COMPOSITIO MATHEMATICA

DAVID E. ROHRLICH

Galois theory, elliptic curves, and root numbers

Compositio Mathematica, tome 100, n° 3 (1996), p. 311-349
<http://www.numdam.org/item?id=CM_1996__100_3_311_0>

Compositio Mathematica **100:** 311–349, 1996.

Galois theory, elliptic curves, and root numbers

DAVID E. ROHRLICH *
Department of Mathematics, Boston University, Boston, MA 02215

Received 2 August 1994; accepted in final form 3 January 1995

The inverse problem of Galois theory asks whether an arbitrary finite group G can be realized as $\mathrm{Gal}(K/\mathbb{Q})$ for some Galois extension K of $\mathbb{Q}$. When such a realization has been given for a particular G then a natural sequel is to find arithmetical realizations of the irreducible representations of G. One possibility is to ask for realizations in the Mordell-Weil groups of elliptic curves over $\mathbb{Q}$: Given an irreducible complex representation τ of $\mathrm{Gal}(K/\mathbb{Q})$, does there exist an elliptic curve E over $\mathbb{Q}$ such that τ occurs in the natural representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C}\otimes_{\mathbb{Z}} E(K)$? The present paper does not attempt to investigate this question directly. Instead we adopt Greenberg's point of view in his remarks on nonabelian Iwasawa theory [5] and consider a related question about root numbers. Let ρ_E denote the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C}\otimes_{\mathbb{Z}} E(K)$ and $\langle \tau, \rho_E \rangle$ the multiplicity of τ in ρ_E, and write $L(E,\tau,s)$ for the tensor product L-function associated to E and τ. The conjectures of Birch-Swinnerton-Dyer and Deligne-Gross imply that

$$\mathrm{ord}_{s=1} L(E,\tau,s) = \langle \tau, \rho_E \rangle \tag{0.1}$$

(cf. [10], p. 127), whence for representations τ with real-valued character the root number $W(E,\tau)$ should satisfy

$$W(E,\tau) = (-1)^{\langle \tau, \rho_E \rangle}. \tag{0.2}$$

The reasoning here is based on the conjectural functional equation of $L(E,\tau,s)$, which for representations with real-valued character relates $L(E,\tau,s)$ to itself and therefore gives us (0.2) as a consequence of (0.1). Now if $W(E,\tau) = -1$ then (0.2) implies that the multiplicity of τ in $\mathbb{C}\otimes_{\mathbb{Z}} E(K)$ is odd and hence positive. Thus we are led to our basic question: Given τ, an irreducible complex representation of $\mathrm{Gal}(K/\mathbb{Q})$ with real-valued character, does there exist an elliptic curve E over $\mathbb{Q}$ such that $W(E,\tau) = -1$?

The best-known and most easily stated *sufficient* condition, and the one which figures in Greenberg's paper [5], is the following:

PROPOSITION A. *If* $\dim \tau$ *is odd or* $\det \tau$ *is nontrivial then there exists an elliptic curve* E *over* $\mathbb{Q}$ *such that* $W(E,\tau) = -1$.

* Research partially supported by NSF grant DMS-9396090

Our primary concern is therefore with representations of even dimension and trivial determinant. By way of illustration, consider the case of a Galois extension of $\mathbb{Q}$ with Galois group A_5, the alternating group on 5 letters. Up to isomorphism, A_5 has exactly four nontrivial irreducible representations, all with real-valued character: two of dimension 3, one of dimension 4, and one of dimension 5. Since A_5 is simple all of these representations have trivial determinant. In view of Proposition A, only the representation of dimension 4 presents an issue.

PROPOSITION B. *Let K be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$, and let τ be the 4-dimensional irreducible representation of $\mathrm{Gal}(K/\mathbb{Q})$, unique up to isomorphism. There exists an elliptic curve E over $\mathbb{Q}$ such that $W(E,\tau) = -1$ if and only if some decomposition subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to A_4, S_3, or $(\mathbb{Z}/2\mathbb{Z})^2$.*

Buhler ([1], pp. 47 and 136–141) has tabulated 174 fields K with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$, and about half of the fields in his table satisfy our criterion. For example, if K is the splitting field of $x^5 + 10x^3 - 10x^2 + 35x - 18$ (the field of conductor 800 in the table) then the decomposition groups of $\mathrm{Gal}(K/\mathbb{Q})$ at 2 are isomorphic to A_4, and hence there exists an E for which $W(E,\tau) = -1$. In fact one can take for E any elliptic curve over $\mathbb{Q}$ with split multiplicative reduction at 2. On the other hand, if K is the splitting field of $x^5 + 6x^4 + 19x^3 + 25x^2 + 11x + 2$ (the field of conductor 1501 in the table) then none of the groups in Proposition B occurs as a decomposition group, and consequently $W(E,\tau) = 1$ for every E over $\mathbb{Q}$.

Proposition B illustrates the type of statement which can be deduced from our main result, Theorem 3. However, we would like to emphasize that Theorem 3 is far from being a definitive result of its kind, because the underlying local calculations do not cover all possibilities when the residue characteristic is 2 or 3. While this defect turns out not to matter in the case of A_5 and in many other cases, the effect in general is that the necessary conditions afforded by Theorem 3 are weaker than the sufficient conditions. A second point about the theorem is that usually there is no way to predict what it says about a given group G and a given irreducible representation τ of G except by calculating the restriction of τ to various small subgroups of G. Consider for example the next simple group after A_5, namely $\mathrm{PSL}(2,\mathbb{F}_7)$. Up to equivalence $\mathrm{PSL}(2,\mathbb{F}_7)$ has five nontrivial irreducible representations: two of dimension 3, which do not have real-valued character, and one each of dimensions 6, 7, and 8. Of concern here are the representations of dimensions 6 and 8. The disparate behavior of these two representations under restriction to subgroups is reflected in the following proposition. Let D_n denote the dihedral group of order $2n$.

PROPOSITION C. *Let K be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}(2,\mathbb{F}_7)$, and let $\tau^{(6)}$ and $\tau^{(8)}$ be the irreducible representations of $\mathrm{Gal}(K/\mathbb{Q})$ of dimensions 6 and 8 respectively, unique up to isomorphism.*

(1) *There exists an elliptic curve* E *over* $\mathbb{Q}$ *such that* $W(E, \tau^{(6)}) = -1$ *if and only if some decomposition subgroup of* $\mathrm{Gal}(K/\mathbb{Q})$ *is isomorphic to* S_4, A_4, D_4, *or* $(\mathbb{Z}/2\mathbb{Z})^2$.

(2) *There exists an elliptic curve* E *over* $\mathbb{Q}$ *such that* $W(E, \tau^{(8)}) = -1$ *if and only if some decomposition subgroup of* $\mathrm{Gal}(K/\mathbb{Q})$ *is isomorphic to* S_4, D_4, *or* S_3.

A beautiful example of a Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{PSL}(2, \mathbb{F}_7)$ has been given by Trinks (see LaMacchia [7], p. 990, or Matzat [9], p. 212): K is the splitting field of the polynomial $x^7 - 7x + 3$. In this example the decomposition groups at 3 are isomorphic to S_3, but none of the other groups listed in Proposition C occurs as a decomposition group. Hence there is an elliptic curve E over $\mathbb{Q}$ for which $W(E, \tau^{(8)}) = -1$ but none for which $W(E, \tau^{(6)}) = -1$. We shall see that $W(E, \tau^{(8)}) = -1$ whenever E has split multiplicative reduction at 3.

To complete our survey of illustrative special cases, let us note that there are situations in which $W(E, \tau)$ is always 1:

PROPOSITION D. *Let* K *be a Galois extension of* $\mathbb{Q}$ *such that* $\mathrm{Gal}(K/\mathbb{Q}) \cong D_q \times D_r \times D_s \times D_t$ *with distinct primes* $q, r, s, t \geqslant 5$, *and let* τ *be an irreducible* 16*-dimensional representation of* $\mathrm{Gal}(K/\mathbb{Q})$. *Then* $W(E, \tau) = 1$ *for every elliptic curve* E *over* $\mathbb{Q}$.

As with other deductions from Theorem 3, Proposition D does not appear to be predictable on *a priori* grounds. However, there is one case in which a result like Proposition D would be entirely expected, namely the case where the Schur index of τ is even (by contrast, every irreducible representation of $D_q \times D_r \times D_s \times D_t$ has Schur index 1). The point here is that the representation ρ_E of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$ is the complexification of a representation over $\mathbb{Q}$. Hence if τ is any irreducible representation of $\mathrm{Gal}(K/\mathbb{Q})$ then $\langle \tau, \rho_E \rangle$ is divisible by the Schur index $m(\tau)$ of τ. In particular, if tr τ is real-valued and $m(\tau)$ is even then (0.2) would imply that $W(E, \tau) = 1$. The next proposition verifies this conclusion under some condition at the primes 2 and 3. Since the Schur index of an irreducible representation with real-valued character is either 1 or 2 (the Brauer-Speiser theorem), to say that $m(\tau)$ is even is to say that $m(\tau) = 2$.

PROPOSITION E. *Let* K *be a finite Galois extension of* $\mathbb{Q}$ *and* τ *an irreducible complex representation of* $\mathrm{Gal}(K/\mathbb{Q})$ *with real-valued character. Assume that the decomposition subgroups of* $\mathrm{Gal}(K/\mathbb{Q})$ *at* 2 *and* 3 *are abelian. If* $m(\tau) = 2$ *then* $W(E, \tau) = 1$ *for every elliptic curve* E *over* $\mathbb{Q}$.

Given the incompleteness of our local calculations at the primes 2 and 3, some extraneous condition at these primes seems inevitable, but the particular condition chosen here could be replaced by a number of alternative hypotheses. For example, instead of imposing a condition on the decomposition groups at 2 and 3 we could

require that E have semistable reduction at 2 and 3, or more generally that E attain semistable reduction over abelian extensions of $\mathbb{Q}_2$ and $\mathbb{Q}_3$. In any case, the main point is that if $m(\tau) = 2$ then root numbers are of no use in detecting the possible occurrence of τ in the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$. This is an inherent limitation of our point of view.

In conclusion let us point out that Theorem 2 of the present paper is a generalization of the local results in [11], the latter being the special case where τ is the trivial representation. We also take this opportunity to mention the paper of Kramer and Tunnell [6], which should be added to the list of references in [11]. The ingredients in the proof of Theorem 2.7 of [6] and of Proposition 2 of [11] are the same; the latter result merely carries the argument one step further.

It is a pleasure to thank John Millson for clarifying a property of Stiefel-Whitney classes and Brian Conrey for providing the reference [5].

1. A local calculation

By a representation of a group G we shall always mean a finite-dimensional representation over the complex numbers, understood to be continuous if G has a natural topology. The contragredient of a representation π will be denoted π^*. We say that π is *self-contragredient* if $\pi \cong \pi^*$, *symplectic* if the space of π admits a nondegenerate symplectic form invariant under π, and *realizable over* a subfield $\mathbb{E}$ of $\mathbb{C}$ if there is an $\mathbb{E}$-form of the space of π which is preserved by π. We mention in passing that if the image of π is finite then π is realizable over $\mathbb{R}$ if and only if π is *orthogonal*, i.e. if and only if the space of π admits a nondegenerate symmetric bilinear form invariant under π.

