposition 3.2, part (4)). The term *Hecke-Shintani representation* was introduced in [8], and the underlying group-theoretic property figures prominently in a paper of Schmidt and Turki [9], who refer to an abstract group representation of the relevant type as *triply imprimitive*. This useful terminology is adopted here with a slight modification. Finally, it is important to recognize the contributions of Das [5] and Seo [10], whose work was fundamental to the development of Anderson's theory.

1. Almost abelian groups

Throughout this note, G denotes a finite group, $Z(G)$ its center, and $[G,G]$ its commutator subgroup. By the *exponent* of G we mean the minimal exponent, in other words the smallest positive integer e such that $g^e = 1$ for all $g \in G$. Following Anderson [1], we say that G is *almost abelian* if $[G,G]$ is contained in $Z(G)$ and of exponent 1 or 2. The case of exponent 1 ensures that abelian groups are almost abelian. One readily verifies that subgroups, quotient groups, and finite direct products of almost abelian groups are almost abelian.

Proposition 1. *If G is an almost abelian group then $G \cong P \times A$, where P is an almost abelian 2-group and A is abelian of odd order.*

Proof. Since $[G,G] \subset Z(G)$, we see that G is nilpotent, hence isomorphic to the product of its Sylow subgoups. Thus $G \cong P \times A$ with P as above and A almost abelian of odd order. As the exponent of $[A,A]$ is odd and divides 2, it equals 1. (I am indebted to the referee for this simple argument.) □

Proposition 2. *If $[G,G]$ has order $\leqslant 2$ then G is almost abelian. Conversely, if G is almost abelian with cyclic center then $[G,G]$ has order $\leqslant 2$.*

Proof. The first assertion follows from the fact that normal subgroups of order $\leqslant 2$ are central, and the second from the fact that cyclic groups have order equal to their exponent. □

For any finite group G we can consider the isoclinism pairing

$$\langle *,* \rangle : G/Z(G) \ \times \ G/Z(G) \longrightarrow [G,G] \tag{4}$$

given by $\langle aZ(G), bZ(G)\rangle = aba^{-1}b^{-1}$ (cf. [3], p. xxiii). An easy calculation shows that if $[G,G] \subset Z(G)$ – in particular, if G is almost abelian – then (4) is $\mathbb{Z}$-bilinear, but even without this assumption, (4) is nondegenerate in the sense that if for some $a \in G$ we have $\langle aZ(G), bZ(G)\rangle = 1$ for all $b \in G$ then $a \in Z(G)$. We shall be interested in the case where

$$G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^{2m} \tag{5}$$

for some integer $m \geqslant 0$. If G satisfies (5) then we put $m(G) = m$. The following example (Heisenberg groups over $\mathbb{F}_2$) shows that for each positive integer m there exists an almost abelian group G such that (5) holds with $m(G) = m$.

Example. Put $n = m+2$ and let $G \subset \mathrm{GL}_n(\mathbb{F}_2)$ be the subgroup $1+W$, where 1 is the $n \times n$ identity matrix and W is the additive group of $n \times n$ matrices (w_{ij}) over $\mathbb{F}_2$ such that $w_{ij} = 0$ unless either $i = 1$ and $2 \leqslant j \leqslant n$ or $j = n$ and $1 \leqslant i \leqslant n-1$. Let $\omega \in G$ be the element with 1's on the diagonal and in the upper right-hand corner and 0's elsewhere. Then $Z(G) = \{1, \omega\}$ and (5) holds, and G is almost abelian by the following proposition:

Proposition 3. *If* (5) *holds then G is almost abelian. Conversely, if G is almost abelian with cyclic center then* (5) *holds.*

Proof. Suppose that (5) holds. Then $G/Z(G)$ is abelian, so given $a, b \in G$ there exists $z \in Z(G)$ such that $aba^{-1} = bz$. Iterating, we find that $a^2ba^{-2} = bz^2$. On the other hand, $a^2 \in Z(G)$, so $a^2ba^{-2} = b$. Thus $z^2 = 1$. In summary, for all $a, b \in G$ we have $aba^{-1}b^{-1} \in Z(G)$ and $(aba^{-1}b^{-1})^2 = 1$, so G is almost abelian.

Conversely, suppose that G is almost abelian with cyclic center. If G is abelian, then (5) holds with $m = 0$. Otherwise, Proposition 2 gives $[G, G] = \{1, \omega\}$ with $\omega \in Z(G)$. We claim that for any $a \in G$ we have $a^2 \in Z(G)$, or in other words $a^2ba^{-2} = b$ for all $b \in G$. This is obvious if $aba^{-1} = b$, so suppose that $aba^{-1}b^{-1} = \omega$. Write this equation as a conjugation: $aba^{-1} = \omega b$. Iterating the conjugation, we obtain $a^2ba^{-2} = b$, because $\omega^2 = 1$.

We have just seen that $G/Z(G)$ has exponent 2. It follows that $G/Z(G)$ is abelian (which is obvious anyway, since $[G, G] \subset Z(G)$). Thus $G/Z(G)$ is a vector space over $\mathbb{F}_2$. Since $[G, G] = \mathbb{F}_2$ as an abelian group, (4) defines a nondegenerate symplectic pairing on the $\mathbb{F}_2$-vector space $G/Z(G)$, and (5) follows. □

2. Almost abelian representations

Throughout, a *representation* of a finite group G is a finite-dimensional complex representation of G. Similarly, a *character* of G is a complex character of G, denoted $\mathrm{tr}\,\rho$ if ρ is the underlying representation, and a *one-dimensional character* is a homomorphism $G \to \mathbb{C}^\times$. When there is no risk of confusion we often refer to a one-dimensional character simply as a character. If ρ is an irreducible representation of G then we also speak of the *central character* of G, which is the one-dimensional character of G giving the action of $\rho|Z(G)$ by scalar multiplication. If H is a subgroup of G and ξ is a one-dimensional character of H then $\mathrm{ind}_H^G\xi$ denotes the representation of G induced by ξ, and if H is normal in G and $g \in G$ then ξ^g is the character of H given by $\xi^g(h) = \xi(g^{-1}hg)$ for $h \in H$.

Suppose that H is normal in G, and put $\rho = \mathrm{ind}_H^G\xi$. Then

$$\rho|H = \oplus_{g \bmod H}\xi^g, \tag{6}$$

where g runs over a set of representatives for the distinct cosets of H in G, and ρ is irreducible if and only if $\xi^g \neq \xi$ for $g \in G \smallsetminus H$ (Mackey's criterion). In particular, if ρ is irreducible then H contains $Z(G)$. Note also that if ρ is faithful then H is abelian, because (6) gives an embedding of H in the product of $[G : H]$ copies of $\mathbb{C}^\times$. These facts will be used frequently in what follows.

