MULTIPLICITIES IN MORDELL-WEIL GROUPS

DAVID E. ROHRLICH

ABSTRACT. Let K be a finite Galois extension of $\mathbb{Q}$ and let ρ be an irreducible complex representation of $\mathrm{Gal}(K/\mathbb{Q})$. For an elliptic curve E over $\mathbb{Q}$ let $W(E,\rho)$ be the root number in the functional equation of $L(s,E,\rho)$. We give an example where ρ has dimension 4 and Schur index 1 but $W(E,\rho)=1$ for all E over $\mathbb{Q}$. The image of ρ has order 32.

In recent years, speculation about ranks of elliptic curves over $\mathbb{Q}$ has changed. The constructions by Shafarevich and Tate [38] and by Ulmer [39] of elliptic curves of high rank over function fields may have once encouraged a belief in the abundance of elliptic curves over $\mathbb{Q}$ of high rank, but the current expectation seems to be that the rank of an elliptic curve over $\mathbb{Q}$ is 0 or 1 with probability 1 (the "minimalist conjecture") and that the average rank is 1/2 (the "average rank conjecture"). See for example [1], [2], [3], [4], [5], [6], [16], [18] [20], [21], [26], [27], [28], [29], [36], [40], and many other works. The goal of the present work is to sound a cautionary note regarding a possible extension of these conjectures to Artin representations.

Here an Artin representation of $\mathbb{Q}$ is understood as usual to be a continuous homomorphism $\beta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$, where V is a finite-dimensional vector space over $\mathbb{C}$ and $\overline{\mathbb{Q}}$ is some fixed algebraic closure of $\mathbb{Q}$ which is taken to contain all number fields under discussion. In practice we usually identify β with a representation of $\mathrm{Gal}(K/\mathbb{Q})$ for some finite Galois extension K of $\mathbb{Q}$ such that β is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Such a representation will be called an Artin representation also. In fact suppose that we start with a finite Galois extension K of $\mathbb{Q}$. Then for every elliptic curve E over $\mathbb{Q}$ we can consider the natural action of $\mathrm{Gal}(K/\mathbb{Q})$ on the Mordell-Weil group $E(K)$. This action gives rise to a representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C}\otimes E(K)$, where the tensor product is taken over $\mathbb{Z}$, and if ρ is an irreducible representation of $\mathrm{Gal}(K/\mathbb{Q})$ over $\mathbb{C}$, then we can speak of the multiplicity of the Artin representation ρ in $\mathbb{C}\otimes E(K)$. We denote this multiplicity $\langle \rho, E\rangle$.

Henceforth we assume that ρ is self-dual. If ρ has odd dimension or nontrivial determinant then at least conjecturally, there is always an elliptic curve E over $\mathbb{Q}$ such that $\langle \rho, E\rangle$ is odd (cf. [32], p. 338, Prop. 11). However for certain self-dual ρ of even dimension and trivial determinant it can happen that $\langle E, \rho\rangle$ is even for every elliptic curve E over $\mathbb{Q}$. This phenomenon is transparent in some instances and less so in others, as we shall now explain.

Transparent examples are afforded by ρ with absolute Schur index $m(\rho) > 1$. Indeed the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C}\otimes E(K)$ is naturally a representation by matrices with coefficients in $\mathbb{Q}$ (even in $\mathbb{Z}$), and therefore $m(\rho)$ divides $\langle \rho, E\rangle$. For example, let Q denote the quaternion group of order 8, and suppose that $\mathrm{Gal}(K/\mathbb{Q}) \cong Q$. Take ρ to be the two-dimensional irreducible representation of $\mathrm{Gal}(K/\mathbb{Q})$, unique up to isomorphism. Then ρ is symplectic, and consquently $m(\rho) = 2$. Hence $\langle \rho, E\rangle$ is even for every elliptic curve E over $\mathbb{Q}$. This assertion is

nonvacuous in the sense that for a given ρ there does exist an E such that ρ occurs in $\mathbb{C} \otimes E(K)$ (see [30], p. 129, Prop. 3 for an elementary construction).

Our less transparent examples are inferences from root numbers based on the Birch-Swinnertion-Dyer conjecture. Here we are following a tradition that starts with Birch and Stephens [7] in 1966 and has since grown to encompass root numbers of abelian varieties of arbitrary dimension. See for example [8], [9], [10], [11], [12], [13], [17], [22], [23], [24], [34] and many other papers. Let $L(s, E, \rho)$ be the tensor-product L-function associated to E and ρ, and let $W(E, \rho)$ be the root number associated to $L(s, E, \rho)$, or rather to the local Weil-Deligne representations $\sigma'_{E/\mathbb{Q}_p} \otimes \rho_p$ underlying $L(s, E, \rho)$, where $p \leqslant \infty$ and the notation is as in [31] or [32]. The precise conjectural statement on which our examples depend is that if ρ is self-dual then

$$W(E, \rho) = (-1)^{\langle \rho, E \rangle}. \tag{1}$$

In general, (1) depends not only on the Birch-Swinnerton-Dyer conjecture but also on the Deligne-Gross conjecture ([14] p. 323, Conjecture 2.7(ii)). However the ρ which will be our primary focus happens to be realizable over $\mathbb{Q}$, and for such ρ one can dispense with the Deligne-Gross conjecture (see the proof of Proposition 2 of [30], p. 127). In any case, our goal is to present an example of a ρ, necessarily of even dimension and trivial determinant, with the property that $W(E, \rho) = 1$ for all elliptic curves E over $\mathbb{Q}$, even though $m(\rho) = 1$.

Such examples are not new. For instance let D_n be the dihedral group of order $2n$, and consider a Galois extension K of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong D_q \times D_r \times D_s \times D_t$, where q, r, s, and t are distinct primes $\geqslant 5$. Then for any faithful irreducible representation ρ of $\mathrm{Gal}(K/\mathbb{Q})$ we have $W(E, \rho) = 1$ for all E over $\mathbb{Q}$ despite the fact that $m(\rho) = 1$ (cf. [32], p. 313, Prop. D). However even with the minimal choices of q, r, s, and t we are dealing with a group of order $2^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 80080$ and a representation of dimension 16. These numbers are too big for us to obtain a nonvacuity result comparable to part (i) of the following theorem:

Theorem 1. *Let L and L' be Galois extensions of $\mathbb{Q}$ with*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L'/\mathbb{Q}) \cong Q$$

and with relatively prime discriminants. Put $K = LL'$ and let ρ be the irreducible four-dimensional representation of $\mathrm{Gal}(K/\mathbb{Q})$, unique up to isomorphism. Then $m(\rho) = 1$ and the following assertions hold:

(i) *There exists an elliptic curve E over $\mathbb{Q}$ such that ρ occurs in $\mathbb{C} \otimes E(K)$. In fact there exist infinitely many such elliptic curves with pairwise distinct j-invariants.*
(ii) *$W(E, \rho) = 1$ for every elliptic curve E over $\mathbb{Q}$.*

In particular, if the Birch-Swinnerton-Dyer conjecture holds, then it follows that $\langle \rho, E \rangle$ is even for every elliptic curve E over $\mathbb{Q}$ and is positive for an infinite set of E with distinct j-invariants.