By a character of G we shall mean either a one-dimensional representation (i.e. a 'quasicharacter' $\chi : G \to \mathbb{C}^\times$) or the trace of a representation of dimension $\geqslant 1$, depending on the context. In the case of 'one-dimensional characters' the two meanings coincide, of course. Of particular importance to us are one-dimensional characters of $\mathrm{Gal}(\overline{F}/F)$, or equivalently, of $\mathrm{Gal}(F^{\mathrm{ab}}/F)$, where F is a local field of characteristic 0 and F^{ab} its abelian closure. We shall routinely identify such characters with finite-order characters of $F^\times$ by agreeing that

$$\chi(x) = \chi((x^{-1}, F^{\mathrm{ab}}/F)) \quad (x \in F^\times), \tag{1.1}$$

where $(*, F^{\mathrm{ab}}/F)$ is the reciprocity law homomorphism as normalized by Artin. For example, 1_F can denote either the trivial character of $\mathrm{Gal}(\overline{F}/F)$ or the trivial character of $F^\times$, and if K is a quadratic extension of F then $\chi_{K/F}$ can denote either the quadratic character of $\mathrm{Gal}(\overline{F}/F)$ with kernel $\mathrm{Gal}(\overline{F}/K)$ or the quadratic character of $F^\times$ with kernel $N_{K/F}(K^\times)$. We remark that the choice of x^{-1} rather than x on the right-hand side of (1.1) is made for the sake of consistency with [2] and [18].

If K is any finite extension of F then we denote by $\mathrm{ind}_{K/F}$ and $\mathrm{res}_{K/F}$ the induction and restriction functors associated to $\mathrm{Gal}(\overline{F}/F)$ and its subgroup of finite

index $\mathrm{Gal}(\overline{F}/K)$. In the case where F is nonarchimedean we shall make frequent use of the fact that the Artin conductor-exponent $a(*)$ satisfies the formula

$$a(\mathrm{ind}_{K/F}\pi) = d(K/F)\dim\pi + f(K/F)a(\pi), \tag{1.2}$$

where π is an arbitrary representation of $\mathrm{Gal}(\overline{F}/K)$ and $d(K/F)$ and $f(K/F)$ denote respectively the exponent of the relative discriminant of K over F and the residue class degree of K over F. A general reference for the properties of $a(*)$ that will be needed here is [15].

Given a representation π of $\mathrm{Gal}(\overline{F}/F)$, an additive character ψ of F, and a Haar measure dx on F, let $\epsilon(\pi, \psi, dx)$ denote the associated epsilon factor. If the determinant of π is trivial then we define the root number $W(\pi)$ of π by the formula

$$W(\pi) = \frac{\epsilon(\pi, \psi, dx)}{|\epsilon(\pi, \psi, dx)|}, \tag{1.3}$$

the point being that when $\det\pi$ is trivial the right-hand side of (1.3) – which is in any case independent of the choice of dx – is independent of the choice of ψ as well. If π is self-contragredient as well as of trivial determinant then $W(\pi) = \pm 1$. This is in particular the case for the representations of primary interest here, namely those of the form $\pi = \sigma \otimes \tau$ with σ a symplectic representation of $\mathrm{Gal}(\overline{F}/F)$ and τ an arbitrary representation of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character. Indeed the self-contragredience of $\sigma \otimes \tau$ and the triviality of $\det\sigma \otimes \tau$ follow from the formulas

$$(\sigma \otimes \tau)^* \cong \sigma^* \otimes \tau^*$$

and

$$\det(\sigma \otimes \tau) = (\det\sigma)^{\dim\tau}(\det\tau)^{\dim\sigma}$$

respectively, because a symplectic representation is self-contragredient, even-dimensional, and of trivial determinant, while a representation with finite image is self-contragredient if and only if its character is real-valued.

Although our goal is to calculate $W(\pi)$ in a case where this quantity is independent of any choices, the method of calculation forces us to consider representations for which the root number depends on the choice of ψ. Such a root number is still defined by the right-hand side of (1.3) but should in principle be denoted $W(\pi, \psi)$. However, to avoid carrying ψ in the notation, let us agree that for each local field F of characteristic 0 we choose the additive character

$$\psi_F = \psi_p \circ \mathrm{tr}_{F/\mathbb{Q}_p},$$

where $\mathbb{Q}_p$ is the topological closure of $\mathbb{Q}$ in F,

$$\psi_p(x) = \begin{cases} \mathrm{e}^{-2\pi i x} & \text{if } p = \infty \\ \mathrm{e}^{2\pi i\{x\}_p} & \text{if } p < \infty, \end{cases}$$

and $\{x\}_p$ denotes the image of x under the composition of natural maps

$$\mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z} \quad (p < \infty).$$

With this convention we have $\psi_K = \psi_F \circ \mathrm{tr}_{K/F}$ for a finite extension K of F, and consequently if π is a representation of $\mathrm{Gal}(\overline{F}/K)$ then

$$W(\mathrm{ind}_{K/F}\pi) = W(\pi)W(\mathrm{ind}_{K/F}1_K)^{\dim \pi}. \tag{1.4}$$

Formula (1.4) is the analogue for root numbers of (1.2) and an expression of the fact that 'epsilon factors are inductive in dimension 0'. For further background on root numbers the reader is referred to [2], [18], or [12].

Later in the paper we shall encounter representations of the Weil group $\mathcal{W}(\overline{F}/F)$ and of the Weil-Deligne group $\mathcal{W}'(\overline{F}/F)$ as well as representations of $\mathrm{Gal}(\overline{F}/F)$. Thus it is appropriate to note that all of the definitions and conventions just mentioned are meaningful in the larger context. In particular, if σ is a symplectic representation of $\mathcal{W}(\overline{F}/F)$ or $\mathcal{W}'(\overline{F}/F)$ and τ is a representation of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character, then it is still true that $W(\sigma \otimes \tau)$ is a well-defined number equal to ± 1. We also point out that formula (1.1) allows us to identify arbitrary characters of $F^\times$ (not necessarily of finite order) with characters of $\mathcal{W}(\overline{F}/F)$ and hence with characters of $\mathcal{W}'(\overline{F}/F)$.

Some two-dimensional representations

By a dihedral representation we shall mean an irreducible two-dimensional representation which has finite image and is realizable over $\mathbb{R}$. Equivalently, a dihedral representation is a two-dimensional representation with image a dihedral group of order $\geqslant 6$. The equivalence of the two definitions follows from the fact that a finite subgroup of $\mathrm{GL}(2,\mathbb{R})$ is conjugate to a subgroup of $\mathrm{O}(2,\mathbb{R})$ and is therefore either cyclic or dihedral.

To avoid a possible ambiguity we make one further remark. In part (i) of the following proposition we consider a representation of the form $\mathrm{ind}_{H/F}\varphi$, where H/F is a quadratic extension of nonarchimedean local fields of characteristic 0 and φ is a character of $H^\times$. Since we do not assume that φ has finite order the representation $\mathrm{ind}_{H/F}\varphi$ must be interpreted *a priori* as a representation of $\mathcal{W}(\overline{F}/F)$ rather than of $\mathrm{Gal}(\overline{F}/F)$. However, we prove that if $\mathrm{ind}_{H/F}\varphi$ is irreducible and symplectic then $\varphi|F^\times$ coincides with $\chi_{H/F}$, the quadratic character of $F^\times$ corresponding to H. Since F is nonarchimedean, the equality $\varphi|F^\times = \chi_{H/F}$ implies that φ has finite order, whence $\mathrm{ind}_{H/F}\varphi$ is a representation of $\mathrm{Gal}(\overline{F}/F)$.

PROPOSITION 1. *Let F be a nonarchimedean local field of characteristic* 0.

(i) *Let H be a quadratic extension of F and φ a character of $H^\times$. The representation* $\mathrm{ind}_{H/F}\varphi$ *is irreducible and symplectic if and only if $\varphi|F^\times = \chi_{H/F}$ and $\varphi^2 \neq 1_H$.*

(ii) *A representation of* $\mathrm{Gal}(\overline{F}/F)$ *is dihedral if and only if it has the form* $\mathrm{ind}_{H/F}\varphi$ *for some quadratic extension* H *of* F *and some character* φ *of* $H^\times$ *satisfying* $\varphi|F^\times = 1_F$ *and* $\varphi^2 \neq 1_H$.

Proof. Both assertions are quite standard, but for the sake of completeness we provide a detailed argument.

(i) A two-dimensional representation is symplectic if and only if it has trivial determinant, because $\mathrm{Sp}(2,\mathbb{C}) = \mathrm{SL}(2,\mathbb{C})$. Now according to the formula for the determinant of an induced representation (cf. [2], p. 508),

$$\det(\mathrm{ind}_{H/F}\varphi) = \chi_{H/F}(\varphi|F^\times). \tag{1.5}$$

Therefore $\mathrm{ind}_{H/F}\varphi$ is symplectic if and only if $\varphi|F^\times = \chi_{H/F}$. We claim that under these equivalent conditions, $\mathrm{ind}_{H/F}\varphi$ is irreducible if and only if $\varphi^2 \neq 1_H$. Indeed the condition $\varphi|F^\times = \chi_{H/F}$ implies that $\varphi \circ N_{H/F} = 1_F$ and consequently that $\varphi \circ \gamma = \varphi^{-1}$, where γ denotes the nontrivial automorphism of H over F. Hence the standard criterion $\varphi \neq \varphi \circ \gamma$ for the irreducibility of $\mathrm{ind}_{H/F}\varphi$ is equivalent to the condition $\varphi \neq \varphi^{-1}$, i.e. $\varphi^2 \neq 1_H$.

(ii) Let π be a dihedral representation of $\mathrm{Gal}(\overline{F}/F)$, viewed as a map

$$\pi : \mathrm{Gal}(\overline{F}/F) \to \mathrm{O}(2,\mathbb{R}).$$

Since π is (absolutely) irreducible the image of π is not contained in $\mathrm{SO}(2,\mathbb{R})$. It follows that the fixed field of $\pi^{-1}(\mathrm{SO}(2,\mathbb{R}))$ is a quadratic extension H of F and that $\pi \cong \mathrm{ind}_{H/F}\varphi$ for some character φ of $H^\times$. Then $\det\pi = \chi_{H/F}$, whence $\varphi|F^\times = 1_F$ by (1.5). Also $\mathrm{res}_{H/F}\pi \cong \varphi \oplus \varphi^{-1}$, because the nontrivial coset of $\mathrm{SO}(2,\mathbb{R})$ in $\mathrm{O}(2,\mathbb{R})$ acts on $\mathrm{SO}(2,\mathbb{R})$ by inversion. Since the image of π is nonabelian $\mathrm{res}_{H/F}\pi$ is not scalar, and consequently $\varphi^2 \neq 1_H$.

For the converse we use the fact that an irreducible representation with finite image and real-valued character is either symplectic or realizable over $\mathbb{R}$. Suppose that H is a quadratic extension of F and φ a character of $H^\times$ such that $\varphi|F^\times = 1_F$ and $\varphi^2 \neq 1_H$. The condition $\varphi|F^\times = 1_F$ implies first that φ has finite order and second that $\varphi \circ \gamma = \varphi^{-1}$, where γ is the nontrivial automorphism of H over F. Since $\varphi \neq \varphi^{-1}$ it follows that $\varphi \circ \gamma \neq \varphi$. Therefore $\mathrm{ind}_{H/F}\varphi$ is irreducible. Also $\det(\mathrm{ind}_{H/F}\varphi) = \chi_{H/F}$ by (1.5) and

$$\mathrm{tr}(\mathrm{ind}_{H/F}\varphi)(x) = \begin{cases} \varphi(x) + \varphi^{-1}(x) & \text{if } x \in \mathrm{Gal}(\overline{F}/H) \\ 0 & \text{otherwise} \end{cases}$$

by the formula for an induced character. Thus $\mathrm{ind}_{H/F}\varphi$ is a two-dimensional irreducible representation with finite image, real-valued character, and nontrivial determinant. Since a symplectic representation has trivial determinant we conclude that $\mathrm{ind}_{H/F}\varphi$ is realizable over $\mathbb{R}$.

REMARK. It can happen that $\mathrm{ind}_{H/F}\varphi$ is dihedral even though $\varphi^2 = 1_H$. Proposition 1 merely asserts that $\mathrm{ind}_{H/F}\varphi$ can also be written as $\mathrm{ind}_{H'/F}\varphi'$ with H'/F quadratic, $\varphi'|F^\times = 1_F$, and $(\varphi')^2 \neq 1_{H'}$.