Proposition 4. *Let G be almost abelian with cyclic center. If ρ is an irreducible representation of G of dimension > 1 then there exists a one-dimensional character χ of G of odd order such that $\rho \otimes \chi$ is faithful.*

Proof. By Proposition 1 we may assume that $G = P \times C$, where P is an almost abelian 2-group and C is *cyclic* of odd order as $Z(G) = Z(P) \times C$. Since the restriction of ρ to $Z(G)$ and in particular to C is scalar, we can choose a character χ of C such that $(\rho|C)\otimes\chi$ is a faithful representation of C. Viewing χ as a character of G trivial on P, we claim that $\rho\otimes\chi$ is faithful.

First we show that $\rho\otimes\chi$ is faithful on $Z(G)$. Since $|Z(P)|$ and $|C|$ are relatively prime and $(\rho\otimes\chi)|C$ is faithful by construction, it suffices to see that $(\rho\otimes\chi)|Z(P)$ is faithful. But $(\rho\otimes\chi)|Z(P) = \rho|Z(P)$, and as ρ is irreducible of dimension > 1 it does not factor through $G/[G,G]$. Thus if we write $[G,G] = [P,P] = \{1,\omega\}$ (Proposition 2) then $\rho(\omega) \neq 1$. As ω is the element of order 2 in the cyclic 2-group $Z(P)$, it follows that $\rho|Z(P)$ is indeed faithful.

To complete the proof, take $g \in G \smallsetminus Z(G)$; we must show that $(\rho\otimes\chi)(g) \neq 1$. Since (4) is nondegenerate, there exists $h \in G$ such that $ghg^{-1}h^{-1} = \omega$. So if $(\rho\otimes\chi)(g) = 1$ then $(\rho\otimes\chi)(\omega) = 1$, a contradiction since $\chi|P = 1$ and $\rho(\omega) \neq 1$. □

Proposition 5. *Let G be an almost abelian group. Then $Z(G)$ is cyclic if and only if G has a faithful irreducible representation.*

Proof. We may assume that G nonabelian; otherwise the proposition is immediate. If $Z(G)$ is cyclic, choose any irreducible representation ρ of G of dimension > 1; then $\rho\otimes\chi$ is faithful for some character χ of G by Proposition 4. Conversely, suppose that G has an irreducible representation ρ which is faithful. Then $\rho|Z(G)$ is faithful also, so by Schur's lemma ρ provides an embedding of $Z(G)$ in $\mathbb{C}^\times$. But a finite subgroup of $\mathbb{C}^\times$ is cyclic. □

If G is almost abelian and $Z(G)$ is cyclic then (5) holds by Proposition 3. Recall that we then write $m(G)$ for the integer m in (5). If in addition G is nonabelian then $[G,G] \cong \mathbb{F}_2$ by Proposition 2, whence (4) makes $G/Z(G)$ into a symplectic vector space over $\mathbb{F}_2$. A subspace W of dimension m such that $\langle w, w'\rangle = 0$ for all $w, w' \in W$ is a *maximal isotropic subspace* of $G/Z(G)$.

Proposition 6. *Let G be an almost abelian group with cyclic center, and let ρ be an irreducible representation of G of dimension > 1. Then ρ is monomial of dimension 2^m, where $m = m(G)$. In fact given a subgroup H of G there exists a one-dimensional character ξ of H such that $\rho = \mathrm{ind}_H^G\xi$ if and only if H contains $Z(G)$ and $H/Z(G)$ is a maximal isotropic subspace of $G/Z(G)$.*

Proof. Let H be the inverse image in G of a maximal isotropic subspace of $G/Z(G)$. Then H is an abelian normal subgroup of index 2^m in G, and we claim that $\rho = \mathrm{ind}_H^G\xi$, where ξ is any one-dimensional character of H occurring in $\rho|H$. To verify the claim, take $g \in G \smallsetminus H$; it suffices to show that $\xi^g \neq \xi$. As H is the inverse image of a *maximal* isotropic subspace of $G/Z(G)$, there exists $h \in H$ such that $ghg^{-1}h^{-1} \neq 1$, and consequently $ghg^{-1} = \omega h$, where ω is the nonidentity element of $[G,G]$. But ρ is irreducible of dimension > 1 and thus does not factor through $G/[G,G]$. Furthermore $\rho|Z(G)$ is scalar. Thus $\rho(\omega) = -1$ and $\xi^g(h) = -\xi(h)$. It follows that $\xi^g \neq \xi$, whence $\rho = \mathrm{ind}_H^G\xi$.

Now let H be any subgroup of G such that $\rho = \mathrm{ind}_H^G\xi$ for some character ξ of H. Then H contains $Z(G)$, because ρ is irreducible. Thus H is the inverse image of a subgroup W of $G/Z(G)$; in particular, H is normal in G, and therefore (6) holds. If ρ is faithful then it follows that H is abelian, whence W is isotropic and in fact maximal isotropic since the index of W in $G/Z(G)$ is 2^m. If ρ is not faithful then by Proposition 4 there exists a character χ of G such that $\rho\otimes\chi$ is faithful. Since

$\rho \otimes \chi \cong \mathrm{ind}_H^G(\xi \cdot \chi|H)$, we see that (6) holds with ρ replaced by $\rho \otimes \chi$ and ξ by $\xi \cdot \chi|H$. As before, we conclude that H is abelian and W maximal isotropic. □

Remark. It follows that if $m(G) > 1$ then there are no irreducible two-dimensional representations of G at all. It is in this sense that Theorem 1 is not a purely group-theoretic statement.

Proposition 7. *Let G be an almost abelian group and ρ a faithful irreducible representation of G. Then* $\mathrm{tr}\,\rho(g) = 0$ *if and only if* $g \in G \smallsetminus Z(G)$.

Proof. It suffices to prove that if $g \notin Z(G)$ then $\mathrm{tr}\,\rho(g) = 0$, for the converse is obvious. In particular, the theorem is vacuous for G is abelian, so we may assume that $\dim(\rho) > 1$. Note also that $Z(G)$ is cyclic by Proposition 5. So suppose that $g \notin Z(G)$. Then $gZ(G) \neq 0$ in $G/Z(G)$, so there exists a maximal isotropic subspace $W \subset G/Z(G)$ such that $gZ(G) \notin W$. By Proposition 6 the inverse image H of W in G is a subgroup such that $\rho = \mathrm{ind}_H^G \xi$ for some one-dimensional character ξ of H. Since H is normal in G and $g \notin H$ we conclude that $\mathrm{tr}\,\rho(g) = 0$. □

Finally we come to an elementary analogue of the theorem of Stone and von Neumann. The version below differs from statements in the literature in at most a few details. It is the key group-theoretic input to the proof of Theorem 1:

Proposition 8. *Suppose that J is almost abelian, and let ρ and ρ' be irreducible representations of J with respective central characters φ and φ'. If*

$$\varphi|[J, J] = \varphi'|[J, J]$$

then $\rho' \cong \rho \otimes \chi$ for some one-dimensional character χ of J.

Proof. First let χ be any one-dimensional character of J, and consider the sum

$$s(\chi) = \frac{1}{|J|} \sum_{j \in J} \chi(j) \mathrm{tr}\,\rho(j) \overline{\mathrm{tr}\,\rho'(j)}. \tag{7}$$

As $\rho \otimes \chi$ and ρ' are irreducible the right-hand side of (7) is 1 if $\rho \otimes \chi \cong \rho'$ and 0 otherwise. Thus it will suffice to show that for some χ we have $s(\chi) \neq 0$.