Although $\mathrm{Gal}(LL'/\mathbb{Q})$ is isomorphic to $Q \times Q$ and is therefore of order 64, the representation ρ factors through a quotient $\mathrm{Gal}(F/\mathbb{Q})$ of $\mathrm{Gal}(LL'/\mathbb{Q})$ of order 32. In group-theoretic parlance and notation, $\mathrm{Gal}(F/\mathbb{Q})$ is the *extraspecial group* 2_+^{1+4}. More to the point, 2_+^{1+4} is a minimal example of the phenomenon at issue: If ρ is an irreducible self-dual representation of a finite group G such that $\dim \rho$ is even,

$\det\rho$ is trivial, and $m(\rho)=1$, then $\dim\rho\geqslant 4$ and $|G|\geqslant 32$. Group-theoretically, the holomorph of the cyclic group of order 8 is another minimal example, but I don't know whether one can prove a theorem similar to Theorem 1 for $\mathrm{Hol}(C_8)$.

Let $1_{\mathbb{Q}}$ denote the one-dimensional trivial representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then the rank of $E(\mathbb{Q})$ coincides with $\langle 1_{\mathbb{Q}}, E\rangle$, so it is easy to imagine an extension of the minimalist conjecture: For any fixed irreducible Artin representation ρ of $\mathbb{Q}$ we have $\langle\rho, E\rangle\leqslant 1$ with probability 1. This conjecture would imply that the set of elliptic curves figuring in part (i) of Theorem 1 is of density 0. But then the average multiplicity of this ρ in an elliptic curve over $\mathbb{Q}$ would be 0, in contrast to the average rank conjecture.

Be that as it may, the ingredients in the proof of Theorem 1 are as follows. For part (i), we apply a recent theorem of Suresh [37] about the general realization problem for Galois representations in Mordell-Weil groups of abelian varieties. The first statement in (i) also follows from Matsuno [25] and from [33]. Part (ii) uses the classification of groups of order 16 obtained about 130 years ago by Hölder [19] and Young [42] (for a modern treatment see Wild [41], and for a helpful synopsis see the online article "Groups of order 16" by Keith Conrad). Actually, as pointed out by the referee, many of our group-theoretic arguments could be replaced simply by references to online resources. In the end, however, (ii) is not a purely group-theoretic statment but rather an application of the following well-known principle:

Theorem 2. *Let ρ be an Artin representation of $\mathbb{Q}$ such that the restriction of ρ to every decomposition subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is symplectic. Then $W(E,\rho)=1$ for every elliptic curve E over $\mathbb{Q}$.*

The example of $D_q\times D_r\times D_s\times D_t$ mentioned above was treated in [32] by combining the facts underlying Theorem 2 with an explicit formula for local root numbers. By contrast, to prove Theorem 1 we use only Theorem 2. That Theorem 2 suffices may seem paradoxical, because the ρ in Theorem 1 is irreducible *orthogonal* and therefore not itself symplectic. But it will turn out that the restriction of ρ to a decomposition subgroup is always reducible, and a reducible representation can be both orthogonal and symplectic. Indeed if σ is any representation of any group and $\sigma^\vee$ is its dual then $\sigma\oplus\sigma^\vee$ is both orthogonal and symplectic, a fact which will be used repeatedly in the proof of Theorem 1.

After proving Theorem 1 we will recall a criterion of Fröhlich [15] which makes it easy to produce examples of pairs (L,L') satisfying the hypotheses of the theorem. We will also use Fröhlich's criterion to show that in part (ii), the hypothesis that L and L' have relatively prime discriminants cannot simply be replaced by the weaker hypothesis $L\cap L'=\mathbb{Q}$.

We conclude this introduction with some conventions and notations to be used throughout the paper. A *representation* of a finite group G is always a finite-dimensional representation over $\mathbb{C}$, and if G has just one isomorphism class of irreducible representations of some dimension n then we will sometimes refer to a member of that isomorphism class as *the* irreducible representation of G of dimension n. The center and commutator subgroup of G will be denoted $Z(G)$ and $[G,G]$ respectively, and if ρ is an irreducible representation of G then the central character of ρ, which is a homomorphism $Z(G)\to\mathbb{C}^\times$, will be denoted ω_ρ. An *involution* is an element of order 2. The trivial one-dimensional representation of G will be denoted 1_G or simply 1, and if H is a subgroup of G then we write ind_H^G for the induction functor from representations of H to representations of G. If K

is a fixed Galois extension of a number field M and $K \supset L \supset M$ then instead of writing ind_H^G with $G = \mathrm{Gal}(K/M)$ and $H = \mathrm{Gal}(K/L)$ we often write $\mathrm{ind}_{L/M}$, and we may also write 1_L for 1_H.

I thank the referee for several insightful comments and for drawing my attention to the website https://people.maths.bris.ac.uk/∼matyd/GroupNames/ and to the wealth of information it contains.

1. First steps

We begin with the elementary group theory underlying the rest of the paper. The textbook of Serre [35] is an excellent reference.

Write $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ with the usual relations $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, $i^2 = j^2 = k^2 = -1$, and $(-1)^2 = 1$. Elements of the product $Q \times Q$ will be written as ordered pairs (x, y), and the subgroup of order 2 generated by $(-1, -1)$ will be denoted R. The image of (x, y) in the quotient group

$$G = (Q \times Q)/R \tag{2}$$

will be denoted $[x, y]$. The following property of G is easily verified:

Proposition 1. *The elements of order 4 in G are the elements of the form $[\pm h, 1]$ or $[1, \pm h]$ with $h \in \{i, j, k\}$. All other nonidentity elements in G have order 2. In particular, if $g \in G$ is an element of order 4 then $g^2 = [-1, 1] = [1, -1]$.*

Quite generally, if A and B are groups and $\alpha : A \to \mathrm{GL}(U)$ and $\beta : B \to \mathrm{GL}(V)$ are representations of A and B on vector spaces U and V over $\mathbb{C}$, then we write

$$\alpha \boxtimes \beta : A \times B \to \mathrm{GL}(U \otimes V)$$

for the representation given by the formula

$$(\alpha \boxtimes \beta)(a, b) = \alpha(a) \otimes \beta(b) \tag{3}$$

($a \in A$, $b \in B$). In particular, let π be the irreducible two-dimensional representation of Q and put $\rho = \pi \boxtimes \pi$. Then ρ is an irreducible four-dimensional representation of $Q \times Q$ and is the unique such representation up to isomorphism (cf. [35], p. 27, Thm. 10). Since $\omega_\pi(-1) = -1$ it follows that $\rho(-1, -1)$ is trivial. Therefore ρ factors through G, and we shall view ρ as a representation of $Q \times Q$ or of G according to the convenience of the moment.