Statement of Theorem 1

To state the theorem, fix a nonarchimedean local field F of characteristic 0 and let H be the unramified quadratic extension of F. Put $\eta = \chi_{H/F}$. We also fix a two-dimensional symplectic representation σ of $\mathrm{Gal}(\overline{F}/F)$ which is irreducibly induced from a tame character of $H^\times$. Thus σ is irreducible, symplectic, and of the form

$$\sigma = \mathrm{ind}_{H/F}\varphi,$$

where φ is a character of $H^\times$ with $a(\varphi) = 1$. According to Proposition 1, $\varphi|F^\times = \eta$ and $\varphi^2 \neq 1_H$. Let θ denote the unramified quadratic character of $H^\times$, so that $\theta|F^\times = \eta$, and put

$$\hat{\varphi} = \theta\varphi$$

and

$$\hat{\sigma} = \mathrm{ind}_{H/F}\hat{\varphi}.$$

Then $\hat{\varphi}|F^\times = 1_F$ and $\hat{\varphi}^2 \neq 1_H$. Consequently, Proposition 1 implies that $\hat{\sigma}$ is dihedral.

Let $\mathcal{O}_H$ denote the ring of integers of H. Since H is unramified over F there is a unit $u_{H/F} \in \mathcal{O}_H^\times$ such that $H = F(u_{H/F})$ and $u_{H/F}^2 \in F$. The value of $\varphi(u_{H/F})$ is independent of the choice of $u_{H/F}$, because $\varphi|F^\times = \eta$ and therefore $\varphi|\mathcal{O}_F^\times$ is trivial. For the same reason, $\varphi(u_{H/F}) = \pm 1$.

Given representations ρ and τ of $\mathrm{Gal}(\overline{F}/F)$, we define their inner product $\langle \rho, \tau \rangle$ by

$$\langle \rho, \tau \rangle = \langle \mathrm{tr}\rho, \mathrm{tr}\,\tau \rangle,$$

where on the right-hand side ρ and τ are viewed as representations of $\mathrm{Gal}(K/F)$ for some finite Galois extension K of F and $\langle \mathrm{tr}\rho, \mathrm{tr}\,\tau \rangle$ is the usual inner product on characters of $\mathrm{Gal}(K/F)$. Thus if ρ is irreducible then $\langle \rho, \tau \rangle$ is just the multiplicity of ρ in τ.

We denote 1_F simply by 1.

THEOREM 1. *Let τ be a representation of* $\mathrm{Gal}(\overline{F}/F)$ *with real-valued character. Then*

$$W(\sigma \otimes \tau) = \det\tau(-1)\varphi(u_{H/F})^{\dim\tau}(-1)^{\langle 1,\tau\rangle + \langle \eta,\tau\rangle + \langle \hat{\sigma},\tau\rangle}.$$

To prove the theorem it will suffice to treat two special cases:
(i) τ is symplectic.
(ii) τ is realizable over $\mathbb{R}$.
Indeed every representation of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character is a direct sum of representations of types (i) and (ii), and as functions of τ, both sides of the formula to be proved are multiplicative across direct sums. We begin by proving the theorem for representations of type (i).

The case where τ is symplectic

Suppose that τ is symplectic. Then $\det\tau$ is trivial, $\dim\tau$ is even, and also $\langle\xi,\tau\rangle$ is even for any irreducible representation ξ of $\mathrm{Gal}(\overline{F}/F)$ which is realizable over $\mathbb{R}$. Hence the right-hand side of the formula to be proved is 1, and Theorem 1 follows in this case from a general fact:

PROPOSITION 2. *If σ and τ are symplectic representations of* $\mathrm{Gal}(\overline{F}/F)$, *then* $W(\sigma\otimes\tau)=1$.

Proof. Let V and W be the spaces of σ and τ. Thus V and W are equipped with nondegenerate invariant symplectic forms, and we may view σ and τ as maps $\mathrm{Gal}(\overline{F}/F)\to\mathrm{Sp}(V)$ and $\mathrm{Gal}(\overline{F}/F)\to\mathrm{Sp}(W)$. Put $U=V\otimes W$ and $\pi=\sigma\otimes\tau$. The tensor product of the symplectic forms on V and W is a nondegenerate symmetric bilinear form on U which is invariant under π. Furthermore, π has trivial determinant, so that we may view π as a map $\mathrm{Gal}(\overline{F}/F)\to\mathrm{SO}(U)$. Hence by Deligne's theorem on root numbers of orthogonal representations ([3], p. 301), $W(\pi)$ is 1 or -1 according as π does or does not lift to the spin cover $\mathrm{Spin}(U)\to\mathrm{SO}(U)$. Now the natural embedding

$$\mathrm{Sp}(V)\times\mathrm{Sp}(W)\hookrightarrow\mathrm{SO}(U) \tag{1.6}$$

afforded by the tensor product does lift to $\mathrm{Spin}(U)$, because the fundamental group of $\mathrm{Sp}(V)$ and of $\mathrm{Sp}(W)$ – hence also of $\mathrm{Sp}(V)\times\mathrm{Sp}(W)$ – is trival. Since (1.6) lifts to $\mathrm{Spin}(U)$, so does π, and therefore $W(\pi)=1$.

REMARK. For later reference we note that Deligne's theorem (hence also Proposition 2) holds with $\mathrm{Gal}(\overline{F}/F)$ replaced by $\mathcal{W}(\overline{F}/F)$, cf. [3], p. 314.

The theorem of Fröhlich-Queyrut

To prove Theorem 1 in the case where τ is realizable over $\mathbb{R}$ we will need the following result:

PROPOSITION 3. *Let K be a nonarchimedean local field of characteristic* 0, *L the unramified quadratic extension of K, and λ a character of $L^\times$ such that $\lambda|K^\times=\chi_{L/K}$. Then*

$$W(\lambda)W(\mathrm{ind}_{L/K}1_L)=(-1)^{a(\lambda)}\lambda(u_{L/K}),$$

where $u_{L/K} \in \mathcal{O}_L^\times$ is any element such that $L = K(u_{L/K})$ and $u_{L/K}^2 \in K$.

Proof. Let ϑ be the unramified quadratic character of $L^\times$. Then $\vartheta|K^\times = \chi_{L/K}$. Hence putting $\hat{\lambda} = \vartheta\lambda$ we have $\hat{\lambda}|K^\times = 1_K$, so that

$$W(\hat{\lambda}) = \hat{\lambda}(u_{L/K}) = \lambda(u_{L/K})$$

by the theorem of Fröhlich-Queyrut ([4], Thm. 3). On the other hand, let ϖ be a uniformizer of K and let $n(\psi_K)$ be the largest integer n such that ψ_K is trivial on $\varpi^{-n}\mathcal{O}_K$. Since ϑ is unramified,

$$W(\hat{\lambda}) = W(\vartheta\lambda) = \vartheta(\varpi)^{n(\psi_K)+a(\lambda)}W(\lambda) = (-1)^{n(\psi_K)+a(\lambda)}W(\lambda).$$

Comparison with our previous formula for $W(\hat{\lambda})$ yields

$$(-1)^{n(\psi_K)}W(\lambda) = (-1)^{a(\lambda)}\lambda(u_{L/K}).$$

This is the stated result, because

$$W(\mathrm{ind}_{L/K}1_L) = W(1_K \oplus \chi_{L/K}) = W(\chi_{L/K}) = (-1)^{n(\psi_K)}.$$

The case where τ is realizable over $\mathbb{R}$

In the case where τ is realizable over $\mathbb{R}$ we first prove a preliminary version of Theorem 1 in which the exponent $\langle 1, \tau\rangle + \langle \eta, \tau\rangle + \langle \hat{\sigma}, \tau\rangle$ is replaced by $a(\sigma \otimes \tau)/2 - a(\tau)$. To see that the latter expression is an integer, write $\sigma = \mathrm{ind}_{H/F}\varphi$. Then $\sigma \otimes \tau = \mathrm{ind}_{H/F}(\varphi \otimes \mathrm{res}_{H/F}\tau)$ and consequently

$$a(\sigma \otimes \tau) = f(H/F)a(\varphi \otimes \mathrm{res}_{H/F}\tau) = 2a(\varphi \otimes \mathrm{res}_{H/F}\tau)$$

by (1.2).

PROPOSITION 4. *If τ is realizable over $\mathbb{R}$, then*

$$W(\sigma \otimes \tau) = \det\tau(-1)\varphi(u_{H/F})^{\dim\tau}(-1)^{a(\sigma\otimes\tau)/2-a(\tau)}.$$

Proof. As functions of τ, both sides of the formula to be proved define homomorphisms from the Grothendieck group of virtual representations of $\mathrm{Gal}(\overline{F}/F)$ realizable over the reals into the group $\{\pm 1\}$. Hence it suffices to verify the formula on a set of generators of the Grothendieck group. In fact applying Serre's induction theorem ([13], Prop. 2, p. 177) we see that we may restrict our attention to representations of the form $\tau = \mathrm{ind}_{K/F}\pi$, where K is a finite extension of F and π a representation of $\mathrm{Gal}(\overline{F}/K)$ of one of the following types:

(a) $\pi = 1_K$.

(b) π is a quadratic character of $\mathrm{Gal}(\overline{F}/K)$.
(c) $\pi = \chi \oplus \overline{\chi}$, where χ is a character of $\mathrm{Gal}(\overline{F}/K)$ of order $\geqslant 3$.
(d) π is dihedral.

Before turning to a consideration of cases we observe that if $\tau = \mathrm{ind}_{K/F}\pi$ then

$$\sigma \otimes \tau = \mathrm{ind}_{K/F}(\pi \otimes \mathrm{res}_{K/F}\sigma), \tag{1.7}$$

whence

$$W(\sigma \otimes \tau) = W(\pi \otimes \mathrm{res}_{K/F}\sigma)W(\mathrm{ind}_{K/F}1_K)^{2\dim\pi} \tag{1.8}$$

by (1.4). Also

$$\begin{aligned} W(\mathrm{ind}_{K/F}1_K)^{2\dim\pi} &= (W(\mathrm{ind}_{K/F}1_K)W((\mathrm{ind}_{K/F}1_K)^*))^{\dim\pi} \\ &= \det(\mathrm{ind}_{K/F}1_K)(-1)^{\dim\pi} \end{aligned} \tag{1.9}$$

because the product of the root number of a representation and the root number of its contragredient is the determinant at -1 (cf. [12], p. 144 or [18], (3.4.7)). Now according to the formula for the determinant of an induced representation, the final expression in (1.9) is $\det\tau(-1)/\det\pi(-1)$. Hence (1.8) and (1.9) give

$$W(\sigma \otimes \tau) = W(\pi \otimes \mathrm{res}_{K/F}\sigma)\frac{\det\tau(-1)}{\det\pi(-1)}. \tag{1.10}$$

On the other hand, by (1.2) we have

$$a(\tau) = d(K/F)\dim\pi + f(K/F)a(\pi)$$

and also

$$a(\sigma \otimes \tau) = 2d(K/F)\dim\pi + f(K/F)a(\pi \otimes \mathrm{res}_{K/F}\sigma)$$

via (1.7). Hence

$$a(\sigma \otimes \tau)/2 - a(\tau) = f(K/F)(a(\pi \otimes \mathrm{res}_{K/F}\sigma)/2 - a(\pi)). \tag{1.11}$$

Combining (1.10) and (1.11), we conclude that for $\tau = \mathrm{ind}_{K/F}\pi$ the assertion of Proposition 4 is equivalent to the formula

$$\begin{aligned} &W(\pi \otimes \mathrm{res}_{K/F}\sigma) \\ &\quad = \det\pi(-1)\varphi(u_{H/F})^{[K:F]\dim\pi}(-1)^{f(K/F)(a(\pi\otimes\mathrm{res}_{K/F}\sigma)/2-a(\pi))}. \end{aligned} \tag{1.12}$$

Next we observe that (1.12) is satisfied whenever K contains H. Indeed if K contains H then

$$\mathrm{res}_{K/F}\sigma = (\varphi \circ N_{K/H}) \oplus (\varphi \circ N_{K/H})^{-1},$$

so that

$$\begin{aligned} W(\pi \otimes \mathrm{res}_{K/F}\sigma) &= \det(\pi \otimes (\varphi \circ N_{K/F}))(-1) \\ &= \det \pi(-1)(\varphi \circ N_{K/F}(-1))^{\dim \pi} = \det \pi(-1) \end{aligned}$$

(recall that $\varphi|\mathcal{O}_F^\times$ is trivial). This result does coincide with (1.12), because $[K : F] = 2[K : H]$ and $f(K/F) = 2f(K/H)$.