Put $G = J/\ker\rho$ and $G' = J/\ker\rho'$, and let $\pi : J \to G$ and $\pi' : J \to G'$ be the quotient maps. Then we can write $\rho = \varrho \circ \pi$ and $\rho' = \varrho' \circ \pi'$ with faithful irreducible representations ϱ and ϱ' of G and G' respectively. Applying Proposition 7 to ϱ and ϱ', we see that $\mathrm{tr}\,\rho(j)\mathrm{tr}\,\rho'(j) = 0$ unless $\pi(j) \in Z(G)$ and $\pi'(j) \in Z(G')$. Hence (7) becomes

$$s(\chi) = \frac{1}{|J|} \sum_{h \in H} \chi(h) \mathrm{tr}\,\rho(h) \overline{\mathrm{tr}\,\rho'(h)} \tag{8}$$

with $H = \pi^{-1}(Z(G)) \cap (\pi')^{-1}(Z(G'))$.

Since π and π' are surjective, $Z(J) \subset H$. We claim that φ and φ' can be extended to characters of H. Indeed let ϕ and ϕ' be the central characters of ϱ and ϱ'. Then $\varphi = \phi \circ \pi$ and $\varphi' = \phi' \circ \pi'$ on $Z(J)$, and we can take these same equations as defining extensions of φ and φ' to H. Equation (8) is now

$$s(\chi) = \frac{(\dim\rho)(\dim\rho')}{|J|} \sum_{h \in H} \chi(h)\varphi(h)\overline{\varphi'(h)}, \tag{9}$$

because $\rho|H$ and $\rho'|H$ are scalar multiplication by φ and φ' respectively.

We now choose χ. Since $[J,J]$ is a subgroup of $Z(J)$ and *a fortiori* of H, we can view $\overline{\varphi}\varphi'$ as a one-dimensional character of $H/[J,J]$. But $H/[J,J]$ is a subgroup of the abelian group $J/[J,J]$, so we can extend $\overline{\varphi}\varphi'$ to a character χ of $J/[J,J]$. Viewing χ as a character of J trivial on $[J,J]$, we see that the summand on the right-hand side of (9) is identically 1, whence $s(\chi) > 0$ and in particular $s(\chi) \neq 0$. □

3. Triply monomial representations

We now specialize to the case $m = 1$. We say that an irreducible two-dimensional representation of a finite group G is *triply monomial* if it can be induced from exactly three subgroups of index 2 in G. As mentioned in the introduction, this is a slight modification of the terminology in [9].

Although triply monomial representations are not required to be faithful, one can always reduce to the faithful case, for if ρ is a triply monomial representation of G with kernel K then the representation $\overline{\rho}$ of G/K afforded by ρ is also triply monomial. Indeed if H and H' are distinct index-two subgroups of G from which ρ can be induced, then H and H' contain K and H/K and H'/K are distinct index-two subgroups of G/K from which $\overline{\rho}$ can be induced, and conversely.

Proposition 9. *Let ρ be a faithful irreducible two-dimensional representation of a finite group G. The following are equivalent:*

(i) *G is almost abelian.*
(ii) *ρ is triply monomial.*
(iii) *ρ can be induced from more than one subgroup of index 2 in G.*

If these equivalent conditions hold and if H and H' are distinct subgroups of index 2 in G from which ρ can be induced, then the third such subgroup is the subgroup containing $H \cap H'$ which is of index 2 in G and not equal to H or H'; furthermore, $Z(G) = H \cap H'$.

Proof. The implication (i) $\Rightarrow$ (ii) follows from Propositions 5 and 6, given that in a two-dimensional symplectic vector space every one-dimensional subspace is maximal isotropic. The implication (ii) $\Rightarrow$ (iii) is trivial. To prove that (iii) implies (i), we merely rework the proof of Proposition 5 of [8], which asserts that (iii) implies (ii). Let H and H' be distinct subgroups of index 2 in G from which ρ can be induced, and write

$$G/(H \cap H') \cong G/H \ \times \ G/H' \cong (\mathbb{Z}/2\mathbb{Z})^2. \tag{10}$$

Let h and h' be representatives for the nontrivial coset of $H \cap H'$ in H and H' respectively. Then h, h' and hh' represent the nontrivial cosets of $H \cap H'$ in G, and consequently G is generated by h, h', and $H \cap H'$. Since h and h' both centralize $H \cap H'$ – for as ρ is faithful both H and H' are abelian – we see that $H \cap H' \subset Z(G)$, whence $H \cap H' = Z(G)$ (else $Z(G)$ has index two in G and G is abelian). Thus (10) gives (5) and (i) follows from Proposition 3. At the same time we have proved the final assertion of the proposition. □

The following proposition provides an alternative characterization:

Proposition 10. *Let G be a finite group, H a subgroup of index 2, and ξ a one-dimensional character of H, and suppose that the representation $\rho = \mathrm{ind}_H^G \xi$ is faithful and irreducible. Then ρ is triply monomial if and only if ξ^2 extends to a character of G.*

Proof. Suppose that ρ is triply monomial, so that G is almost abelian by Proposition 9. Then $(aba^{-1}b^{-1})^2 = 1$ for any $a, b \in G$, and consequently $\xi^2(aba^{-1}b^{-1}) = 1$ (note that $[G, G] \subset H$ since G/H is abelian). So ξ^2 factors through the subgroup $H/[G, G]$ of the abelian group $G/[G, G]$ and therefore extends to a character of G.

Conversely, suppose that χ is an extension of ξ^2 to G. Then $\chi(a^{-1}ba) = \chi(b)$ for $a, b \in G$. Taking $b = h \in H$, we see that $\xi(a^{-1}h^2a) = \xi(h^2)$. Replacing a first by ag and then by g, where $g \in G \smallsetminus H$, we also find that $\xi^g(a^{-1}h^2a) = \xi^g(h^2)$. Since ρ is faithful and $\rho|H = \xi \oplus \xi^g$, we deduce that $a^{-1}h^2a = h^2$. In other words, if $h \in H$ then $h^2 \in Z(G)$. So $H/Z(G)$ is an abelian subgroup of $G/Z(G)$ of exponent 2 and index 2.

To complete the argument, view ρ as an irreducible representation $G \to \mathrm{GL}_2(\mathbb{C})$. Then we may identify $G/Z(G)$ with a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$, hence with the dihedral group D_{2n} of order $2n$ ($n \geqslant 2$) or with A_4, S_4 or A_5. But the last three groups do not have abelian subgroups of index 2, and D_{2n} has an abelian subgroup of index 2 and exponent 2 only if n is 2 or 4. If $n = 2$ then (5) holds with $m = 1$ and G is almost abelian by Proposition 3, hence ρ is triply monomial by Proposition 9. Thus we may assume that $G/Z(G) \cong D_8$.