Proposition 2. *The four-dimensional irreducible representation ρ is orthogonal, with trivial determinant and Schur index one.*

Proof. To see that ρ is orthogonal with $\det \rho = 1$ we view ρ as a representation of $Q \times Q$. Then it is the tensor product $\pi \boxtimes \pi$ of two symplectic representations, hence orthogonal, and since $\det \pi$ is trivial, the triviality of $\det \rho$ follows from the formula

$$\det(\alpha \otimes \beta) = (\det \alpha)^{\dim \beta} (\det \beta)^{\dim \alpha}$$

for α, β as in (3). As for $m(\rho)$, view ρ as a representation of G. We prove below (Proposition 5) that ρ occurs with multiplicity 1 in a representation induced by 1_H for a certain subgroup H of G. Therefore $m(\rho) = 1$. □

It is easily verified that $Z(G) = \{[1, 1], [-1, 1]\}$ and that $\omega_\rho([-1, 1]) = -1$. To illustrate this remark we record a simple fact that will be needed later.

Proposition 3. *Let J be a subgroup of G such that $Z(J)$ contains an element of order 4. Then $\rho|J$ is symplectic.*

Proof. If $g \in Z(J)$ is of order 4 then $g^2 = [-1, 1]$ by Proposition 1, whence $\omega_\rho(g^2) = -1$. It follows that if σ is an irreducible representation of J occurring in $\rho|J$ then $\omega_\sigma(g^2) = -1$, so that $\omega_\sigma(g) = \pm i$. Thus ω_σ is not self-dual, and consequently neither is σ. But ρ is self-dual, so $\rho|J$ is self-dual also. Therefore the multiplicity of σ in $\rho|J$ is the same as the multiplicity of $\sigma^\vee$, whence $\rho|J$ is a direct sum of representations of the form $\sigma \oplus \sigma^\vee$ and is therefore symplectic. □

The center and commutator subgroup of G coincide, just as they do for Q, so the abelianization of G is

$$G/Z(G) \cong (Q \times Q)/(\{\pm 1\} \times \{\pm 1\}) \cong (\mathbb{Z}/2\mathbb{Z})^4. \tag{4}$$

The isomorphism $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^4$ can be described explicitly as an identification of $G/Z(G)$ with the product of the groups of order 2 generated by the cosets of $[i, 1]$, $[j, 1]$, $[1, i]$, and $[1, j]$ modulo $Z(G)$. Equivalently, we have:

Proposition 4. *The cosets of $[i, i]$, $[j, j]$, $[i, 1]$, and $[j, 1]$ modulo $Z(G)$ are a basis for $G/Z(G)$ over $\mathbb{Z}/2\mathbb{Z}$.*

Next observe that the elements of G of the form $[h, h]$ with $h \in \{i, j, k\}$ constitute a set of pairwise commuting involutions. Indeed $(h, h)^2 = (-1, -1)$, and if h and h' are distinct elements of $\{i, j, k\}$ then $(h, h)(h', h') = (-1, -1)(h', h')(h, h)$. Let H be the subgroup of G consisting of the three elements $[h, h]$ with $h \in \{i, j, k\}$ together with the identity, and let Λ be the group of one-dimensional characters of G which are trivial on H. It follows from Proposition 4 that Λ has order 4.

Proposition 5. $\operatorname{ind}_H^G 1_H \cong \rho \oplus (\oplus_{\lambda \in \Lambda} \lambda)$.

Proof. Since $|H| = 4$ and $|\Lambda| = 4$, both sides of the claimed equality have dimension 8. It suffices to see that each of the direct summands on the right-hand side occurs in $\operatorname{ind}_H^G 1_H$, for then it follows by dimension-counting that these summands all occur with multiplicity one and collectively fill up $\operatorname{ind}_H^G 1_H$. Applying Frobenius reciprocity, we are reduced to proving that if φ is a direct summand on the right then 1_H occurs in $\varphi|H$. Now for $\lambda \in \Lambda$, the very definition of Λ ensures that 1_H *equals* $\lambda|H$. So it suffices to see that 1_H occurs in $\rho|H$. This is a consequence of the following poposition. □

Proposition 6. *Let H be a subgroup of G of order 4 such that all nonidentity elements of H are noncentral involutions. Then $\rho|H$ is the regular representation of H.*

Proof. It suffices to to see that the characters of $\rho|H$ and the regular representation are equal:

$$\operatorname{tr} \rho[x, y] = \begin{cases} 4 & \text{if } [x, y] = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Only the second case requires proof. Any noncentral involution has the form $[x, y]$ with $x, y \in \{\pm i, \pm j, \pm k\}$ (Proposition 1). Viewing ρ as a representation of $Q \times Q$, we have $\operatorname{tr} \rho(x, y) = \operatorname{tr}(\pi(x) \otimes \pi(y))$. Since the trace of a tensor product is the product of the traces and $\operatorname{tr} \pi(x) = 0$ for $x \in \{\pm i, \pm j, \pm k\}$, we obtain $\operatorname{tr} \rho(x, y) = \operatorname{tr} \pi(x) \operatorname{tr} \pi(y) = 0$. □

2. Realization in Mordell-Weil groups

We can now deduce part (i) of Theorem 1. Given Galois extensions L and L' of $\mathbb{Q}$ with comprime discriminants and with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L'/\mathbb{Q}) \cong Q$, let $K = LL'$. The coprimality of discriminants ensures that $L \cap L' = \mathbb{Q}$ so that

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(L'/\mathbb{Q}) \cong Q \times Q. \tag{6}$$

While there are many ways to identify $\mathrm{Gal}(L/Q)$ and $\mathrm{Gal}(L'/\mathbb{Q})$ with Q, all identifications match $-1 \in Q$ with the unique element of order 2 in $\mathrm{Gal}(L/Q)$ and $\mathrm{Gal}(L'/\mathbb{Q})$. It follows that the subgroup R of $Q \times Q$ determines a subgroup of order 2 in $\mathrm{Gal}(K/\mathbb{Q})$, so that if F is the corresponding fixed field then

$$\mathrm{Gal}(F/\mathbb{Q}) \cong (Q \times Q)/R = G. \tag{7}$$

Furthermore, since we have identified $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(L'/\mathbb{Q})$ with Q, it is natural to write π and π' for the respective irreducible two-dimensional representations of $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(L'/\mathbb{Q})$ and ρ for the tensor product of π and π'. If ρ is viewed as a representation of $\mathrm{Gal}(K/\mathbb{Q})$ via (6) then the notation $\rho = \pi \boxtimes \pi'$ is natural, but if we think of π and π' as representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ then we must write $\rho = \pi \otimes \pi'$. Either way, ρ is the irreducible four-dimensional representation of $\mathrm{Gal}(F/\mathbb{Q})$. Finally, we can think of the set of elements $[h, h]$ with $h \in \{i, j, k\}$ as a well-defined subset of $\mathrm{Gal}(F/\mathbb{Q})$, because (6) identifies $\mathrm{Gal}(L/\mathbb{Q})$ and $\mathrm{Gal}(L'/\mathbb{Q})$ with Q, hence with each other. Thus we may regard H as a subgroup of $G = \mathrm{Gal}(F/\mathbb{Q})$. Let N be the corresponding fixed field. Then Proposition 5 gives

$$\mathrm{ind}_{N/\mathbb{Q}} 1_N = \rho \oplus (\oplus_{\lambda \in \Lambda} \lambda).$$

Since $[F : \mathbb{Q}] = 32$ and $[F : N] = 4$, we have $[N : \mathbb{Q}] = 8$ and in particular $[N : \mathbb{Q}] \leqslant 10$. Thus part (i) of Theorem 1 follows from Theorem 1.5 of Suresh [37].