It remains to prove (1.12) for π as in (a), (b), (c), or (d), and K a finite extension of F not containing H. The latter assumption implies that $f(K/F)$ is odd, whence (1.12) becomes

$$\begin{aligned} &W(\pi \otimes \mathrm{res}_{K/F}\sigma) \\ &\quad = \det \pi(-1)\varphi(u_{H/F})^{[K:F]\dim \pi}(-1)^{a(\pi \otimes \mathrm{res}_{K/F}\sigma)/2 - a(\pi)}. \end{aligned} \tag{1.13}$$

Put $L = HK$ and $\lambda = \varphi \circ N_{L/H}$, so that L is the unramified quadratic extension of K and $\mathrm{res}_{K/F}\sigma = \mathrm{ind}_{L/K}\lambda$. Then

$$\pi \otimes \mathrm{res}_{K/F}\sigma = \mathrm{ind}_{L/K}((\mathrm{res}_{L/K}\pi) \otimes \lambda).$$

Consequently

$$a(\pi \otimes \mathrm{res}_{K/F}\sigma) = 2a((\mathrm{res}_{L/K}\pi) \otimes \lambda) \tag{1.14}$$

and

$$W(\pi \otimes \mathrm{res}_{K/F}\sigma) = W((\mathrm{res}_{L/K}\pi) \otimes \lambda)W(\mathrm{ind}_{L/K}1_L)^{\dim \pi} \tag{1.15}$$

by (1.2) and (1.4) respectively. After substitution of (1.14) and (1.15) into (1.13) the statement to be proved is

$$\begin{aligned} &W(\lambda \otimes \mathrm{res}_{L/K}\pi)W(\mathrm{ind}_{L/K}1_L)^{\dim \pi} \\ &\quad = \det \pi(-1)\varphi(u_{H/F})^{[K:F]\dim \pi}(-1)^{a(\lambda \otimes \mathrm{res}_{L/K}\pi) - a(\pi)}. \end{aligned} \tag{1.16}$$

Note that

$$\lambda|K^\times = \chi_{L/K} \tag{1.17}$$

since $\chi_{L/K} = \chi_{H/F} \circ N_{K/F} = \eta \circ N_{K/F}$. We now proceed to a consideration of cases.

(a) If $\pi = 1_K$ then (1.16) follows from (1.17) and Proposition 3, because $L = K(u_{H/F})$ and

$$\lambda(u_{H/F}) = \varphi(N_{L/H}(u_{H/F})) = \varphi(u_{H/F})^{[K:F]}.$$

(b) If π is a quadratic character of $\mathrm{Gal}(\overline{F}/K)$ with kernel $\mathrm{Gal}(\overline{F}/K')$ then

$$\pi = \mathrm{ind}_{K'/K} 1_{K'} - 1_K$$

as virtual representations. In view of the transitivity of induction the proof of the proposition for $\tau = \mathrm{ind}_{K/F}\pi$ reduces to the case treated in (a).

(c) If $\pi = \chi \oplus \overline{\chi}$ then it is more convenient to verify (1.13) than (1.16). Since σ is self-contragredient we have $(\chi \otimes \mathrm{res}_{K/F}\sigma)^* = \overline{\chi} \otimes \mathrm{res}_{K/F}\sigma$, whence

$$W(\pi \otimes \mathrm{res}_{K/F}\sigma) = \det(\chi \otimes \mathrm{res}_{K/F}\sigma)(-1) = \chi^2(-1) = 1.$$

The right-hand side of (1.13) is also 1, because $\det\pi(-1) = 1$, $\dim\pi = 2$, $a(\pi) = 2a(\chi)$, and $a(\pi \otimes \mathrm{res}_{K/F}\sigma) = 4a((\chi \circ N_{L/K})\lambda)$. This last point follows from (1.2) on noting that

$$\begin{aligned} a(\pi \otimes \mathrm{res}_{K/F}\sigma) &= a(\chi \otimes \mathrm{res}_{K/F}\sigma) + a((\chi \otimes \mathrm{res}_{K/F}\sigma)^*) \\ &= 2a(\chi \otimes \mathrm{res}_{K/F}\sigma) \end{aligned}$$

and that $\chi \otimes \mathrm{res}_{K/F}\sigma = \mathrm{ind}_{L/K}((\chi \circ N_{L/K})\lambda)$.

(d) If π is dihedral then by Proposition 1 we can write $\pi = \mathrm{ind}_{M/K}\mu$ with a quadratic extension M of K and a character μ of $M^\times$ such that $\mu|K^\times = 1_K$. There are now two cases, according as $L = M$ or $L \neq M$.

Case 1: $L = M$. Let γ be the nontrivial automorphism of L over K. The condition $\mu|K^\times = 1_K$ implies that $\mu \circ \gamma = \mu^{-1}$. Since $\pi = \mathrm{ind}_{L/K}\mu$ it follows that $\mathrm{res}_{L/K}\pi = \mu \oplus \mu^{-1}$. Also $a(\pi) = 2a(\mu)$ and $\det\pi(-1) = \chi_{L/K}(-1) = 1$ because L is unramified over K. Thus the assertion of (1.16) is that

$$W(\lambda\mu)W(\lambda\mu^{-1})W(\mathrm{ind}_{L/K}1_L)^2 = (-1)^{a(\lambda\mu)+a(\lambda\mu^{-1})}.$$

Since $\mu|K^\times = 1_K$ this follows from (1.17) and Proposition 3.

Case 2: $L \neq M$. In this case LM is a biquadratic extension of K. Let P be the third quadratic extension of K contained in LM. Since $LM = LP$ and L is unramified over K the extension LM/P is unramified and $LM = P(u_{H/F})$. Furthermore, the character ν of $(LM)^\times$ defined by

$$\nu = (\lambda \circ N_{LM/L})(\mu \circ N_{LM/M})$$

satisfies

$$\nu|P^\times = \chi_{L/K} \circ N_{P/K} = \chi_{LM/P}$$

by (1.17). Therefore

$$W(\nu)W(\mathrm{ind}_{LM/P}1_{LM}) = (-1)^{a(\nu)}\nu(u_{H/F})$$

by Proposition 3. In fact

$$W(\nu)W(\mathrm{ind}_{LM/P}1_{LM}) = (-1)^{a(\nu)} \tag{1.18}$$

because $\nu(u_{H/F}) = \varphi(u_{H/F}^2)^{[K:F]}\mu(-u_{H/F}^2) = 1$.

On the other hand,

$$\lambda \otimes \mathrm{res}_{L/K}\pi = \lambda \otimes \mathrm{ind}_{LM/L}(\mu \circ N_{LM/M}) = \mathrm{ind}_{LM/L}\nu.$$

Therefore

$$a(\lambda \otimes \mathrm{res}_{L/K}\pi) = d(LM/L) + a(\nu) = d(M/K) + a(\nu) \tag{1.19}$$

and

$$W(\lambda \otimes \mathrm{res}_{L/K}\pi) = W(\nu)W(\mathrm{ind}_{LM/L}1_{LM}) \tag{1.20}$$

by (1.2) and (1.4). Formula (1.4) also tells us that

$$\begin{aligned} W(\mathrm{ind}_{LM/K}1_{LM}) &= W(\mathrm{ind}_{L/K}(\mathrm{ind}_{LM/L}1_{LM})) \\ &= W(\mathrm{ind}_{LM/L}1_{LM})W(\mathrm{ind}_{L/K}1_L)^2. \end{aligned}$$

Replacing L by P everywhere in the preceding calculation, and then using the fact that $LM = PM$, we deduce that

$$\begin{aligned} &W(\mathrm{ind}_{LM/L}1_{LM})W(\mathrm{ind}_{L/K}1_L)^2 \\ &\quad = W(\mathrm{ind}_{LM/P}1_{LM})W(\mathrm{ind}_{P/K}1_P)^2. \end{aligned} \tag{1.21}$$

But

$$W(\mathrm{ind}_{P/K}1_P)^2 = \det\pi(-1), \tag{1.22}$$

because $\mathrm{ind}_{P/K}1_P = 1_K \oplus \chi_{P/K}$ and

$$\begin{aligned} W(\chi_{P/K})^2 &= \chi_{P/K}(-1) = \chi_{L/K}\chi_{M/K}(-1) \\ &= \chi_{L/K}(-1)\det\pi(-1) = \det\pi(-1) \end{aligned}$$

($\chi_{L/K}$ is unramified). Together, (1.21) and (1.22) give

$$W(\mathrm{ind}_{L/K}1_L)^2 = \det\pi(-1)\frac{W(\mathrm{ind}_{LM/P}1_{LM})}{W(\mathrm{ind}_{LM/L}1_{LM})}.$$

Combining this with (1.18), (1.19), and (1.20), we conclude that

$$W(\lambda \otimes \mathrm{res}_{L/K}\pi)W(\mathrm{ind}_{L/K}1_L)^2 = \det\pi(-1)(-1)^{a(\lambda\otimes\mathrm{res}_{L/K}\pi)-d(M/K)}. \tag{1.23}$$

Now $a(\pi) \equiv d(M/K) \pmod 2$: this can be seen either by using the fact that $a(\pi) = d(M/K) + a(\mu)$ and $\mu|K^\times = 1_K$ or by noting that $d(M/K) = a(\chi_{M/K}) = a(\det\pi)$ and quoting a theorem of Serre ([13], thm. 1, p. 173). Thus the exponent $d(M/K)$ in (1.23) can be replaced by $a(\pi)$, and (1.16) follows.

Completion of the proof

The final step of the proof depends on a general fact about conductors.

LEMMA . *Let π be an irreducible representation of* $\mathrm{Gal}(\overline{F}/F)$ *and φ a tamely ramified character of* $\mathrm{Gal}(\overline{F}/F)$. *If $a(\varphi\otimes\pi) \neq a(\pi)$ then π is one-dimensional and either π or $\varphi\otimes\pi$ is unramified.*

Proof. Let V be the space of π and I the inertia subgroup of $\mathrm{Gal}(\overline{F}/F)$, and let $V^{\pi(I)}$ be the subspace of V consisting of vectors fixed by I. Then

$$a(\pi) = \dim V - \dim V^{\pi(I)} + \text{higher-order terms},$$

where the 'higher-order terms' depend only on the action of the higher ramification groups on V. Since φ is tame, the assumption that $a(\varphi\otimes\pi) \neq a(\pi)$ means that

$$\dim V^{(\varphi\otimes\pi)(I)} \neq \dim V^{\pi(I)}$$

and hence in particular that

$$V^{(\varphi\otimes\pi)(I)} \neq V^{\pi(I)}.$$

As I is normal in $\mathrm{Gal}(\overline{F}/F)$ these spaces are invariant subspaces for the irreducible representations $\varphi\otimes\pi$ and π respectively. Consequently, one of the two spaces coincides with $\{0\}$ and the other with V. Hence one of $\varphi\otimes\pi$ and π is ramified and the other unramified. If π is unramified then π can be viewed as an irreducible representation of the procyclic group $\mathrm{Gal}(\overline{F}/F)/I$, so that π is one-dimensional. On the other hand, if $\varphi\otimes\pi$ is unramified, then $\pi|I$ acts by scalar multiplication by the character $\varphi^{-1}|I$, whence $\pi(I)$ is central in $\pi(\mathrm{Gal}(\overline{F}/F))$. Since $\pi(\mathrm{Gal}(\overline{F}/F))/\pi(I)$ is cyclic it follows that $\pi(\mathrm{Gal}(\overline{F}/F))$ is abelian and again we conclude that π is one-dimensional.