If $H/Z(G)$ is cyclic then it is of order 2, for its exponent is 2. Since $[G : H] = 2$ it follows that $|G/Z(G)| = 4$, a contradiction. Therefore $H/Z(H)$ is not cyclic. But D_8 has a cyclic subgroup of index 2, hence so does $G/Z(G)$. Thus there is a subgroup H' of G containing $Z(G)$ with $H'/Z(G)$ cyclic of index 2 in $G/Z(G)$. The cyclicity of $H'/Z(G)$ ensures that H' is an *abelian* subgroup of index 2, and since $\rho|H'$ is nonscalar (for ρ is faithful and $Z(G)$ is a *proper* subgroup of H'), ρ is induced from H'. By assumption, ρ is also induced from H, but $H \neq H'$ because $H/Z(G)$ is not cyclic. Thus ρ is triply monomial by Proposition 9. □

Finally, we note that the class of triply monomial representations is closed under dualization and one-dimensional twists:

Proposition 11. *If ρ is a triply monomial representation of a finite group G and χ is a one-dimensional character of G then both $\rho^\vee$ and $\rho \otimes \chi$ are triply monomial.*

Proof. For each subgroup H of index 2 in G such that $\rho = \mathrm{ind}_H^G \xi$ with a character ξ of H, we have $\rho^\vee = \mathrm{ind}_H^G \xi^{-1}$ and $\rho \otimes \chi = \mathrm{ind}_H^G \xi'$ with $\xi' = \xi \cdot \chi|H$. □

4. Hecke-Shintani representations

Given a profinite group Γ, we write $Z(\Gamma)$ for its center, $[\Gamma, \Gamma]$ for its commutator subgroup, and $[\Gamma, \Gamma]^{\mathrm{cl}}$ for the closure of $[\Gamma, \Gamma]$. A *representation* of Γ is a continuous homomorphism $\Gamma \to \mathrm{GL}(V)$, where V is a finite-dimensional vector space over $\mathbb{C}$. Such a homomorphism is trivial on an open subgroup of Γ and so can be viewed as a representation of a finite group G. In particular, if $K \subset \overline{\mathbb{Q}}$ is a number field, then an *Artin representation* of K can be viewed either as a continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}(V)$ or as a representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$ for some finite Galois extension L of K. Via the latter alternative, terms pertaining to representations of finite groups carry over to Artin representations. We say that ρ is *almost abelian* if its image is an almost abelian group and *triply monomial* if it is two-dimensional and irreducible and can be induced from exactly three quadratic extensions of K. A *Hecke-Shintani representation* is a triply monomial Artin representation of $\mathbb{Q}$.

A word of caution is in order. Let Γ be a profinite group and G the quotient of Γ by an open subgroup. While the quotient map $\Gamma \to G$ is surjective, its restriction $Z(\Gamma) \to Z(G)$ may not be, so if ρ is an irreducible representation of Γ which factors through G then the domain of the central character of ρ is open to interpretation. We intend the more restrictive interpretation, in other words $Z(\Gamma)$ or its image in $Z(G)$. However starting in the next paragraph, we specialize to a setting where $[\Gamma,\Gamma]^{\mathrm{cl}} \subset Z(\Gamma)$, and from that point on the central character of ρ will appear primarily via its restriction to $[\Gamma,\Gamma]^{\mathrm{cl}}$. The surjectivity of $[\Gamma,\Gamma]^{\mathrm{cl}} \to [G,G]$ then eliminates any possibility of confusion.

Indeed, from now on we take $\Gamma = \mathrm{Gal}(\mathbb{Q}^{\mathrm{aa}}/\mathbb{Q})$ and put

$$\Omega = \mathrm{Gal}(\mathbb{Q}^{\mathrm{aa}}/\mathbb{Q}^{\mathrm{ab}}) = [\Gamma,\Gamma]^{\mathrm{cl}}.$$

To verify that $\Omega \subset Z(\Gamma)$, let G be a quotient of Γ by an open subgroup, and let $\lambda : \Gamma \to G$ be the quotient map. Then $\lambda(\Omega) \subset [G,G]$, and since G is almost abelian it follows that $\lambda(\Omega) \subset Z(G)$. Since G is arbitrary we obtain $\Omega \subset Z(\Gamma)$.

It follows from (1) that Ω is an abelian group of exponent 2, and even though it is written multiplicatively, we shall view it as a vector space over $\mathbb{F}_2$. The same goes for $\widehat{\Omega}$, where the hat denotes Pontryagin dual. In fact the proof of our main result depends on the choice of an explicit basis for $\widehat{\Omega}$ over $\mathbb{F}_2$. Let U be the subset of $\mathbb{Q}^{\mathrm{ab}}$ consisting of the numbers $\sqrt{\ell}$ for each prime number ℓ and the numbers $t_{p,q}$ for each ordered pair of prime numbers (p,q) with $p < q$. Anderson's theory gives not only (1) but also the linear independence over $\mathbb{F}_2$ of the cosets in $\mathbb{Q}^{\mathrm{ab}\times}/(\mathbb{Q}^{\mathrm{ab}\times})^2$ represented by the elements $u \in U$. Thus putting $\Omega_u = \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}(\sqrt{u})/\mathbb{Q}^{\mathrm{ab}})$, we have

$$\Omega \cong \prod_{u \in U} \Omega_u \tag{11}$$

by Kummer theory, whence

$$\widehat{\Omega} \cong \oplus_{u \in U} \widehat{\Omega_u} \tag{12}$$

on passing to Pontryagin duals. We use the identifications (11) and (12) as follows: For each $u_0 \in U$, we define $\sigma_{u_0} \in \Omega$ by demanding that σ_{u_0} map to the nontrivial element of Ω_u for $u = u_0$ and the trivial element otherwise. And we define $\psi_{u_0} \in \widehat{\Omega}$ by the condition that $\psi_{u_0}(\sigma_u) = -1$ if $u = u_0$ and $\psi_{u_0}(\sigma_u) = 1$ otherwise. The set $\{\psi_{u_0} : u_0 \in U\}$ is the desired basis for $\widehat{\Omega}$. The key step in the proof of our main theorem is now the following:

Proposition 12. *Given $u \in U$, there exists a Hecke-Shintani representation ρ such that the associated central character φ satisfies $\varphi|\Omega = \psi_u$.*

Proof. There are two cases to consider: Either $u = \sqrt{\ell}$ for some prime ℓ, or $u = t_{p,q}$ with primes $p < q$.

Suppose first that $u = \sqrt{\ell}$, and put $L = \mathbb{Q}(\sqrt[4]{\ell}, i)$, so that the group $G = \mathrm{Gal}(L/\mathbb{Q})$ is dihedral of order 8. Thus G satisfies (5) with $m = 1$, and hence the irreducible two-dimensional representation ρ of G (unique up to isomorphism) is a Hecke-Shintani representation. Furthermore $L = K(\sqrt{u})$, where $K = L \cap \mathbb{Q}^{\mathrm{ab}}$ $(= \mathbb{Q}(\sqrt{\ell}, i))$. It follows that when ρ is viewed as a representation of Γ, its central character coincides with ψ_u on Ω.