3. Local root numbers

Before delving into the proof of part (ii) of Theorem 1, we recall some general facts about root numbers, starting with the expression for the global root number as a product of local root numbers. In particular, if E is any elliptic curve over $\mathbb{Q}$ and ρ any Artin representation of $\mathbb{Q}$ then

$$W(E, \rho) = W(E, \rho_\infty) \prod_p W(E, \rho_p), \tag{8}$$

where p runs over prime numbers. We will not need the definition of the local factors on the right-hand side, which can be found for example in [32], p. 329. What we do need is the definition of ρ_p. Let F be a finite Galois extension of $\mathbb{Q}$ such that ρ factors through $\mathrm{Gal}(F/\mathbb{Q})$. Given p, choose a place v of F above p, let F_v be the completion of F at v, and identify $\mathrm{Gal}(F_v/\mathbb{Q}_p)$ with the decomposition subgroup $\mathbf{D}$ of v in $\mathrm{Gal}(F/\mathbb{Q})$. Then $\rho_p = \rho|\mathbf{D}$. This definition works also in the case $p = \infty$, where $\mathbf{D} = \mathrm{Gal}(F_v/\mathbb{R})$ with $F_v = \mathbb{R}$ or $\mathbb{F}_v \cong \mathbb{C}$.

The main fact needed here is that if ρ_p is symplectic then $W(E, \rho_p) = 1$ (see part (iii) of Prop. 8 on p. 332 of [32]). Therefore Theorem 2 follows from (8), and to prove part (ii) of Theorem 1 it suffices to show:

Theorem 3. *If ρ is as in Theorem 1, then ρ_p is symplectic for all $p \leqslant \infty$.*

But we do not specialize to the ρ in Theorem 1 immediately. Instead we start with a simple but general remark:

Proposition 7. *Let ρ be a self-dual Artin representation of $\mathbb{Q}$ of even dimension and trivial determinant. If ρ is unramified at p or if $p = \infty$ then ρ_p is symplectic.*

Since a decomposition group at an unramified prime or infinity is cyclic, the proof of Proposition 7 reduces to an elementary fact:

Proposition 8. *Let C be a finite cyclic group and ρ a self-dual representation of C of even dimension and trivial determinant. Then ρ is symplectic.*

Proof. Since ρ is self-dual, the multiplicity of a one-dimensional character χ of C in ρ equals the multiplicity of χ^{-1}. If C has odd order then $\chi \neq \chi^{-1}$ for every nontrivial character χ of C, and since $\dim \rho$ is even it follows that the trivial character 1_C has even multiplicity in ρ. Therefore ρ is symplectic. If C has even order then we must check that both 1_C and the unique quadratic character ν of C have even multiplicity in ρ. If this is not the case then since $\dim \rho$ is even both 1_C and ν have odd multiplicity, whence $\det \rho = \nu$, contradicting our hypothesis. □

4. The classification

After these general remarks we return to a setting close to that of Theorem 1. Thus $G = (Q \times Q)/R$ while F is a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \cong G$. But we do not yet assume the existence of a field K as in (6). Our goal is to find the set of subgroups of G which can arise as decomposition subgroups.

If J is any finite group and p any prime number then we say that J is a Galois group over $\mathbb{Q}_p$ if $J \cong \mathrm{Gal}(L/\mathbb{Q}_p)$ for some Galois extension L of $\mathbb{Q}_p$. If J is not a Galois group over $\mathbb{Q}_p$ for any p then in particular it is not a decomposition subgroup of $\mathrm{Gal}(F/\mathbb{Q})$.

Proposition 9. *G is not a Galois group over $\mathbb{Q}_p$ for any p.*

Proof. We have $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong (\mathbb{Z}/2\mathbb{Z})^\nu$ with $\nu = 2$ if $p > 2$ and $\nu = 3$ if $p = 2$. Hence by Kummer theory $(\mathbb{Z}/2\mathbb{Z})^4$ is not a Galois group over $\mathbb{Q}_p$. It follows that G itself is not a Galois group over $\mathbb{Q}_p$, because G has a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$, as we saw in (4). □

Thus any decomposition subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ is a *proper* subgroup, so of order dividing 16. Henceforth we denote the dihedral group of order 8 simply by D.

Proposition 10. *Every proper subgroup of G is isomorphic to a subgroup of one of the following groups:*

(i) $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$
(ii) $Q \rtimes \mathbb{Z}/2\mathbb{Z}$
(iii) $(\mathbb{Z}/2\mathbb{Z})^4$
(iv) $D \times \mathbb{Z}/2\mathbb{Z}$

In (ii)*, let r be the generator of $\mathbb{Z}/2\mathbb{Z}$. Then $rxr^{-1} = ixi^{-1}$ for $x \in Q$.*

Proof. A proper subgroup of a p-group is contained in a subgroup of index p. Hence a proper subgroup of G is contained in a subgroup of order 16, and we may apply the classification of groups of order 16: Up to isomorphism, there are exactly 14 of them. But 6 of these groups have elements of order 8, so if we confine our attention to possible subgroups of G then there are only 8 groups to consider. Four of these groups are the 4 groups listed above, and the other 4 are the groups listed in the next proposition, to which the proof of the present proposition now reduces. □

Proposition 11. *A subgroup of G of order 16 is* not *isomorphic to any of the following groups:*

(i) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
(ii) $(\mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$
(iii) $Q \times \mathbb{Z}/2\mathbb{Z}$
(iv) $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes (\mathbb{Z}/4\mathbb{Z})$

In (ii)*, the action of $(\mathbb{Z}/4\mathbb{Z})$ on $(\mathbb{Z}/4\mathbb{Z})$ is the unique nontrivial action, and in* (iv)*, a generator of $\mathbb{Z}/4\mathbb{Z}$ sends an element $(a, b) \in (\mathbb{Z}/2\mathbb{Z})^2$ to $(a + b, b)$.*

Proof. If $g \in G$ has order 4 then $g^2 = [-1, 1]$ by Proposition 1. This remark rules out the first two groups on the list, because if G has a subgroup of the form $A \times B$ or $A \rtimes B$ with $A \cong B \cong \mathbb{Z}/4\mathbb{Z}$ then A and B both have the element $[-1, 1]$ in common, a contradiction.

Next suppose that G has a subgroup of the form $A \times B$ with $A \cong Q$ and $B \cong \mathbb{Z}/2\mathbb{Z}$. Then A contains two noncommuting elements of order 4. Applying Proposition 1, and then using the fact that the map $[x, y] \mapsto [y, x]$ is an automorphism of G, we may assume that A contains $[i, 1]$ and $[j, 1]$. Now let b be the generator of B. Then $b \neq [-1, 1]$, because $[-1, 1] = [i, 1]^2 \in A$. So b has the form $[h, h']$ with $h, h' \in \{\pm i, \pm j, \pm k\}$. But no such $[h, h']$ commutes with both $[i, 1]$ and $[j, 1]$, a contradiction.