The following proposition completes the proof of Theorem 1.

PROPOSITION 5. *If τ is a representation of* $\mathrm{Gal}(\overline{F}/F)$ *which is realizable over* $\mathbb{R}$ *then*

$$a(\sigma \otimes \tau)/2 - a(\tau) \equiv \langle \tau, 1 \rangle + \langle \tau, \eta \rangle + \langle \tau, \hat{\sigma} \rangle \pmod 2.$$

Proof. Since the statement to be proved is additive in τ, we may assume that τ is either irreducible or of the form $\pi \oplus \pi^*$ with π irreducible. In the latter case τ is symplectic and the required congruence follows from Theorem 1 (already proved for symplectic representations) and Proposition 4. Henceforth we assume that τ is irreducible. In this case the statement to be proved is

$$a(\sigma \otimes \tau)/2 - a(\tau) \equiv \begin{cases} 1 \pmod 2 & \text{if } \tau \cong 1, \eta, \text{or } \hat{\sigma} \\ 0 \pmod 2 & \text{otherwise.} \end{cases} \tag{1.24}$$

Let $\pi = \mathrm{res}_{H/F}\tau$. Then

$$a(\sigma \otimes \tau) = a((\mathrm{ind}_{H/F}\varphi) \otimes \tau) = a(\mathrm{ind}_{H/F}(\varphi \otimes \pi)),$$

so that

$$a(\sigma \otimes \tau) = 2a(\varphi \otimes \pi).$$

Since $a(*)$ is invariant under restriction to the Galois group of an unramified extension, we also have

$$a(\tau) = a(\mathrm{res}_{H/F}\tau) = a(\pi).$$

Hence (1.24) is equivalent to

$$a(\varphi \otimes \pi) - a(\pi) \equiv \begin{cases} 1 \pmod 2 & \text{if } \tau \cong 1, \eta, \text{or } \hat{\sigma} \\ 0 \pmod 2 & \text{otherwise.} \end{cases} \tag{1.25}$$

Now if $\tau = 1$ or $\tau = \eta$ then $\pi = 1_F$ and $a(\varphi \otimes \pi) - a(\pi) = a(\varphi) = 1$, so that in particular $a(\varphi \otimes \pi) - a(\pi) \equiv 1 \pmod 2$ as stated in (1.25). On the other hand, if $\tau \cong \hat{\sigma}$ then

$$\pi \cong \hat{\varphi} \oplus \hat{\varphi}^{-1} = \theta \otimes (\varphi \oplus \varphi^{-1}),$$

and since θ is unramified we obtain

$$a(\varphi \otimes \pi) - a(\pi) = a(\varphi^2 \oplus 1_H) - a(\varphi \oplus \varphi^{-1}). \tag{1.26}$$

At this point we recall that $\varphi^2 \neq 1_H$. Since $(\varphi | F^\times)^2 = \eta^2 = 1_F$ and $H^\times = F^\times \mathcal{O}_H^\times$, it follows that $\varphi^2 | \mathcal{O}_H^\times$ is nontrivial, or in other words that φ^2 is ramified. Thus $a(\varphi^2) = 1$ and the right-hand side of (1.26) is -1. Hence (1.25) holds also for $\tau \cong \hat{\sigma}$.

Next suppose that τ is not isomorphic to $1, \eta$, or $\hat{\sigma}$. We claim that $a(\varphi \otimes \pi)$ and $a(\pi)$ are equal, whence congruent modulo 2. To see this, first consider the case where π is irreducible. If $a(\varphi \otimes \pi) \neq a(\pi)$, then π is one-dimensional by the lemma, and consequently τ is also one-dimensional. Since τ is realizable over $\mathbb{R}$ but different from 1 and η, we deduce that τ is a ramified quadratic character. As H is unramified over F it follows that π is also a ramified quadratic character. Since $\varphi^2|\mathcal{O}_H^\times$ is nontrivial, as we saw a moment ago, it follows that π and $\varphi\pi$ are both ramified, contradicting the lemma. Next suppose that π is reducible. Since τ is irreducible we can write $\pi = \kappa \oplus \kappa'$ with irreducible representations κ and κ' such that $\tau = \mathrm{ind}_{H/F}\kappa = \mathrm{ind}_{H/F}\kappa'$. If $a(\varphi \otimes \pi) \neq a(\pi)$ then $a(\varphi \otimes \kappa) \neq a(\kappa)$ or $a(\varphi \otimes \kappa') \neq a(\kappa')$; say $a(\varphi \otimes \kappa) \neq a(\kappa)$. Then κ is one-dimensional by the lemma. If κ is unramified we can write $\kappa = \mathrm{res}_{H/F}\iota$ with an unramified character ι of $\mathrm{Gal}(\overline{F}/F)$. Then $\tau = \mathrm{ind}_{H/F}\kappa = \iota \oplus \eta\iota$, contradicting the irreducibility of τ. Hence κ is ramified. The lemma now implies that $\varphi\kappa$ is unramified. Consequently, $\hat{\varphi}\kappa$ is also unramified, so that $\hat{\varphi}\kappa = \mathrm{res}_{H/F}\iota$ for some unramified character ι of $\mathrm{Gal}(\overline{F}/F)$. Then

$$\tau = \mathrm{ind}_{H/F}\kappa = \mathrm{ind}_{H/F}(\hat{\varphi}^{-1}\mathrm{res}_{H/F}\iota) = \iota \otimes \hat{\sigma}. \tag{1.27}$$

Taking determinants, we obtain $\det\tau = \iota^2 \det\hat{\sigma}$, and since τ and $\hat{\sigma}$ are both realizable over $\mathbb{R}$, we deduce that $\iota^4 = 1$. We now consider two possibilities: $\iota^2 = 1$ or $\iota^2 \neq 1$. If $\iota^2 = 1$ then ι is the unramified quadratic character η of $F^\times$, whence $\mathrm{res}_{H/F}\iota$ is trivial and the conclusion of (1.27) becomes $\tau = \hat{\sigma}$, contrary to hypothesis. On the other hand, if $\iota^2 \neq 1$, then ι is one of the two unramified quartic characters of $F^\times$, whence $\mathrm{res}_{H/F}\iota$ is the unramified quadratic character θ of $H^\times$. Therefore (1.27) becomes

$$\tau = \mathrm{ind}_{H/F}(\hat{\varphi}^{-1}\theta) = \mathrm{ind}_{H/F}\varphi^{-1} = \sigma.$$

Since τ is realizable over $\mathbb{R}$ whereas σ is irreducible symplectic, we have a contradiction here too, and we conclude that our original hypothesis $a(\varphi \otimes \pi) \neq a(\pi)$ was in error.

2. Complementary calculations

As before, F denotes a nonarchimedean local field of characteristic 0. If n is a positive integer then $\mathrm{sp}(n)$ denotes the representation of $\mathcal{W}'(\overline{F}/F)$ commonly referred to as the 'special' or 'Steinberg' representation of dimension n.

PROPOSITION 6. *Let τ be a representation of* $\mathrm{Gal}(\overline{F}/F)$ *with real-valued character. Then*

$$W(\mathrm{sp}(2) \otimes \tau) = \det\tau(-1)(-1)^{\langle 1,\tau\rangle}.$$

Proof. We may assume that τ is either irreducible or of the form $\pi \oplus \pi^*$ with π irreducible and $\pi \ncong \pi^*$. Suppose first that τ is irreducible. If τ is ramified then the corollary on p. 146 of [12] gives

$$W(\mathrm{sp}(2) \otimes \tau) = W(\tau)^2 = W(\tau)W(\tau^*) = \det \tau(-1).$$

This is the stated formula, because $\langle 1, \tau \rangle = 0$. If τ is unramified then τ is an irreducible representation of the procyclic group $\mathrm{Gal}(\overline{F}/F)/I$, hence equal to a character, hence equal to a character χ with $\chi^2 = 1$ (since tr π is real-valued). In this case [12] gives

$$W(\mathrm{sp}(2) \otimes \tau) = W(\mathrm{sp}(2) \otimes \chi) = \begin{cases} -1 & \text{if } \chi = 1 \\ 1 & \text{if } \chi \neq 1. \end{cases}$$

Again this agrees with the stated formula, for as χ is unramified we have $\chi(-1) = 1$.

The case where $\tau = \pi \oplus \pi^*$ is similar. If π is ramified then

$$W(\mathrm{sp}(2) \otimes \tau) = (W(\pi)W(\pi^*))^2 = \det \pi(-1)^2 = 1 = \det \tau(-1),$$

and if π is an unramified character χ then

$$W(\mathrm{sp}(2) \otimes \tau) = W(\mathrm{sp}(2) \otimes \chi)W(\mathrm{sp}(2) \otimes \overline{\chi}) = 1 = \det \tau(-1).$$

Recall that both characters of $F^\times$ and representations of $\mathrm{Gal}(\overline{F}/F)$ can be viewed as representations of $\mathcal{W}(\overline{F}/F)$.

PROPOSITION 7. *Let χ be a character of $F^\times$ and τ a representation of* $\mathrm{Gal}(\overline{F}/F)$ *with real-valued character. Then*

$$W((\chi \oplus \chi^{-1}) \otimes \tau) = \chi(-1)^{\dim \tau} \det \tau(-1).$$

Proof. This follows from the calculation

$$W((\chi \oplus \chi^{-1}) \otimes \tau) = W(\chi \otimes \tau)W((\chi \otimes \tau)^*) = \det(\chi \otimes \tau)(-1)$$

and the formula for the determinant of a tensor product.

3. Elliptic curves

Now let F be an arbitrary local field of characteristic 0, archimedean or nonarchimedean, and put $\omega = |*|^{[F:\mathbb{Q}_p]}$, where $\mathbb{Q}_p$ is the topological closure of $\mathbb{Q}$ in F and $|*|$ is the absolute value on F extending the standard absolute value on $\mathbb{Q}_p$. In the nonarchimedean case ϖ denotes a uniformizer of F and v is the standard

valuation on F, normalized so that $v(\varpi) = 1$. Thus ω and v are related by the formula $\omega(x) = q^{-v(x)}$ with

$$q = p^{f(F/\mathbb{Q}_p)}.$$

Furthermore, if $q \equiv -1 \pmod{e}$ with $e = 3, 4$, or 6 then we define a representation $\hat{\sigma}_e$ of $\mathrm{Gal}(\overline{F}/F)$ by the formula

$$\hat{\sigma}_e = \mathrm{ind}_{H/F}\hat{\varphi}_e = \mathrm{ind}_{H/F}\hat{\varphi}_e^{-1},$$

where H is the unramified quadratic extension of F and $\hat{\varphi}_e$ is either of the tamely ramified characters of $H^\times$ of exact order e such that $\hat{\varphi}_e | F^\times = 1$. Such characters exist because e divides the quantity $q + 1 = (q^2 - 1)/(q - 1)$. Note also that $\hat{\sigma}_e$ is dihedral by Proposition 1. As before, we let $\eta = \chi_{H/F}$.