Next suppose that $u = t_{p,q}$ with $p < q$. Let $K = \mathbb{Q}(e^{2\pi i/(4pq)})$, so that

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times, \tag{13}$$

if p is odd and

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times, \tag{14}$$

if $p = 2$. Let $t \in \mathbb{Q}^{\mathrm{ab}\times}$ be the number denoted $\sin \mathbf{a}$ on p. 467 of [1]. Then t represents the same coset as $t_{p,q}$ modulo $(\mathbb{Q}^{\mathrm{ab}\times})^2$ but has the additional virtue that the field $L = K(\sqrt{t})$ is Galois over $\mathbb{Q}$. Actually if p is odd then we can dispense with t, because Das has shown that $K(\sqrt{t_{p,q}})$ is itself Galois over $\mathbb{Q}$ ([5], p. 3576, Theorem 11), but I do not know whether the same is true for $p = 2$. In any case, $\mathbb{Q}^{\mathrm{ab}}L = \mathbb{Q}^{\mathrm{ab}}(\sqrt{u})$ and $L \cap \mathbb{Q}^{\mathrm{ab}} = K$, whence $J = \mathrm{Gal}(L/\mathbb{Q})$ is nonabelian and thus has an irreducible representation ρ of dimension > 1. But $\rho|\mathrm{Gal}(L/K)$ is nontrivial, else ρ factors through the abelian group $\mathrm{Gal}(K/\mathbb{Q})$. Thus it is again the case that when ρ is viewed as a representation of Γ, its central character coincides with ψ_u on Ω. It remains only to see that $\dim(\rho) = 2$. Let M be the fixed field of the kernel of ρ, and put $G = \mathrm{Gal}(M/Q)$. Then G is a quotient of J, so $G/[G,G]$ is a quotient of $J/[J,J]$, or in other words of $\mathrm{Gal}(K/\mathbb{Q})$. As $[G,G] \subset Z(G)$ it follows that $G/Z(G)$ is a quotient of $\mathrm{Gal}(K/\mathbb{Q})$. But inspecting both (13) and (14), we see that $\mathrm{Gal}(K/\mathbb{Q})$ can be generated by 3 elements. Hence so can $G/Z(G)$. Referring to (5), we see that $m(G) = 1$, so $\dim(\rho) = 2$ by Proposition 6. □

5. Proof of the main theorem

We call a Hecke-Shintani representation ρ an *AHS representation* if the restriction to Ω of the central character of ρ coincides with one of the characters ψ_u for $u \in U$. Furthermore, we say that a list of AHS representations $\rho_1, \rho_2, \dots, \rho_n$ is *independent* if the corresponding characters $\psi_{u_1}, \psi_{u_2}, \dots, \psi_{u_n}$ are linearly independent as elements of the vector space $\widehat{\Omega}$. Equivalently, $\rho_1, \rho_2, \dots, \rho_n$ are independent if $u_1, u_2, \dots, u_n$ are distinct elements of U.

Theorem 2. *Let ρ be an irreducible almost abelian Artin representation of $\mathbb{Q}$ of dimension greater than one. Then there exist independent AHS representations $\rho_1, \rho_2, \dots, \rho_n$ such that ρ occurs in $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$. Furthermore, if $\rho'_1, \rho'_2, \dots, \rho'_{n'}$ are also independent AHS representations such that ρ occurs in $\rho'_1 \otimes \rho'_2 \otimes \cdots \otimes \rho'_{n'}$, then $n' = n$ and there is a permutation β of $\{1, 2, \dots, n\}$ such that $\rho'_{\beta(j)} \cong \rho_j \otimes \chi_j$ with one-dimensional characters χ_j of Γ satisfying $\chi_1\chi_2 \cdots \chi_n = 1$ on $Z(\Gamma)$.*

Proof. Let φ be the central character of ρ. By Proposition 12, there exist independent AHS representations $\rho_1, \rho_2, \dots, \rho_n$ with respective central characters $\varphi_1, \varphi_2, \dots, \varphi_n$ such that

$$\varphi_1\varphi_2 \cdots \varphi_n|\Omega = \varphi|\Omega. \tag{15}$$

The restriction of $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ to $Z(\Gamma)$ is scalar, given by $\varphi_1\varphi_2 \cdots \varphi_n$, and thus if π is an irreducible constituent of $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ then the central character of π is $\varphi_1\varphi_2 \cdots \varphi_n$. Let $M \subset \mathbb{Q}^{\mathrm{aa}}$ be a finite Galois extension of $\mathbb{Q}$ such that π and ρ both factor through $\mathrm{Gal}(M/\mathbb{Q})$. Taking account of (15) and applying Proposition 8 with $J = \mathrm{Gal}(M/\mathbb{Q})$, we deduce that $\rho \cong \pi \otimes \chi$ for some one-dimensional character of Γ. Thus ρ occurs in $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n \otimes \chi$. But $\rho_n \otimes \chi$ is itself a Hecke-Shintani representation by Proposition 11. Furthermore, when restricted to Ω the central characters of ρ_n and $\rho_n \otimes \chi$ are equal, because χ is trivial on Ω. So after replacing

ρ_n by $\rho_n \otimes \chi$ we obtain independent AHS representations with the property that ρ occurs in their tensor product.

Next we prove the uniqueness statement. Let φ_j and φ'_i be the central characters of ρ_j and ρ'_i respectively, and write $\varphi_j|\Omega = \psi_{u_j}$, $\varphi'_i|\Omega = \psi_{u'_i}$. Then

$$\prod_{i=1}^{n'} \psi_{u'_i} = \prod_{j=1}^{n} \psi_{u_j}, \tag{16}$$

because both sides coincide with the restriction to Ω of the central character of ρ. In view of the distinctness of $u_1, \ldots, u_n$, the distinctness of $u'_1, \ldots, u'_{n'}$, and the linear independence of the ψ_u for $u \in U$, we deduce from (16) that $n = n'$ and that $u'_{\beta(j)} = u_j$ for some permutation β of $\{1, 2, \ldots, n\}$. Applying Proposition 8 again, we conclude that $\rho'_{\beta(j)} \cong \rho_j \otimes \chi_j$ for some one-dimensional characters χ_j of Γ. Finally, since $\varphi_1\varphi_2 \ldots \varphi_n$ and $\varphi'_1\varphi'_2 \ldots \varphi'_n$ both coincide with the central character of ρ they coincide with each other. But

$$\varphi'_{\beta(j)} = (\chi_j|Z(\Gamma))\varphi_j,$$

so $\chi_1\chi_2 \cdots \chi_n|Z(\Gamma) = 1$. □

Remark. It is not hard to see that $Z(\Gamma) = \mathrm{Gal}(\mathbb{Q}^{\mathrm{aa}}/\mathbb{Q}^{\mathrm{qu}})$, where $\mathbb{Q}^{\mathrm{qu}}$ is the compositum of all quadratic extensions of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$.