Finally, suppose that G has a subgroup of the form $A \rtimes B$, where $A \cong (\mathbb{Z}/2\mathbb{Z})^2$, $B \cong \mathbb{Z}/4\mathbb{Z}$, and B acts nontrivially on A. Then B contains an element of order 4, and after appealing to Proposition 1 again and applying the automorphism $[x, y] \mapsto [y, x]$ if necessary, we may assume that B is generated by an element of the form $[h, 1]$ with $h \in \{i, j, k\}$. Since B acts nontrivially on A, there is an element $[x, y] \in A$ which does not commute with the generator $[h, 1]$ of B, and the latter requirement implies that $x \in \{i, j, k\}$ but $x \neq h$. Then the element

$$[h, 1][x, y][h, 1]^{-1}[x, y]^{-1} = [-1, 1]$$

belongs to A, a contradiction since $[-1, 1] = [h, 1]^2 \in B$. □

5. Symplectic restrictions

To recapitulate, every decomposition subgroup $\mathbf{D} = \mathrm{Gal}(F_v/\mathbb{Q}_p)$ of $\mathrm{Gal}(F/\mathbb{Q})$ is contained in a subgroup J isomorphic to one of the four groups listed in Proposition 10. In each case we will show that $\rho|\mathbf{D}$ is symplectic, but we emphasize that in cases (i) and (ii) of Proposition 10 our argument works in a setting that is slightly more general than that of Theorem 1: Instead of starting with L and L' as in the theorem and defining F as a subfield of LL' via (6) and (7), we start with a Galois extension F of $\mathbb{Q}$ such that $\mathrm{Gal}(F/\mathbb{Q}) \cong G$, and we define ρ up to isomorphism as the irreducible four-dimensional representation of $\mathrm{Gal}(F/\mathbb{Q})$. However to treat cases (iii) and (iv) we will need to use our assumption that F arises from L and L' as in (6) and (7).

So suppose first that $\mathbf{D} = \mathrm{Gal}(F_v/\mathbb{Q}_p) \subset J$ with J as in cases (i) or (ii) of Proposition 10. To prove Theorem 3 in these cases it suffices to show that $\rho|J$ is symplectic, for then $\rho_p = \rho|\mathbf{D}$ is symplectic also.

Proposition 12. *If J is a subgroup of G isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$ or to $Q \rtimes \mathbb{Z}/2\mathbb{Z}$ then $\rho|J$ is symplectic.*

Proof. We claim that $Z(J)$ contains elements of order 4. If $J \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$ this is obvious since $Z(J) = J$, and if $J \cong Q \rtimes \mathbb{Z}/2\mathbb{Z}$ then a calculation shows that $i \cdot r \in Q \rtimes Z/2\mathbb{Z}$ is central of order 4, where r is the generator of $\mathbb{Z}/2\mathbb{Z}$. An appeal to Proposition 3 completes the proof. □

It remains to prove Theorem 3 in cases (iii) and (iv) of Proposition 10. From now on we let L and L' be as in Theorem 1 and we assume that F arises from $K = LL'$ as indicated in (6) and (7). In the next proposition we use (6) and (7) to identify $\mathrm{Gal}(F/\mathbb{Q})$ with G, writing $\mathrm{Gal}(F/\mathbb{Q})$ and G interchangeably.

Proposition 13. *Let* $\mathbf{I}$ *be the inertia subgroup of* $\mathrm{Gal}(F/\mathbb{Q})$ *at some ramified prime ideal of* F*. Then* $\mathbf{I}$ *contains* $Z(G)$ *and is isomorphic to a subgroup of* Q*.*

Proof. Let $\mathfrak{p}$ be a prime ideal of F such that $\mathbf{I}$ is the inertia subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ at $\mathfrak{p}$. Let p be the prime number below $\mathfrak{p}$. Since p ramifies in F, it ramifies in exactly one of L and L', say in L. Let $\mathfrak{P}$ be a prime ideal of K lying above $\mathfrak{p}$, and let $\mathbf{J} \subset \mathrm{Gal}(K/\mathbb{Q})$ be the inertia subgroup at $\mathfrak{P}$. Then $\mathbf{J} \subset \mathrm{Gal}(K/L')$. Since $\mathrm{Gal}(K/F)$ intersects $\mathrm{Gal}(K/L')$ trivially, it follows that $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(F/\mathbb{Q})$ sends $\mathbf{J}$ isomorphically onto $\mathbf{I}$. We now deduce the two assertions of the proposition in reverse order.

First, since $\mathrm{Gal}(K/L')$ is isomorphic to Q, its subgroup $\mathbf{J}$ is isomorphic to a subgroup of Q. Hence so is $\mathbf{I}$.

Second, identify $\mathrm{Gal}(K/\mathbb{Q})$ with $Q \times Q$ using (6). Then $\mathrm{Gal}(K/L') = Q \times \{1\}$, whence $\mathbf{J} \subset Q \times \{1\}$. Since -1 is an element of every nontrivial subgroup of Q, we have $(-1, 1) \in \mathbf{J}$ and $[-1, 1] \in \mathbf{I}$. Thus $Z(G) \subset \mathbf{I}$. □

To treat cases (iii) and (iv) of Proposition 10 we use the following lemma, applicable to any finite group G and any irreducible self-dual representation ρ of G.

Lemma. *Let* C *be a subgroup of* G *such that* $\rho|C$ *is symplectic. Then* $\rho|Z(G)C$ *is symplectic also.*

Proof. Let $\langle *, * \rangle$ be a nondegenerate alternating form on the space of ρ which is invariant under $\rho|C$. If $z \in Z(G)$ and $c \in C$ then for v and w in the space of ρ,

$$\langle \rho(zc)(v), \rho(zc)(w) \rangle = \langle \omega_\rho(z)\rho(c)(v), \omega_\rho(z)\rho(c)(w) \rangle,$$

which is equal to $\omega_\rho(z)^2 \langle \rho(c)(v), \rho(c)(w) \rangle$ and therefore to $\langle v, w \rangle$. □

Proposition 14. *Let* $\mathbf{D}$ *be a decomposition subgroup of* $\mathrm{Gal}(F/\mathbb{Q})$ *which is isomorphic to a subgroup of* $(\mathbb{Z}/2\mathbb{Z})^4$*. Then* $\rho|\mathbf{D}$ *is symplectic.*

Proof. Let $\mathfrak{p}$ be a prime ideal of F such that $\mathbf{D}$ is the decomposition subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ at $\mathfrak{p}$, and let $\mathbf{I}$ be the inertia subgroup at $\mathfrak{p}$. We may assume that $\mathbf{I}$ is nontrivial, else we are done by Proposition 7. Then $\mathbf{I}$ is isomorphic to a nontrivial subgroup both of $(\mathbb{Z}/2\mathbb{Z})^4$ and of Q (by Proposition 13) and therefore $\mathbf{I} \cong \mathbb{Z}/2\mathbb{Z}$. Another appeal to Proposition 13 shows that $\mathbf{I} \supset Z(G)$ whence $\mathbf{I} = Z(G)$. Since $\mathbf{D}$ is also isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^4$ and $\mathbf{D}/\mathbf{I}$ is cyclic, we conclude that either $\mathbf{D} = \mathbf{I} = Z(G)$ or $\mathbf{D} = \mathbf{I} \oplus C = Z(G) \oplus C$ with a subgroup $C \cong \mathbb{Z}/2\mathbb{Z}$. In the latter case $\rho|C$ is symplectic by Proposition 8. The lemma then shows in both cases that $\rho|\mathbf{D}$ is symplectic. □

The following proposition completes the proof of Theorem 3 and hence of part (ii) of Theorem 1.