Let E be an elliptic curve over F, j its modular invariant, and Δ, c_4, and c_6 the covariants associated to some generalized Weierstrass equation for E over F. The representation of $\mathcal{W}'(\overline{F}/F)$ canonically associated to E over F will be denoted $\sigma'_{E/F}$ or simply $\sigma_{E/F}$ in cases where the distinction between $\mathcal{W}'(\overline{F}/F)$ and $\mathcal{W}(\overline{F}/F)$ is nonexistent or irrelevant. We define

$$a(E/F) = a(\sigma'_{E/F})$$

and

$$W(E/F) = W(\sigma'_{E/F}).$$

More generally, given an arbitrary representation τ of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character, we put

$$W(E/F, \tau) = W(\sigma'_{E/F} \otimes \tau). \tag{3.1}$$

Since $\sigma'_{E/F} \otimes \omega^{1/2}$ is symplectic and $W(*)$ is invariant under twisting by real powers of ω, the right-hand side of (3.1) is well-defined and equal to ± 1.

THEOREM 2. (i) *If $p = \infty$ then $W(E/F, \tau) = (-1)^{\dim \tau}$.*

(ii) *If $p < \infty$ and $v(j) < 0$ then*

$$W(E/F, \tau) = \det \tau(-1)\chi(-1)^{\dim \tau}(-1)^{\langle \chi, \tau \rangle},$$

where χ is the character of $F^\times$ associated to the extension $F(\sqrt{-c_6})$ of F. (Thus χ is trivial if E has split multiplicative reduction, $\chi = \eta$ if E has nonsplit multiplicative reduction, and χ is a ramified quadratic character of $F^\times$ if E has additive reduction.)

(iii) *If* $5 \leqslant p < \infty$ *and* $v(j) \geqslant 0$ *put*

$$e = \frac{12}{\gcd(v(\Delta), 12)} (= 1, 2, 3, 4, \text{or } 6)$$

and

$$\epsilon = \begin{cases} 1 & \text{if } f(F/\mathbb{Q}_p) \text{ is even or } e = 1 \\ \left(\frac{-1}{p}\right) & \text{if } f(F/\mathbb{Q}_p) \text{ is odd and } e = 2 \text{ or } 6 \\ \left(\frac{-3}{p}\right) & \text{if } f(F/\mathbb{Q}_p) \text{ is odd and } e = 3 \\ \left(\frac{-2}{p}\right) & \text{if } f(F/\mathbb{Q}_p) \text{ is odd and } e = 4. \end{cases}$$

Then

$$W(E/F, \tau) = \begin{cases} \det\tau(-1)\epsilon^{\dim\tau} & \text{if } q \equiv 1 \pmod{e} \\ \det\tau(-1)(-\epsilon)^{\dim\tau}(-1)^{\langle 1,\tau\rangle + \langle \eta,\tau\rangle + \langle \hat{\sigma},\tau\rangle} & \text{if } e = 3, 4, \text{or } 6 \text{ and } q \equiv -1 \pmod{e}, \end{cases}$$

where $\hat{\sigma} = \hat{\sigma}_e$.

Proof. (i) If $F = \mathbb{C}$ then τ is isomorphic to the direct sum of $\dim\tau$ copies of the trivial character, so that

$$W(E/F, \tau) = W(\sigma_{E/\mathbb{C}} \otimes \tau) = W(\sigma_{E/\mathbb{C}})^{\dim\tau}. \tag{3.2}$$

Identifying $\mathcal{W}(\mathbb{C}/\mathbb{C})$ with $\mathbb{C}^\times$, we have $\sigma_{E/\mathbb{C}} \cong \varphi \oplus \overline{\varphi}$, where φ is the character $z \mapsto z^{-1}$. Hence

$$W(\sigma_{E/\mathbb{C}}) = W(\varphi)W(\overline{\varphi}) = i^2 = -1. \tag{3.3}$$

Together, (3.2) and (3.3) give the stated formula.

If $F = \mathbb{R}$ then τ is the direct sum of $\dim\tau$ characters drawn from the set $\{1_{\mathbb{R}}, \text{sgn}\}$, where sgn is the sign character. Also $\sigma_{E/\mathbb{R}} = \text{ind}_{\mathbb{C}/\mathbb{R}}\varphi$ (induction from $\mathcal{W}(\mathbb{C}/\mathbb{C})$ to $\mathcal{W}(\mathbb{C}/\mathbb{R})$). Since $\text{res}_{\mathbb{C}/\mathbb{R}}\,\text{sgn} = 1_{\mathbb{C}}$ we have $\sigma_{E/\mathbb{R}} \otimes \text{sgn} \cong \sigma_{E/\mathbb{R}}$, and consequently (3.2) holds with $\mathbb{C}$ replaced by $\mathbb{R}$. As $W(\sigma_{E/\mathbb{R}}) = -1$ in this case too (cf. [11], p. 123), we obtain the stated formula once again.

(ii) In this case E has potential multiplicative reduction and $\sigma'_{E/F} \cong \text{sp}(2) \otimes \chi\omega^{-1}$ (cf. [12], p. 150, and [14], p. 276). Since twisting by ω^{-1} does not change $W(*)$,

$$W(E/F, \tau) = W(\text{sp}(2) \otimes (\chi \otimes \tau)).$$

The stated formula now follows from Proposition 6, because

$$\langle 1, \chi \otimes \tau \rangle = \langle \chi, \tau \rangle.$$

(iii) The argument is essentially a repetition of the proof of Proposition 2 of [11] with the added ingredient of Theorem 1.

Let $F^{\mathrm{unr}} \subset \overline{F}$ be the maximal unramified extension of F and $L \subset \overline{F}$ the minimal extension of F^{unr} over which E acquires good reduction ([16], p. 498, Cor. 3). We shall view $\sigma_{E/F}$ as a faithful representation of the group

$$\mathcal{W}(L/F) = \mathcal{W}(\overline{F}/F)/\mathrm{Gal}(\overline{F}/L).$$

The structure of $\mathcal{W}(L/F)$ can be described as follows: If we write $\langle \Phi \rangle$ for the infinite cyclic group generated by an inverse Frobenius element $\Phi \in \mathcal{W}(L/F)$ and Λ for the image in $\mathcal{W}(L/F)$ of the inertia subgroup $\mathrm{Gal}(\overline{F}/F^{\mathrm{unr}})$ of $\mathcal{W}(\overline{F}/F)$, then

$$\Lambda \cong \mathrm{Gal}(L/F^{\mathrm{unr}}) \cong \mathbb{Z}/e\mathbb{Z} \tag{3.4}$$

(cf. [14], p. 312) and consequently

$$\mathcal{W}(L/F) \cong \Lambda \rtimes \langle \Phi \rangle \cong (\mathbb{Z}/e\mathbb{Z}) \rtimes \langle \Phi \rangle. \tag{3.5}$$

In particular, $\mathcal{W}(L/F)$ is abelian if and only if the semidirect product in (3.5) is actually direct, and in any case the group

$$\mathcal{W}(L/H) = \mathcal{W}(\overline{F}/H)/\mathrm{Gal}(\overline{F}/L) \cong \Lambda \times \langle \Phi^2 \rangle$$

is an abelian subgroup of $\mathcal{W}(L/F)$ of index 2.

Suppose now that $q \equiv 1 \pmod{e}$. Then the field $K = F(\Delta^{1/e})$ is abelian over F. On the other hand, the valuation of Δ relative to a uniformizer of K is divisible by 12. Since $p \geqslant 5$ it follows that E has good reduction over K and therefore also over $F^{\mathrm{unr}}K$, whence $L \subset F^{\mathrm{unr}}K$ by the minimality of L. Consequently $\mathcal{W}(L/F)$ is abelian, and since $\sigma_{E/F}$ is semisimple we have $\sigma_{E/F} \cong \xi \oplus \xi'$ with characters ξ, ξ' of $F^{\times}$. In fact since $\sigma_{E/F} \otimes \omega^{1/2}$ has trivial determinant we can write $\sigma_{E/F} \otimes \omega^{1/2} \cong \chi \oplus \chi^{-1}$ with $\chi = \xi \otimes \omega^{1/2}$, and then Proposition 7 gives

$$W(E/F, \tau) = \det \tau(-1)\chi(-1)^{\dim \tau}. \tag{3.6}$$

Now $\chi | \mathcal{O}_F^{\times}$ has order e, because the image of inertia in $\mathcal{W}(L/F)$ is $\Lambda \cong \mathbb{Z}/e\mathbb{Z}$. Using this fact one checks that $\chi(-1) = \epsilon$, whence (3.6) gives the stated formula.

Next suppose that $e = 3, 4,$ or 6 and $q \equiv -1 \pmod{e}$. Then there is no totally ramified abelian extension of F of degree e. Since the subfield $L^{\langle \Phi \rangle}$ of L fixed

by $\langle\Phi\rangle$ is a totally ramified extension of F of degree e it follows that $\mathcal{W}(L/F)$ is nonabelian. Hence the semidirect product in (3.4) is not direct, and consequently $\sigma_{E/F}$ is irreducibly induced from a character of the index-two abelian subgroup $\mathcal{W}(L/H)$, say $\sigma_{E/F} \cong \mathrm{ind}_{H/F}\xi$ with ξ a character of $H^\times$. Put $\sigma = \sigma_{E/F} \otimes \omega^{1/2}$. Then $\sigma \cong \mathrm{ind}_{H/F}\varphi$ with $\varphi = \xi(\omega^{1/2} \circ N_{H/F})$, and since σ is symplectic we have $\varphi|F^\times = \eta$ and $\varphi^2 \neq 1$ by part (i) of Proposition 1. Put $\hat{\varphi} = \theta\varphi$, where θ is the unramified quadratic character of $H^\times$. Then part (ii) of Proposition 1 implies that the representation $\hat{\sigma} = \mathrm{ind}_{H/F}\hat{\varphi}$ is dihedral. In fact $\hat{\sigma} = \hat{\sigma}_e$, because $\varphi|\mathcal{O}_H^\times$ (hence also $\hat{\varphi}|\mathcal{O}_H^\times$) has order e. The stated formula for $W(E/F,\tau)$ now follows from Theorem 1, because a case-by-case check shows that $\varphi(u_{H/F}) = -\epsilon$.

In principle, Theorem 2 provides a complete determination of $W(E,\tau)$ when $p \geqslant 5$. However, in certain situations there are alternative formulas for $W(E,\tau)$ which are easier to use and are also valid for $p = 2$ or 3:

PROPOSITION 8. (i) *If $p < \infty$ and E has good reduction then* $W(E/F,\tau) = \det\tau(-1)$.

(ii) *If $p < \infty$ and τ is unramified then*

$$W(E/F,\tau) = \det\tau(\varpi)^{a(E/F)}W(E/F)^{\dim\tau}.$$

(iii) *If τ is symplectic then* $W(E/F,\tau) = 1$.

Proof. (i) If E has good reduction over F then $\sigma_{E/F} \otimes \omega^{1/2} \cong \chi \oplus \chi^{-1}$ with an unramified character χ of $\mathcal{W}(\overline{F}/F)$. Hence the assertion follows from Proposition 7.

(ii) Quite generally, if σ' is a representation of $\mathcal{W}'(\overline{F}/F)$ and τ an unramified representation of $\mathrm{Gal}(\overline{F}/F)$, then

$$W(\sigma' \otimes \tau) = W(\sigma')^{\dim\tau}\det\tau(\varpi)^{a(\sigma')+n(\psi_F)\dim\sigma'}, \tag{3.7}$$

where $n(\psi_F)$ is the largest n such that ψ_F is trivial on $\varpi^{-n}\mathcal{O}_F$. Taking $\sigma' = \sigma'_{E/F}$ we obtain the stated formula, because

$$\det\tau(\varpi)^{\dim\sigma'_{E/F}} = (\pm 1)^2 = 1$$

when $\mathrm{tr}\,\tau$ is real-valued.