Theorem 1 follows from Theorem 2 and a silly remark:

Proposition 13. *Every one-dimensional character of Γ occurs in a tensor product of two Hecke-Shintani representations.*

Proof. Let ρ be any Hecke-Shintani representation. Since ρ is irreducible, the trivial character occurs in $\rho \otimes \rho^\vee$, so χ occurs in $(\rho \otimes \chi) \otimes \rho^\vee$. Now use Proposition 11. □

Next we prove two results complementary to Theorems 1 and 2. The first is implicit already in the proof of Theorem 2.

Proposition 14. *If $\rho_1, \rho_2, \ldots, \rho_n$ are Hecke-Shintani representations and ρ and ρ' are irreducible representations occurring in $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$, then $\rho' \cong \rho \otimes \chi$ for some one-dimensional character χ of Γ.*

Proof. If $\varphi_1, \varphi_2, \ldots, \varphi_n$ are the central characters of $\rho_1, \rho_2, \ldots, \rho_n$ and φ and φ' are those of ρ and ρ', then then φ and φ' both coincide with $\varphi_1\varphi_2 \ldots \varphi_n$, hence with each other. In particular, $\varphi|\Omega = \varphi'|\Omega$, and an appeal to Proposition 8 completes the proof. □

The second complement is a criterion for a tensor product of Hecke-Shintani representations to be irreducible. First we prove a lemma.

Lemma. *Let G be a finite group and H a subgroup such that the quotient map $H \to G/Z(G)$ is surjective. Then the irreducible representations of H are precisely the restrictions to H of the irreducible representations of G.*

Proof. The hypothesis means that $G = H \cdot Z(G)$. If ρ is an irreducible representation of G then $Z(G)$ acts by scalars, so an H-stable subspace of the space of ρ is also G-stable. Hence the irreducibility of ρ gives that of $\rho|H$. Conversely, if ρ is an irreducible repesentation of H then the restriction of ρ to $H \cap Z(G)$ is scalar, given by a character φ of $H \cap Z(G)$. After extending φ to a character of $Z(G)$, we extend ρ to G by setting $\rho(zh) = \varphi(z)\rho(h)$ for $z \in Z(G)$ and $h \in H$. □

To state our criterion for irreducibility, we make two definitions, the first of which is standard for $n = 2$ but perhaps less so for $n > 2$: We say that finite Galois extensions $K_1, K_2, \ldots, K_n$ of $\mathbb{Q}$ are *linearly disjoint* over $\mathbb{Q}$ if

$$[K : \mathbb{Q}] = \prod_{j=1}^{n} [K_j : \mathbb{Q}], \tag{17}$$

where $K = K_1 K_2 \cdots K_n$. For the second definition, let ρ be a Hecke-Shintani representation, viewed as a faithful representation of $G = \mathrm{Gal}(L/\mathbb{Q})$ for some finite Galois extension L of $\mathbb{Q}$. From (5) it follows that the fixed field K of $Z(G)$ is a biquadratic field, and we call K the biquadratic field *associated* to ρ.

Proposition 15. *A tensor product of Hecke-Shintani representations is irreducible if and only if the associated biquadratic fields are linearly disjoint over* $\mathbb{Q}$.

Proof. Let $\rho_1, \rho_2, \ldots, \rho_n$ be Hecke-Shintani representations, let $K_1, K_2, \ldots, K_n$ be the associated biquadratic fields, and let $L_1, L_2, \ldots, L_n$ be the fixed fields of the respective kernels. We put $\rho = \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ and write $K = K_1 K_2 \cdots K_n$ and $L = L_1 L_2 \cdots L_n$.

Suppose first that $K_1, K_2, \ldots, K_n$ are linearly disjoint over $\mathbb{Q}$. Put

$$G = \prod_{j=1}^{n} \mathrm{Gal}(L_j/\mathbb{Q})$$

and let H be the image in G of the product of the restriction maps

$$\mathrm{Gal}(L/\mathbb{Q}) \to \prod_{j=1}^{n} \mathrm{Gal}(L_j/\mathbb{Q}). \tag{18}$$

We claim that the hypothesis of the lemma is satisfied. Indeed the center of a product is the product of the centers, and $Z(\mathrm{Gal}(L_j/\mathbb{Q})) = \mathrm{Gal}(L_j/K_j)$, so

$$G/Z(G) = \prod_{j=1}^{n} \mathrm{Gal}(K_j/\mathbb{Q}_j).$$

Thus to check the hypothesis of the lemma we must verify that the composition of (18) with

$$\prod_{j=1}^{n} \mathrm{Gal}(L_j/\mathbb{Q}) \to \prod_{j=1}^{n} \mathrm{Gal}(K_j/\mathbb{Q})$$

is surjective. But this composition factors through $\mathrm{Gal}(K/\mathbb{Q})$ to give

$$\mathrm{Gal}(K/\mathbb{Q}) \to \prod_{j=1}^{n} \mathrm{Gal}(K_j/\mathbb{Q}),$$

which is clearly injective, hence surjective by (17). Thus the lemma implies that the irreducible representations of $\mathrm{Gal}(L/\mathbb{Q})$ are precisely the pullbacks of those of G. But because G is a product, its irreducible representations are the external tensor products of irreducible representations of the factors; consequently ρ is an irreducible representation of $\mathrm{Gal}(L/\mathbb{Q})$.

Conversely, suppose that ρ is irreducible. We observe that for $g \in \mathrm{Gal}(L/\mathbb{Q})$, $\mathrm{tr}\,\rho(g) = 0$ if and only if $\mathrm{tr}\,\rho_j(g) = 0$ for some j, hence if and only if $g \notin \mathrm{Gal}(L/K_j)$ for some j (Proposition 7). Hence $\mathrm{tr}\,\rho(g) = 0$ if and only if $g \notin \mathrm{Gal}(L/K)$. Let M

be the fixed field of the kernel of ρ. Then $K \subset M$, for if $g \in \mathrm{Gal}(L/\mathbb{Q})$ and $g|K$ is nontrivial then $\mathrm{tr}\,\rho(g) = 0$, whence $\rho(g) \neq 1$. Putting $G = \mathrm{Gal}(M/\mathbb{Q})$ and viewing ρ as a faithful irreducible representation of G, we see in fact (appealing to Proposition 7 again) that K is the fixed field of $Z(G)$. Therefore $[K : \mathbb{Q}] = [G : Z(G)]$. Now Propositions 5 and 3 imply that $[G : Z(G)] = 2^{2m}$ for some m, and then $\dim(\rho) = 2^m$ by Proposition 6. But $\dim(\rho) = 2^n$, because ρ is the tensor product of n two-dimensional representations. Thus $m = n$ and consequently

$$[K : \mathbb{Q}] = [G : Z(G)] = 2^{2m} = 2^{2n}.$$

Formula (17) follows. □

6. Two characterizations of Hecke-Shintani representations

We come now to the characterizations mentioned in the introduction. The first one pertains to Rankin-Selberg convolutions and depends on the proposition below. For a finite group G let reg_G denote the regular representation of G. We say that a representation of G is *abelian* if its image is abelian, or equivalently, if it is a direct sum of one-dimensional characters.