Proposition 15. *Let* $\mathbf{D}$ *be a decomposition subgroup of* $\mathrm{Gal}(F/\mathbb{Q})$ *which is isomorphic to a subgroup of* $D \times (\mathbb{Z}/2\mathbb{Z})$. *Then* $\rho|\mathbf{D}$ *is symplectic.*

Proof. As in the proof of Proposition 14, we choose a prime ideal $\mathfrak{p}$ such that $\mathbf{D}$ is the decomposition subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ at $\mathfrak{p}$, and we let $\mathbf{I}$ be the inertia subgroup. By Proposition 7 we may assume that $\mathbf{I}$ is nontrivial. Then $\mathbf{I}$ contains $Z(G)$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or Q by Proposition 13. But Q is not isomorphic to a subgroup of $D \times (\mathbb{Z}/2\mathbb{Z})$ because the latter group has only two cyclic subgroups of order 4. So $\mathbf{I} \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbf{I} \cong \mathbb{Z}/4\mathbb{Z}$.

Suppose first that $\mathbf{I} \cong \mathbb{Z}/2\mathbb{Z}$. Since normal subgroups of order 2 are central and $\mathbf{D}/\mathbf{I}$ is cyclic it follows that $\mathbf{D}$ is abelian. Therefore $\mathbf{D}$ is either cyclic, whence $\rho|\mathbf{D}$ is symplectic by Proposition 8, or $\mathbf{D} = \mathbf{I} \oplus C$ with C cyclic. In the latter case, since $\mathbf{I} = Z(G)$ by Proposition 13, we have $\mathbf{D} = Z(G) \oplus C$, and $\rho|C$ is symplectic by Proposition 8. Hence $\rho|\mathbf{D}$ is symplectic by the lemma.

Now suppose that $\mathbf{I} \cong \mathbb{Z}/4\mathbb{Z}$. If $\mathbf{D}$ is abelian then an appeal to Proposition 3 completes the proof. So we may assume that $\mathbf{D}$ is nonabelian. As we have already noted, $D \times (\mathbb{Z}/2\mathbb{Z})$ has two cyclic subgroups of order 4, one contained in $D \times \{1\}$ and one not contained in $D \times \{1\}$. Either way, the corresponding quotient of $D \times (\mathbb{Z}/2\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. But $\mathbf{D}/\mathbf{I}$ is a subgroup of the quotient at issue and is also cyclic, so $\mathbf{D}/\mathbf{I} \cong \mathbb{Z}/2\mathbb{Z}$. Thus $\mathbf{D}$ has order 8. Since $\mathbf{D}$ is nonabelian either $\mathbf{D} \cong Q$ or $\mathbf{D} \cong D$. But Q is not a subgroup of $D \times (\mathbb{Z}/2\mathbb{Z})$, so we conclude that $\mathbf{D} \cong D$.

Now let σ be an irreducible representation of $\mathbf{D}$ occurring in $\rho|\mathbf{D}$. Since $\mathbf{D} \supset \mathbf{I} \supset Z(G)$ and $\omega_\rho([-1,1]) = -1$, we have $\omega_\sigma([-1,1]) = -1$ also. But the only irreducible representation of D which is nontrivial on the center of D is the two-dimensional one. Therefore σ is the unique two-dimensional irreducible representation of $\mathbf{D}$, whence $\rho|\mathbf{D} = \sigma \oplus \sigma$. Since σ is self-dual, $\rho|\mathbf{D}$ is symplectic. □

6. Fröhlich's criterion

Following Fröhlich, we call a Galois extension L of $\mathbb{Q}$ a *quaternion field* if $\mathrm{Gal}(L/\mathbb{Q}) \cong Q$. Since the maximal abelian quotient of Q is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, the maximal abelian subfield of L is a biquadratic field M, which we may refer to as *the* biquadratic subfield of L since it is unique. Again following Fröhlich, we say that L is a *pure quaternion field* if every prime which is ramified in L is ramified already in M.

Now let us change perspective: Fix a biquadratic field M, and let d_1 and d_2 be the discriminants of two of the three quadratic subfields of M, so that $M = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Using the quadratic Hilbert symbol $(*,*)_\ell$ on $\mathbb{Q}_\ell$, Fröhlich gives a criterion for the existence of a pure quaternion field L with biquadratic subfield M: Such an L exists if and only if

$$(d_1, d_2)_\ell \cdot (d_1, -1)_\ell \cdot (-1, d_2)_\ell = 1 \tag{9}$$

for all primes ℓ, including $\ell = \infty$. ([15], p. 146, Thm. 3). Note that the discriminant of L is divisible by precisely the prime divisors of $d_1 d_2$, because L is pure.

Fröhlich's criterion makes it easy to produce pairs of quaternion fields with relatively prime discriminants, as required in Theorem 1. For example, one can simply apply the following proposition twice, the second time with p, q replaced by primes p', q' distinct from p and q:

Proposition 16. *Let* p *and* q *be distinct primes satisfying:*

(i) $p \equiv q \equiv 1 \pmod 4$.

(ii) $\left(\frac{p}{q}\right) = 1$.

Then there is a pure quaternion field L with biquadratic subfield $M = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

The proof is a straightforward exercise in properties of the Hilbert symbol; one verifies (9) with $d_1 = p$ and $d_2 = q$. However we would also like to show that the comprimality of the discriminants of L_1 and L_2 in Theorem 1 cannot be replaced by the weaker hypothesis of linear disjointness. The counterexample to be given in the next section depends on the following variant of Proposition 16. The congruences mod 8 in (i) below could be replaced by congruences mod 4, but the stronger hypothesis leads to a speedier verification of the proposition.

Proposition 17. *Let p, q, and r be distinct primes satisfying:*

(i) $p \equiv r \equiv 3 \pmod 8$ *and* $q \equiv 1 \pmod 8$.

(ii) $\left(\frac{p}{q}\right) = \left(\frac{r}{q}\right) = -1$.

Then there is a pure quaternion field L with biquadratic subfield $M = \mathbb{Q}(\sqrt{pr}, \sqrt{q})$, and p has ramification index $e = 4$ and residue class degree $f = 2$ in L.

Proof. We verify (9) with $d_1 = pr$ and $d_2 = q$. For a finite prime $\ell \nmid 2pqr$ the three factors on the left-hand side of (9) are individually equal to 1 because pr, q, and -1 are in $\mathbb{Z}_\ell^\times$. For $\ell = \infty$ or $\ell | 2q$ the three factors are again 1 because pr and q are squares in $\mathbb{R}$, $\mathbb{Q}_2$, and $\mathbb{Q}_q$. It remains to check the cases $\ell = p$ and $\ell = r$. Since p and r play interchangeable roles it suffices to consider p. By quadratic reciprocity, $\mathbb{Q}_p(\sqrt{q})$ is the unramified quadratic extension of $\mathbb{Q}_p$, whence $(pr, q)_p = -1$. But $\mathbb{Q}_p(\sqrt{-1})$ is likewise the unramified quadratic extension of $\mathbb{Q}_p$, so $(pr, -1)_p = -1$ also. Finally since $\mathbb{Q}_p(\sqrt{-1})$ is unramified over $\mathbb{Q}_p$ and $q \in \mathbb{Z}_p^\times$, it follows that $(-1, q)_p = 1$. So (9) holds for $\ell = p$ and therefore for all ℓ. Thus L exists.