In the absence of a convenient reference let us indicate how (3.7) can be deduced from standard formulas in the literature. First of all, if $\sigma' = (\sigma, 0) = \sigma$ is a representation of the ordinary Weil group $\mathcal{W}(\overline{F}/F)$, then (3.7) follows from formula (3.4.6) of [18]. In the general case where $\sigma' = (\sigma, N)$ with a nilpotent endomorphism N, we have

$$W(\sigma') = W(\sigma)\Delta(\sigma') \tag{3.8}$$

with

$$\Delta(\sigma') = \frac{\delta(\sigma')}{|\delta(\sigma')|}$$

and

$$\delta(\sigma') = \det(-\sigma(\Phi)|V^I/V_N^I)$$

(notation as in [18] or [12]: Φ is an inverse Frobenius element of $\mathcal{W}(\overline{F}/F)$, V is the space of σ', V_N is the kernel of N, and V^I and V_N^I are the spaces of inertial invariants of V and V_N). It follows from the definitions that if τ is unramified then

$$\Delta(\sigma' \otimes \tau) = \det \tau(\varpi)^{b(\sigma')} \Delta(\sigma')^{\dim \tau}, \tag{3.9}$$

where

$$b(\sigma') = \dim(V^I/V_N^I).$$

On combining the special case $\sigma' = \sigma$ of (3.7) with (3.8) and (3.9) we obtain (3.7) in general, because

$$a(\sigma') = a(\sigma) + b(\sigma')$$

(cf. [18], p. 21, or [12], p. 139).

(iii) This follows from part (i) of Theorem 2 if $p = \infty$, from part (ii) of Theorem 2 if $p < \infty$ and $v(j) < 0$, and from the remark after Proposition 2 if $p < \infty$ and $v(j) \geqslant 0$ (take $\sigma = \sigma_{E/F} \otimes \omega^{1/2}$).

In the case where $p = 2$ or 3 and $v(j) \geqslant 0$ we prove only a minimal result sufficient for present applications. We begin with a lemma. Given an elliptic curve E over F and a positive integer m, let $E[m]$ denote the kernel of multiplication by m on $E(\overline{F})$.

LEMMA. *Suppose that $p = 2$ or 3 and $f(F/\mathbb{Q}_p)$ is odd. Let E be the elliptic curve*

$$\begin{cases} y^2 = x^3 + \varpi^2/4 & \text{if } p = 2 \\ y^2 = x^3 - \varpi x & \text{if } p = 3 \end{cases}$$

and put

$$e = \begin{cases} 3 & \text{if } p = 2 \\ 4 & \text{if } p = 3. \end{cases}$$

Then

$$F(E[e]) = H(\varpi^{1/e}).$$

Proof. If $p = 2$ then the duplication formula ([17], p. 59) shows that $E[3]$ consists of the origin, the two points

$$(0, \pm\varpi/2),$$

and the six points

$$(-\varpi^{2/3}, \sqrt{-3}\varpi/2)$$

with all possible choices of $\varpi^{2/3}$ and $\sqrt{-3}$. Since

$$H = F(\sqrt{-3}) = H(\zeta)$$

where ζ is a primitive cube root of unity, it follows that $F(E[3]) = H(\varpi^{1/3})$. Similarly, if $p = 3$ then $E[4]$ consists of the origin, the three points of order 2 (namely $(0, 0)$ and $(\sqrt{\varpi}, 0)$ with both choices of $\sqrt{\varpi}$), the eight points

$$(\epsilon\sqrt{\varpi}, \epsilon\sqrt{2}\varpi^{3/4})$$

with $\epsilon = 1 \pm \sqrt{2}$, a fixed choice of $\sqrt{2}$, all four choices of $\varpi^{1/4}$, and $\sqrt{\varpi} = (\varpi^{1/4})^2$, and the four points

$$(\sqrt{-\varpi}, \sqrt{2}(-\varpi)^{3/4})$$

with a fixed choice of $\sqrt{2}$, all four choices of $(-\varpi)^{1/4}$, and $\sqrt{-\varpi} = (-\varpi^{1/4})^2$. In this case

$$H = F(\sqrt{2}) = F(\sqrt{-1}) = F(\zeta)$$

where ζ is a primitive eighth root of unity. Therefore $F(E[4]) = H(\varpi^{1/4})$.

Given $A, B \in F$ with $4A^3 + 27B^2 \neq 0$, let $E_{A,B}$ denote the elliptic curve

$$y^2 = x^3 + Ax + B$$

and

$$j_{A,B} = \frac{(-48A)^3}{-16(4A^3 + 27B^2)}$$

its modular invariant.

PROPOSITION 9. *Suppose that* $p = 2$ or 3 *and* $f(F/\mathbb{Q}_p)$ *is odd. There is a nonempty open subset* $\mathcal{U}$ *of* $F \times F$ *such that if* $(A, B) \in \mathcal{U}$, *then* $4A^3 + 27B^2 \neq 0$, $v(j_{A,B}) \geqslant 0$, *and*

$$W(E_{A,B}/F, \tau) = \det \tau(-1)\delta^{\dim \tau}(-1)^{\langle 1,\tau\rangle + \langle \eta,\tau\rangle + \langle \hat{\sigma},\tau\rangle},$$

where δ *is* 1 *or* -1 *according as* p *is* 2 *or* 3, *and*

$$\hat{\sigma} = \begin{cases} \hat{\sigma}_3 & \text{if } p = 2 \\ \hat{\sigma}_4 & \text{if } p = 3. \end{cases}$$

Proof. Let e be as in the lemma and let $\mathcal{U}$ be the set of all pairs $(A, B) \in F \times F$ such that $4A^3 + 27B^2 \neq 0$, $v(j_{A,B}) \geqslant 0$, and $F(E_{A,B}[e]) = H(\varpi^{1/e})$. Then $\mathcal{U}$ is nonempty by the preceding lemma and open by Krasner's Lemma, which implies that the function $(A, B) \mapsto F(E_{A,B}[e])$ is locally constant (cf. the appendix to [8]). We claim that if $(A, B) \in \mathcal{U}$ then $W(E_{A,B}/F, \tau)$ is as stated. Put $\sigma = \mathrm{ind}_{H/F}\varphi$, where φ is either of the two tamely ramified characters of $H^\times$ such that $\varphi|F^\times = \chi_{H/F}$ and $\varphi|\mathcal{O}_H^\times$ has order e. Also write $E = E_{A,B}$ and $j = j_{A,B}$. It suffices to show that $\sigma_{E/F} \otimes \omega^{1/2} = \sigma$, for our claim then follows from Theorem 1 (one must also check that $\hat{\varphi}(u_{H/F}) = \varphi(u_{H/F}) = \delta$). Now the assumption $v(j) \geqslant 0$ implies that E has good reduction over the field $L = F^{\mathrm{unr}}(E[e])$ and that L is the minimal extension of F^{unr} with this property ([16], p. 498, Cor. 3). Since $F(E[e]) = H(\varpi^{1/e})$ we have

$$L = F^{\mathrm{unr}}(\varpi^{1/e}).$$

Thus if Λ is the image of inertia in $\mathcal{W}(L/F)$ and $\Phi \in \mathcal{W}(L/F)$ is an inverse Frobenius element then equations (3.4) and (3.5) in the proof of part (iii) of Theorem 2 continue to hold in the case at hand. Furthermore, the semidirect product in (3.5) is not direct, because $H(\varpi^{1/e})/F$ is nonabelian (F does not contain a primitive eth root of unity). Hence arguing as before we find that $\sigma_{E/F} \otimes \omega^{1/2} \cong \mathrm{ind}_{H/F}\varphi'$ with a character φ' of $H^\times$ such that $\varphi'|\mathcal{O}_H^\times$ has order e. Since $\sigma_{E/F} \otimes \omega^{1/2}$ is symplectic it follows from Proposition 1 that $\varphi'|F^\times = \eta$, whence $\varphi' = \varphi^{\pm 1}$. Therefore $\sigma_{E/F} \otimes \omega^{1/2} \cong \sigma$, proving our claim.

4. The global root number

Now we switch to a global setting. Henceforth F denotes a number field and F_v its completion at a place v. Extending v to a place of $\overline{F}$, we may identify the decomposition group of v in $\mathrm{Gal}(\overline{F}/F)$ with $\mathrm{Gal}(\overline{F}_v/F_v)$, and if τ is a representation of $\mathrm{Gal}(\overline{F}/F)$ then the restriction of τ to $\mathrm{Gal}(\overline{F}_v/F_v)$ will be denoted τ_v. Thus given τ and v, and given an arbitrary irreducible representation ρ of $\mathrm{Gal}(\overline{F}_v/F_v)$, we can

speak of the multiplicity $\langle \rho, \tau_v \rangle$ of ρ in τ_v. We shall be interested in $\langle \rho, \tau_v \rangle$ for ρ belonging to a certain finite set $\mathcal{R}_v$ defined as follows. If v is an infinite place of F then $\mathcal{R}_v$ consists of all irreducible representations of $\mathrm{Gal}(\overline{F}_v/F_v)$, i.e. the trivial character if $F_v \cong \mathbb{C}$ and the trivial and sign characters if $F_v = \mathbb{R}$. If v is a finite place of F, then $\mathcal{R}_v$ consists of the trivial character, all quadratic characters, and the dihedral representations $\hat{\sigma}_e$, where $e = 3, 4$, or 6 and $q_v \equiv -1 \pmod{e}$. Here q_v is the order of the residue class field of F_v, and we recall that

$$\hat{\sigma}_e = \mathrm{ind}_{H/F_v} \hat{\varphi}_e,$$

where H is the unramified quadratic extension of F_v and $\hat{\varphi}_e$ is either of the tamely ramified characters of $H^\times$ of order e such that $\hat{\varphi}_e | F_v^\times = 1$. We note that for all v the elements of $\mathcal{R}_v$ are realizable over $\mathbb{Q}$.

Given an elliptic curve E over F, we define its root number $W(E)$ by the formula

$$W(E) = \prod_v W(E/F_v),$$

where v runs over all places of F. More generally, if τ is a representation of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character, then we put

$$W(E, \tau) = \prod_v W(E/F_v, \tau_v).$$

THEOREM 3. *Let τ be a representation of* $\mathrm{Gal}(\overline{F}/F)$ *with real-valued character.*

(i) *Suppose that for some place v_0 of F and some $\rho \in \mathcal{R}_{v_0}$ the multiplicity $\langle \rho, \tau_{v_0} \rangle$ is odd. Then there is an elliptic curve E over F such that $W(E, \tau) = -1$.*

(ii) *Conversely, suppose that for each place v of F at least one of the following conditions is satisfied:*
   (a) *$\langle \rho, \tau_v \rangle$ is even for every $\rho \in \mathcal{R}_v$, and v does not divide* 2 *or* 3.
   (b) *τ_v is symplectic.*

Then $W(E, \tau) = 1$ for every elliptic curve E over F.

We have formulated the theorem in such a way that it includes the case where τ has odd dimension or nontrivial determinant as well as the case where τ has even dimension and trivial determinant. However, these two cases are fundamentally different and the proof of the theorem will be divided accordingly.