Proposition 16. *Let ρ be a faithful two-dimensional irreducible representation of a finite group G, and let $\rho^\vee$ be the dual representation. The tensor product $\rho \otimes \rho^\vee$ is abelian if and only if ρ is triply monomial. Furthermore, if these equivalent conditions hold, then $\rho \otimes \rho^\vee \cong \mathrm{reg}_A$, where $A = G/Z(G)$ and reg_A is viewed as a representation of G.*

Proof. If $\rho \otimes \rho^\vee$ is abelian then it is trivial on $[G, G]$, whence $\rho|[G, G]$ is reducible – otherwise the multiplicity of the trivial representation in $(\rho \otimes \rho^\vee)|[G, G]$ would be 1, not 4. So $\rho|[G, G] = \psi \oplus \psi'$ with two one-dimensional characters ψ and ψ' of $[G, G]$. If $\psi \neq \psi'$ then $\psi^{-1}\psi'$ is a nontrivial character occurring in $\rho \otimes \rho^\vee$, contradiction. So $\psi = \psi'$ and $\rho|[G, G]$ is scalar. Since ρ is faithful it follows that $[G, G] \subset Z(G)$ and hence that $G/Z(G)$ is abelian (but not cyclic, else G is abelian). If we view ρ as giving an embedding of G in $\mathrm{GL}_2(\mathbb{C})$ and hence of $G/Z(G)$ in $\mathrm{PGL}_2(\mathbb{C})$, then the classification of finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ shows that $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Therefore G is almost abelian by Proposition 3, and then Proposition 9 shows that ρ is triply monomial.

Conversely, suppose that ρ is triply monomial, and write $\rho = \mathrm{ind}_H^G \xi$ with a subgroup H of index two in G and a one-dimensional character ξ of H. Then $\rho|H \cong \xi \oplus \xi^g$ for any $g \in G \smallsetminus H$, and therefore $\rho^\vee|H = \xi^{-1} + (\xi^g)^{-1}$. Consequently

$$\rho \otimes \rho^\vee \cong \mathrm{ind}_H^G(\xi \otimes (\xi^{-1} \oplus (\xi^g)^{-1})).$$

The right-hand side is $(\mathrm{ind}_H^G 1) \oplus (\mathrm{ind}_H^G \xi(\xi^g)^{-1})$. Furthermore $\mathrm{ind}_H^G 1 \cong 1 \oplus \chi$, where χ is the character of G with kernel H, so we deduce that χ occurs in $\rho \otimes \rho^\vee$. But ρ is triply monomial, whence we can redo the calculation with H replaced by the other two subgroups of index two from which ρ can be induced, say H' and H''. Let χ' and χ'' be the characters of G with kernel H' and H'' respectively. Then χ, χ', and χ'' all occur in $\rho \otimes \rho^\vee$, as does the trivial character of G. Since $\rho \otimes \rho^\vee$ has dimension 4 we conclude that

$$\rho \otimes \rho^\vee \cong 1 \oplus \chi \oplus \chi' \oplus \chi''.$$

Thus $\rho \otimes \rho^\vee$ is abelian and in fact coincides with reg_A by Proposition 9. □

For a number field K let $\zeta_K(s)$ denote the Dedekind zeta function of K.

Corollary 1. *Let ρ be a two-dimensional irreducible Artin representation of $\mathbb{Q}$. There is a factorization of $L(s, \rho \otimes \rho^\vee)$ of the form*

$$L(s, \rho \otimes \rho^\vee) = \zeta(s)L(s, \chi)L(s, \chi')L(s, \chi'')$$

with primitive Dirichlet characters χ, χ', and χ'' if and only if ρ is a Hecke-Shintani representation. The characters χ, χ', and χ'' are then quadratic, corresponding to the three quadratic subfields of the biquadratic field K associated to ρ. Thus $L(s, \rho \otimes \rho^\vee) = \zeta_K(s)$.

Proof. If ρ is a Hecke-Shintani representation then the factorization is an immediate consequence of Proposition 16 and the Artin formalism for L-functions. Conversely, suppose that the stated factorization holds, and suppose that p is a prime not dividing the conductor of ρ. Let $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at p. Examining the coefficient of p^{-s} on both sides of the factorization, we find

$$\mathrm{tr}\,(\rho \otimes \rho^\vee)(\sigma_p) = 1 + \chi(\sigma_p) + \chi'(\sigma_p) + \chi''(\sigma_p).$$

Since Frobenius elements are dense in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and a representation is determined up to isomorphism by its character, it follows that

$$\rho \otimes \rho^\vee \cong 1 \oplus \chi \oplus \chi' \oplus \chi''.$$

Hence Proposition 16 implies that ρ is a Hecke-Shintani representation. □

The second characterization depends on the following proposition:

Proposition 17. *Let ρ be a two-dimensional irreducible representation of a finite group G, and let $C \subset G$ be the subset of elements $g \in G$ such that $\mathrm{tr}\,\rho(g) \neq 0$. Then $|C|/|G| \geqslant 1/4$, with equality if and only if ρ is triply monomial.*

Proof. We may assume without loss of generality that ρ is faithful. Now

$$\frac{1}{|G|}\sum_{g\in G} |\mathrm{tr}\,\rho(g)|^2 = 1 \tag{19}$$

by the orthogonality relations, and the summation can be restricted to $g \in C$. Furthermore, since $\dim(\rho) = 2$ we have $|\mathrm{tr}\,\rho(g)| \leqslant 2$ with equality if and only if the two eigenvalues of $\rho(g)$ are equal. The latter condition means that $\rho(g)$ is scalar, or equivalently (since ρ is faithful and irreducible) that $g \in Z(G)$. Thus the left-hand side of (19) is $\leqslant 4|C|/|G|$, with equality if and only if $C = Z(G)$. It remains to prove that $C = Z(G)$ if and only if ρ is triply monomial.

That $C = Z(G)$ if ρ is triply monomial follows from Propositions 9 and 7. Conversely, suppose that $C = Z(G)$. Then for $g \in G \smallsetminus Z(G)$ the eigenvalues of $\rho(g)$ are λ and $-\lambda$, say, and consequently $\rho(g^2)$ is scalar. Since ρ is faithful it follows that $g^2 \in Z(G)$. Thus the group $G/Z(G)$ has exponent 2 and is therefore abelian, hence of the form $(\mathbb{Z}/2\mathbb{Z})^k$ for some k. It follows that $|Z(G)|/|G| = 2^{-k}$; but we are assuming that $Z(G) = C$, and we have already seen that $|C|/|G| = 1/4$. So $k = 2$. We conclude that G is almost abelian by Proposition 3, whence ρ is triply monomial by Proposition 9. □

Now suppose that ρ is a two-dimensional irreducible Artin representation of $\mathbb{Q}$, let M be the fixed field of the kernel of ρ, and put $G = \mathrm{Gal}(M/\mathbb{Q})$. Let C be the subset of $g \in G$ for which $\mathrm{tr}\,\rho(g) \neq 0$, and put $\alpha = 1 - |C|/|G|$. We assume that $C \neq G$, so that $\alpha > 0$. Write $L(s, \rho) = \sum_{n\geqslant 1} a_n n^{-s}$, and as in the introduction, let $\vartheta(x)$ be the number of $n \leqslant x$ such that $a_n \neq 0$. Serre has shown that $\vartheta(x) \sim cx/\log^\alpha x$ with $c > 0$ ([11], pp. 237–238). Hence Proposition 17 implies:

Corollary 2. *The exponent* α *satisfies* $\alpha \leqslant 3/4$*, with equality if and only if* ρ *is a Hecke-Shintani representation.*

7. Almost abelian groups of degree two

We shall classify the almost abelian groups with a faithful irreducible representation of dimension 2. If G is such a group then Propositions 5 and 6 imply that $Z(G)$ is cyclic and $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Conversely, if G is a finite group such that $Z(G)$ is cyclic and $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then G is almost abelian by Proposition 3, and from Proposition 6 it follows that G has an a two-dimensional irreducible representation, which may be assumed faithful by Proposition 4. Thus our task is simply to classify finite groups G such that $Z(G)$ is cyclic and $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$. By Proposition 1, we can restrict our attention to 2-groups with these properties.

Let D_8 and Q_8 be the dihedral and quaternion groups of order 8, and for $k \geqslant 4$ put

$$N_{2^k} = \langle a, b | a^{2^{k-1}} = b^2 = 1,\ bab = a^{2^{k-2}+1} \rangle \tag{20}$$

and

$$DT_{2^k} = \langle z, a, b | z^{2^{k-2}} = a^2 = b^2 = 1,\ aza = bzb = z,\ bab = z^{2^{k-3}} a \rangle. \tag{21}$$

The "N" in N_{2^k} stands for "nameless": The standard classification of nonabelian 2-groups having a cyclic subgroup of index 2 (cf. Huppert [6], p. 91) lists four infinite families, of which three get names; (20) does not. As for (21), among the groups with a faithful triply monomial representation, the groups DT_{2^k} are the only ones which are "triply generated" in the sense that they can be generated by 3 elements but not 2. Thus they are "doubly triple."

Proposition 18. *Up to isomorphism, the almost abelian* 2*-groups with a faithful irreducible representation of dimension* 2 *are* D_8, Q_8, N_{2^k}*, and* DT_{2^k}*, where* $k \geqslant 4$.

Proof. It is easy to see that if G is one of these groups then $Z(G)$ is cyclic and $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Conversely, suppose that G satisfies these conditions, and assume first that G has a cyclic subgroup of index 2. Then G belongs to one of the four infinite families mentioned above: Either G is a dihedral, hence isomorphic to

$$D_{2^k} = \langle a, b | a^{2^{k-1}} = b^2 = 1,\ bab = a^{-1} \rangle$$

for $k \geqslant 3$, or G is a generalized quaternion group, hence isomorphic to

$$Q_{2^k} = \langle a, b | a^{2^{k-1}} = 1,\ a^{2^{k-2}} = b^2,\ bab^{-1} = a^{-1} \rangle$$

for $k \geqslant 3$, or G is quasidihedral, hence isomorphic to

$$QD_{2^k} = \langle a, b | a^{2^{k-1}} = b^2 = 1,\ bab = a^{2^{k-2}-1} \rangle$$

for $k \geqslant 4$, or $G \cong N_{2^k}$ for $k \geqslant 4$. However if G is D_{2^k}, Q_{2^k}, or QD_{2^k} and $k \geqslant 4$ then $|Z(G)| = 2$ and thus $|Z(G)| < |G|/4$, whence $G/Z(G) \not\cong (\mathbb{Z}/2\mathbb{Z})^2$. Hence only D_8, Q_8, and N_{2^k} $(k \geqslant 4)$ are almost abelian of degree 2.

Next suppose that G does not have a cyclic subgroup of index 2, and fix a generator z of $Z(G)$. Since $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$, we see that if $g \in G \setminus Z(G)$ then g^2 does not generate $Z(G)$, else g generates a cyclic subgroup of index 2 in G. Hence $g^2 = z^{2n}$ for some $n \in \mathbb{Z}$, and consequently $(gz^{-n})^2 = 1$. Thus the nonidentity cosets of $Z(G)$ in G all have representatives of order 2. Choose two such representatives, say a and b, for distinct nonidentity cosets of $Z(G)$. Writing $\langle x \rangle$ for the cyclic group generated by an element x, we see that

$$G \cong (Z(G) \times \langle a \rangle) \rtimes \langle b \rangle. \tag{22}$$

If $|G| = 8$ then G is isomorphic to D_8. Otherwise $|G| > 8$, and by considering the possible actions of $\langle b \rangle$ on $Z(G) \times \langle a \rangle$ we see that $G \cong DT_{2^k}$ for some $k \geqslant 4$. $\square$

References

[1] G. W. Anderson, *Kronecker-Weber plus epsilon*, Duke Math. J. 114 (2002), 439 – 475.

[2] S. Bae, Y. Hu, and L. Yin, *Artin L-functions and modular forms associated to quasi-cyclotomic fields*, Acta Arith. 143 (2010), 59 – 80.

[3] J. H. Conway, R. T. Curtis, S.P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford (1985).

[4] H. Darmon, V. Rotger, and Y. Zhao, *The Birch and Swinnerton-Dyer conjecture for Q-curves and Oda's period relations* In: Geometry and Analysis of Automorphic Forms of Several Variables, Proceedings of the International Symposium in Honor of Takayuki Oda on the Occasion of his 60th Birthday, Series on Number Theory and its Applications, Vol. 7, Y. Hamahata, T. Ichikawa, A. Murase, and T. Sugano, eds., World Scientific (2012), 1 – 40.

[5] P. Das, *Algebraic gamma monomials and double coverings of cyclotomic fields*, Transactions of the AMS 352 (2000), 3557 – 3594.

[6] B. Huppert *Endliche Gruppen I*, Springer Grundlehren der math. Wissenschaften 134 (1967).

[7] E. Hecke, *Zur Theorie der elliptischen Modulfunktionen*, Math. Annalen 97 (1926), 210 – 242.

[8] D. E. Rohrlich, *Artin representations of* $\mathbb{Q}$ *of dihedral type*, Mathematical Research Letters 22 (2015), 1767 – 1789.

[9] R. Schmidt and S. Turki, *Triply imprimitive representations of* GL(2), Proc. Amer. Math. Soc., to appear.

[10] S. Seo, *A note on algebraic* Γ*-monomials and double coverings*, J. Number Theory 93 (2002), 76 – 85.

[11] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Enseignement Mathématique 22, (1976), 227 – 260.

[12] T. Shintani, *On certain ray class invariants of real quadratic fields*, J. Math. Soc. Japan 30 (1978), 139 – 167.

[13] L. S. Yin and C. Zhang, *Arithmetic of quasi-cyclotomic fields*, J. Number Theory 128 (2008), 1717 – 1730.

[14] L. S. Yin and Q. Z. Zhang, *All double coverings of cyclotomic fields*, Math. Z. 253 (2006), 479 – 488.

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