As for the ramification index e and residue class degree f, it suffices to verify that $4|e$ and $2|f$, for then $8|ef$, and as $[L : \mathbb{Q}] = 8$ the divisibilities are equalities. Since p is ramified in $\mathbb{Q}(\sqrt{rp})$, the inertia subgroup $\mathbf{I} \subset \mathrm{Gal}(L/\mathbb{Q})$ of a prime ideal of L above p is not contained in $Z(Q)$. But any noncentral element of Q has order 4, so $\mathbf{I}$ has order divisible by 4, and $4|e$. Finally, since q is a nonresidue mod p by quadratic reciprocity, p is inert in $\mathbb{Q}(\sqrt{q})$, so $2|f$. □

7. A counterexample

Fix a prime $p \equiv 3$ mod 8, and choose two primes q and q', distinct from each other and from p, satisfying $q \equiv q' \equiv 1$ mod 8 and

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right) = -1.$$

Such q and q' exist by the Chinese remainder theorem, because the conditions on the Legendre symbols amount to congruences mod p. Finally, choose primes r and r', distinct from each other and from p, q, and q', satisfying $r \equiv r' \equiv 3$ mod 8 and

$$\left(\frac{r}{q}\right) = \left(\frac{r'}{q}\right) = -1.$$

Applying Proposition 17, we obtain pure quaternion fields L and L' with biquadratic subfields $M = \mathbb{Q}(\sqrt{pr}, \sqrt{q})$ and $M' = \mathbb{Q}(\sqrt{pr'}, \sqrt{q'})$ such that p has ramification index 4 and residue class degree 2 in each of L and L'.

Proposition 18. *$L \cap L' = \mathbb{Q}$.*

Proof. If $L \cap L'$ is not $\mathbb{Q}$ then it contains a quadratic subfield of L, so one of the three fields $\mathbb{Q}(\sqrt{d})$ with $d = pr$, $d = q$, or $d = pqr$. But none of these fields is contained in L', contradiction. □

Let $K = LL'$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(L'/\mathbb{Q})$ by Proposition 18, and consequently $\mathrm{Gal}(K/\mathbb{Q})$ can be identified with $Q \times Q$ as in (6). Then F can be defined as the fixed field of R as in (7). Given these identifications, we shall continue to write (x, y) and $[x, y]$ for elements of $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(F/\mathbb{Q})$ respectively, and we shall view the four-dimensional irreducible representation ρ of G as a representation of $\mathrm{Gal}(F/\mathbb{Q})$.

Proposition 19. *Let $\mathbf{D} \subset \mathrm{Gal}(F/\mathbb{Q})$ be the decomposition subgroup of a prime ideal of F above p. Then $\mathbf{D} \cong (\mathbb{Z}/2\mathbb{Z})^2$ and ρ_p is the regular representation of $\mathbf{D}$.*

Proof. When $\mathrm{Gal}(K/\mathbb{Q})$ is identified with $Q \times Q$, M is the fixed field of $\{\pm 1\} \times Q$ and M' is the fixed field of $Q \times \{\pm 1\}$. Since F is the fixed field of $\{1, (-1, -1)\}$, it follows that F contains M and M' and that the kernel of the restriction map from $\mathrm{Gal}(F/\mathbb{Q})$ to $\mathrm{Gal}(M/\mathbb{Q})$ and from $\mathrm{Gal}(F/\mathbb{Q})$ to $\mathrm{Gal}(M'/\mathbb{Q})$ consists of elements of the form $[\pm 1, y]$ and $[x, \pm 1]$ respectively.

Let $\mathfrak{p}$ be a prime ideal of F above p such that $\mathbf{D}$ is the decomposition subgroup of $\mathfrak{p}$, and let $\mathbf{I} \subset \mathbf{D}$ be the inertia subgroup. Since p is odd, the ramification at p is tame, and consequently $\mathbf{I}$ is cyclic. Let $[x, y]$ be a generator. Since the restriction map of $\mathrm{Gal}(F/\mathbb{Q})$ onto $\mathrm{Gal}(M/\mathbb{Q})$ and $\mathrm{Gal}(M'/\mathbb{Q})$ sends $\mathbf{I}$ onto the inertia subgroups of $\mathrm{Gal}(M/\mathbb{Q})$ and $\mathrm{Gal}(M'/\mathbb{Q})$ at $\mathfrak{p} \cap M$ and $\mathfrak{p} \cap M'$ respectively, and since the latter inertia subgroups are nontrivial, we have $x \neq \pm 1$ and $y \neq \pm 1$. Therefore $[x, y]$ is a noncentral involution (Proposition 1).

Next let $[h, h'] \in \mathrm{Gal}(F/\mathbb{Q})$ be a Frobenius element at $\mathfrak{p}$. Again, $[h, h']$ restricts to Frobenius elements in $\mathrm{Gal}(M/\mathbb{Q})$ and $\mathrm{Gal}(M'/\mathbb{Q})$ at $\mathfrak{p} \cap M$ and $\mathfrak{p} \cap M'$, and the latter Frobenius elements are nontrivial because p is inert in $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{q'})$. It follows that $h, h' \neq \pm 1$, so that $[h, h']$ is also a noncentral involution, as is $[xh, yh']$, since it too is a Frobenius element at $\mathfrak{p}$.

To summarize, $\mathbf{I}$ is a normal subgroup of order 2 in $\mathbf{D}$, hence central, and $\mathbf{D}/\mathbf{I}$ is cyclic, so that $\mathbf{D}$ is abelian. Since the coset of $[h, h']$ generates $\mathbf{D}/\mathbf{I}$ but $[h, h']$ is itself of order 2, we conclude that $\mathbf{D} \cong (\mathbb{Z}/2\mathbb{Z})^2$, and since the 3 nonidentity elements of $\mathbf{D}$ are noncentral involutions, we see from Proposition 6 that $\rho|\mathbf{D}$ is the regular representation of $\mathbf{D}$. □

There is a unique biquadratic extension of $\mathbb{Q}_p$, namely the compositum of the unique unramified quadratic extension and either of the two ramified extensions. This biquadratic extension coincides with M_v, the completion of M at the place above p. Hence we can rephrase Proposition 19 as follows:

Corollary. *The decomposition subgroup $\mathbf{D}$ of $\mathrm{Gal}(F/\mathbb{Q})$ at a prime ideal of F above p coincides with $\mathrm{Gal}(M_v/\mathbb{Q}_p)$, and ρ_p is the direct sum of the four one-dimensional characters of $\mathrm{Gal}(M_v/\mathbb{Q}_p)$.*

Now we show that F gives a counterexample to part (ii) of Theorem 1 when coprimality of the discriminants of L and L' is replaced by mere linear disjointness over $\mathbb{Q}$:

Proposition 20. *There are infinitely many numbers $j \in \mathbb{Q}$ such that there is an elliptic curve E_j of invariant j with $W(E_j, \rho) = -1$.*

Proof. As is well known, for any $j \in \mathbb{Q} \smallsetminus \{0, 1728\}$, the equation

$$y^2 + xy = x^3 - \frac{36x}{j - 1728} - \frac{1}{j - 1728} \tag{10}$$

defines an elliptic curve E_j over $\mathbb{Q}$ with modular invariant j, and the discriminant of (10) is $\Delta = j^2/(j - 1728)^3$. Consider numbers j of the form $j = 1728 - (pm)^{-1}$, where m runs over integers relatively prime to $qq'rr'$ satisfying $1728pm \not\equiv 1 \bmod \ell$ for $\ell = q, q', r, r'$. Then (10) becomes

$$y^2 + xy = x^3 + 36pmx + pm, \tag{11}$$

an equation over $\mathbb{Z}$ with discriminant $\Delta = -pm(1728pm - 1)^2$. Thus E_j has good reduction at q, q', r, and r'. And since L and L' are pure quaternion fields, a prime ℓ ramifies in F only if $\ell | pqq'rr'$.

To compute $W(E_j, \rho)$ we apply a general principle, partially incorporated into Proposition 7: If E is any elliptic curve over $\mathbb{Q}$ and ρ is any self-dual Artin representation of $\mathbb{Q}$ of even dimension and trivial determinant then the local root number $W(E, \rho_\ell)$ is 1 unless $\ell < \infty$ and ℓ is a bad prime for both E and ρ. In other words, $W(E, \rho_\ell) = -1$ only if E has bad reduction at ℓ and ρ is ramified at ℓ (cf. [32], p. 332, Proposition 8, parts (i) and (ii)). In the case at hand, ρ is unramified at all $\ell \nmid pqq'rr'$ and E_j has good reduction at all $\ell | qq'rr'$, so $W(E_j, \rho) = W(E_j, \rho_p)$. Since E_j has potentially multiplicative reduction at p and ρ_p is the direct sum of the four one-dimensional characters of $\mathrm{Gal}(M_v/\mathbb{Q}_p)$, we have $W(E_j, \rho_p) = -1$ by [32], p. 329, Theorem 2, part (ii). □

References

[1] J. Balakrishnan, W. Ho, N. Kaplan, S. Spicer, W. Stein, and J. Weigandt, *Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks*, LMS J. of Computation and Math. 19 Issue A (Algorithmic Number Theory Symposium XII) (2016), 351-370.

[2] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, *Average ranks of elliptic curves: Tension between data and conjecture*, Bull. AMS 44 (2007), 233-254.

[3] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman, *3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field* Duke Math J. 168 (2019), 2951-2989.

[4] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. 181 (2015), 191-242.

[5] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. 181 (2015), 587-621.

[6] M. Bhargava, C. Skinner, and W. Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, available at arXiv:1407.1826v2.

[7] B. J. Birch, Nelson Stephens, *The parity of the rank of the Mordell-Weil group*, Topology 5 (1966), 295-299.

[8] M. Bisatt, *Explicit root numbers of abelian varieties*, Trans. Amer. Math. Soc. 372 (2019), 7889-7920.

[9] A. Brumer, K. Kramer, and M. Sabitova, *Explicit determination of root numbers of abelian varieties*, Trans. Amer. Math. Soc. 370 (2018), 2589-2604.

[10] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. 178 (2009), 23-71.
[11] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Annals of Math. 172 (2010) 567-596.
[12] T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. 658 (2011), 39-64.
[13] V. Dokchitser and Céline Maistret, *Parity conjecture for abelian surfaces*, available at arXiv:1911.04626v4.
[14] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales* In: *Automorphic Forms, Representations, and L-functions*, Proc. Symp. Pure Math. vol. XXXIII, Part 2, AMS (1979), 313-346.
[15] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. 17 (1972), 143 – 166.
[16] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbodale 1979 (Proc. Southern Illinois Univ. Carbondale, Ill. 1979) Lecture Notes in Math. 751) Springer (1979), 108-118.
[17] B. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Springer Lect. Notes 776 (1980).
[18] D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Math. J. 122 (2004), 591-623.
[19] O. Hölder, *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. 43 (1893), 301-412.
[20] D. Kriz and C. Li, *Prime twists of elliptic curves*, Math. Res. Lett. 26 (2019), 1187-1195.
[21] D. Kriz and C. Li, *Goldfeld's conjecture and congruences between Heegner points*. Forum Math. Sigma 7 e15 (2019)
[22] T. de La Rochefoucauld, *Invariance of the parity conjecture for p-Selmer groups of elliptic curves in a D_{2p^n}-extension*, Bull. Soc. Math. France 139 (2011), 571-592.
[23] T. de La Rochefoucauld, *Signes locaux et nombres de Tamagawa*, J. théorie des nombres Bordeaux 28 (2016), 1-38.
[24] E. Liverance, *A formula for the root number of a family of elliptic curves*, J. Number Thy. 51 (1995), 288-305.
[25] K. Matsuno, *A note on the growth of Mordell-Weil ranks of elliptic curves in cyclotomic $\mathbf{Z}_p$ extensions*, Proc. Japan Acad. Ser. A Math. Sci. 79 (2003), 101-104.
[26] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. reine angew. Math. 533 (2001), 81-97.
[27] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. 134 (1998) 651-660.
[28] J. Park, B. Poonen, J. Voight, M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. 21 (2019), 2859-2903.
[29] A. Perelli and J. Pomykala, *Averages of twisted elliptic L-functions* Acta Arithmetica 80 (1997), 149-163.
[30] D. E. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*. In: Automorphic Forms and Analytic Number Theory, Les Publications CRM, Montreal (1990), 123 – 133.
[31] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*. In: *Elliptic Curves and Related Topics*, HK̇isilevsky and M. R. Murty, eds, CRM Proceedings and Lecture Notes 4, Amer. Math. Soc. (1994), 125 – 157.
[32] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. 100 (1996), 311 – 349.
[33] D. E. Rohrlich, *Realization of some Galois representations of low degree in Mordell-Weil groups*, Mathematical Research Letters 4 (1997), 123 – 130.
[34] M. Sabitova, *Root numbers of abelian varieties*, Trans. Amer. Math. Soc. 359 (2007), 4259-4284.
[35] J.-P. Serre, *Linear Representations of Finite Groups*, Springer GTM 42 (1977).
[36] A. Smith, *2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture*, available at arXiv:1702.02325v2.
[37] A. Suresh, *Realizing Galois representations in abelian varieties by specialization*, arXiv:2206.09778v3.
[38] J. Tate, I. Shafarevich, *The rank of elliptic curves*, Akad. Nauk SSSR 175 (1967) 770-773.

[39] D. Ulmer, *Elliptic curves with large rank over function fields*, Annals of Math. 155 (2002), 295-315.
[40] M. Watkins, *Some heuristics about elliptic curves*, Experimental Math. 17 (2008), 105-125.
[41] M. Wild, *The Groups of Order Sixteen Made Easy*, Amer. Math. Monthly 112 (2005), 20-31.
[42] J. Young, *On the determination of the groups whose order is a power of a prime*, Amer. J. Math. 15 (1893), 124-178.

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