The case of odd dimension or nontrivial determinant

To begin with τ denotes an arbitrary representation of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character. We identify $\det \tau$ with an idele class character of F by the global analogue

of (1.1). Since $\det\tau$ has finite order – in fact order dividing 2 – we can also think of $\det\tau$ as a primitive ray class character and evaluate it on nonzero integral ideals of F relatively prime to $\mathfrak{N}(\det\tau)$, where $\mathfrak{N}(*)$ denotes the conductor of $*$. In particular, if E is an elliptic curve over F such that $\mathfrak{N}(E)$ and $\mathfrak{N}(\tau)$ are relatively prime, then $\det\tau(\mathfrak{N}(E))$ is defined, and

$$\det\tau(\mathfrak{N}(E)) = \prod_{v \text{ finite}} \det\tau_v(\varpi_v)^{a(E/F_v)}$$

(ϖ_v denotes a uniformizer of F_v). Put

$$\operatorname{sign}(\det\tau) = \prod_{v|\infty} \det\tau_v(-1).$$

PROPOSITION 10. *If $\mathfrak{N}(E)$ and $\mathfrak{N}(\tau)$ are relatively prime, then*

$$W(E,\tau) = \operatorname{sign}(\det\tau)\det\tau(\mathfrak{N}(E))W(E)^{\dim\tau}.$$

Proof. This is a special case of a well-known formula, but we recall the proof. Our hypothesis means that if v is a finite place of F then E has good reduction over F_v or τ_v is unramified. We claim that

$$W(E/F_v,\tau_v) = \det\tau_v(-1)\det\tau_v(\varpi_v)^{a(E/F_v)}W(E/F_v)^{\dim\tau}$$

in either case. Indeed if E/F_v has good reduction then $W(E/F_v,\tau_v) = \det\tau_v(-1)$ by part (i) of Proposition 8, while $a(E/F_v) = 0$ and $W(E/F_v) = 1$ (for the latter point, apply part (i) of Proposition 8 again with τ equal to the trivial representation). On the other hand, if τ_v is unramified then $\det\tau_v(-1) = 1$ and $W(E/F_v,\tau_v) = \det\tau_v(\varpi_v)^{a(E/F_v)}W(E/F_v)^{\dim\tau}$ by part (ii) of Proposition 8. Therefore

$$\begin{aligned} W(E,\tau) &= \prod_v W(E/F_v,\tau_v) \\ &= \left(\prod_{v \text{ finite}} \det\tau_v(-1)\det\tau_v(\varpi_v)^{a(E/F_v)}W(E/F_v)^{\dim\tau}\right) \\ &\quad \cdot \left(\prod_{v|\infty}(-1)^{\dim\tau}\right) \end{aligned}$$

using part (i) of Theorem 2. The result follows on noting that

$$\prod_{v \text{ finite}} W(E/F_v)^{\dim\tau} \prod_{v|\infty}(-1)^{\dim\tau} = \left(\prod_v W(E/F_v)\right)^{\dim\tau} = W(E)^{\dim\tau}$$

and that

$$\prod_{v \text{ finite}} \det \tau_v(-1) = \operatorname{sign}(\det \tau)$$

(the idele class character $\det \tau$ is trivial on the principal idele -1).

If χ is a quadratic idele class character of F we let E^χ denote the twist of E by χ. The following corollary is also well known:

COROLLARY. *If χ is a quadratic idele class character of F of conductor relatively prime to $\mathfrak{N}(E)$, then*

$$W(E^\chi) = \operatorname{sign}(\chi)\chi(\mathfrak{N}(E))W(E).$$

Proof. Observe that $W(E^\chi) = W(E, \chi)$ and apply Proposition 10.

We shall prove Theorem 3 for representations of odd dimension or nontrivial determinant by showing that the conclusion of part (i) of the theorem always holds and the hypothesis of part (ii) never holds. The former objective is accomplished by the following result, which contains Proposition A of the introduction.

PROPOSITION 11. *If τ has odd dimension or nontrivial determinant then there exists an elliptic curve E over F with $\mathfrak{N}(E)$ relatively prime to $\mathfrak{N}(\tau)$ such that $W(E, \tau) = -1$.*

Proof. Suppose first that $\dim \tau$ is odd. Choose an elliptic curve E over F such that $\mathfrak{N}(E)$ is relatively prime to $\mathfrak{N}(\tau)$ and E has multiplicative reduction at some prime. (This amounts to choosing a generalized Weierstrass equation over $\mathcal{O}_\mathcal{F}$ which satisfies appropriate congruences at finitely many primes.) Since E has multiplicative reduction at some place, $\mathfrak{N}(E)$ is not the square of an ideal of F, whence there exists a quadratic idele class character χ of F which is unramified at infinity and of conductor relatively prime to $\mathfrak{N}(E)\mathfrak{N}(\tau)$ and for which $\chi(\mathfrak{N}(E)) = -1$. The corollary implies that either $W(E)$ or $W(E^\chi)$ is -1. Since $\mathfrak{N}(E)$ and $\mathfrak{N}(E^\chi)$ differ by the square of an ideal (in fact $\mathfrak{N}(E^\chi) = \mathfrak{N}(E)\mathfrak{N}(\chi)^2$), Proposition 10 implies that either $W(E, \tau)$ or $W(E^\chi, \tau)$ is -1.

Henceforth we assume that $\dim \tau$ is even. Then $\det \tau$ is nontrivial. Suppose in addition that

$$\operatorname{sign}(\det \tau) = -1,$$

and choose an elliptic curve E over F such that $\mathfrak{N}(E)$ is relatively prime to $6\mathfrak{N}(\tau)$ and E has additive reduction at all places of bad reduction. (Take any E such that $\mathfrak{N}(E)$ is relatively prime to $6\mathfrak{N}(\tau)$ and then replace E by E^χ, where

χ is a quadratic idele class character which is ramified at the prime ideals where E has multiplicative reduction and unramified at all other prime ideals dividing $6\mathfrak{N}(\tau)\mathfrak{N}(E)$.) Then $\mathfrak{N}(E)$ is the square of an ideal, whence $W(E,\tau) = -1$ by Proposition 10.

Finally, suppose that $\det\tau$ is nontrivial but that

$$\operatorname{sign}(\det\tau) = 1.$$

Choose a prime ideal $\mathfrak{p}$ not dividing $6\mathfrak{N}(\tau)$ such that $\det\tau(\mathfrak{p}) = -1$, and then choose an elliptic curve E such that $\mathfrak{N}(E)$ is relatively prime to $6\mathfrak{N}(\tau)$ and has multiplicative reduction at $\mathfrak{p}$. After replacing E by a quadratic twist we may assume that $\mathfrak{p}$ is the only place where E has multiplicative reduction. Then $\mathfrak{N}(E)$ equals $\mathfrak{p}$ times the square of an ideal, whence $W(E,\tau) = -1$ by Proposition 10.

To complete the proof of Theorem 3 in the case at hand it suffices to show that if τ has odd dimension or nontrivial determinant then there is a place v of F for which neither condition (a) nor condition (b) of part (ii) of the theorem is satisfied. This is a consequence of the following lemma, for if K is a finite Galois extension of F such that τ factors through $\mathrm{Gal}(K/F)$, then every cyclic subgroup of $\mathrm{Gal}(K/F)$ is a decomposition group at infinitely many primes (Chebotarev).

If τ is a representation of a group G and D is a subgroup of G then τ_D denotes the restriction of τ to D.

LEMMA. *Let G be a finite group and τ a representation of G with real-valued character. If τ has odd dimension or nontrivial determinant then there is a cyclic subgroup D of G and a character χ of D with $\chi^2 = 1$ such that the following assertions hold:*

(a) *$\langle\chi, \tau_D\rangle$ is odd.*
(b) *τ_D is not symplectic.*

Proof. If $\dim\tau$ is odd take D to be the trivial group and χ the trivial character. Otherwise choose an element $g \in G$ such that $\det\tau(g) = -1$, and let D be the cyclic subgroup of even order generated by g. Then τ_D is a direct sum of characters of D, and since each character of order $\geqslant 3$ appears with the same multiplicty as its complex conjugate, we have

$$\det\tau_D = \chi^{\langle\chi,\tau_D\rangle},$$

where χ is the unique quadratic character of D. Since $\det\tau_D$ is nontrivial we conclude that $\langle\chi,\tau_D\rangle$ is odd, and this conclusion implies in turn that τ_D is not symplectic.

The case of even dimension and trivial determinant

In contrast to the case just treated, now it is only the primes dividing both $\mathfrak{N}(E)$ and $\mathfrak{N}(\tau)$ which contribute to $W(E,\tau)$:

PROPOSITION 12. *Suppose that τ has even dimension and trivial determinant, and let E be an elliptic curve over F and v a place of F. If $W(E/F_v,\tau_v) = -1$ then v divides both $\mathfrak{N}(E)$ and $\mathfrak{N}(\tau)$.*

Proof. If v is an infinite place of F then $W(E/F_v) = 1$ by part (i) of Theorem 2. If v is a finite place of F where E has good reduction or τ is unramified, then $W(E/F_v,\tau_v) = 1$ by parts (i) and (ii) of Proposition 8.

Now fix a representation τ of $\mathrm{Gal}(\overline{F}/F)$ of even dimension and trivial determinant and suppose that v_0 is a place of F such that $\langle\rho,\tau_{v_0}\rangle$ is odd for some $\rho \in \mathcal{R}_{v_0}$. Then v_0 is finite: for if $F_{v_0} \cong \mathbb{C}$ then $\mathcal{R}_{v_0} = \{1\}$ and

$$\langle 1,\tau_{v_0}\rangle = \dim\tau,$$

while if $F_{v_0} = \mathbb{R}$ then $\mathcal{R}_{v_0} = \{1,\mathrm{sgn}\}$ and

$$(-1)^{\langle \mathrm{sgn},\tau_{v_0}\rangle} = \det\tau_{v_0}(-1),$$

$$\langle 1,\tau_{v_0}\rangle = \dim\tau_{v_0} - \langle \mathrm{sgn},\tau_{v_0}\rangle.$$

We will produce an elliptic curve E over F with good reduction at all prime divisors of $\mathfrak{N}(\tau)$ other than v_0 such that $W(E/F_{v_0},\tau_{v_0}) = -1$. Then $W(E,\tau) = W(E/F_{v_0},\tau_{v_0}) = -1$ by Proposition 12, proving part (i) of Theorem 3.

The choice of E proceeds by a consideration of cases. Suppose first that $\langle\chi,\tau_{v_0}\rangle$ is odd for some character χ of $F_{v_0}^\times$ such that $\chi^2 = 1$. Let E be an elliptic curve over F with potential multiplicative reduction at v_0 and good reduction at all prime divisors of $\mathfrak{N}(\tau)$ different from v_0. Also let ξ be the character of $F_{v_0}^\times$ corresponding to the extension $F_{v_0}(\sqrt{-c_6})/F_{v_0}$, where c_6 is the weight-six covariant of some generalized Weierstrass equation for E over F. After twisting E by a quadratic idele class character of F with v_0-component $\chi\xi^{-1}$, we may assume that $\xi = \chi$. Then $W(E,\tau) = W(E/F_{v_0},\tau_{v_0}) = -1$ by part (ii) of Theorem 2.

Next suppose that $\langle\chi,\tau_{v_0}\rangle$ is even for all characters χ of $F_{v_0}^\times$ such that $\chi^2 = 1$. Then there exists $\hat{\sigma} = \hat{\sigma}_e \in \mathcal{R}_{v_0}$ (with $e = 3, 4$, or 6) such that $\langle\hat{\sigma},\tau_{v_0}\rangle$ is odd. Assume first that v_0 does not divide 2 or 3, and let E be an elliptic curve over F such that $v_0(j) \geqslant 0$ and $v_0(\Delta) = 12/e$ (notation as in Theorem 2). For example, take E to be the curve $y^2 = x^3 + Ax + B$, where $v_0(A) = 1$ and $v_0(B) = 2$ if $e = 4$ and $v_0(A) = 2$ and $v_0(B) = 6/e$ if $e = 3$ or 6. Imposing appropriate congruences at finitely many other places, we may assume that E has good reduction at all prime divisors of $\mathfrak{N}(\tau)$ other than v_0. Then $W(E,\tau) = W(E/F_{v_0},\tau_{v_0}) = -1$ by part (iii) of Theorem 2. If v_0 divides 2 or 3 then we repeat the argument just given but we appeal to Proposition 9 rather than to part (iii) of Theorem 2.

This completes the proof of part (i) of Theorem 3 for representations of even dimension and trivial determinant. As for part (ii) of Theorem 3, observe that if condition (a) holds for a given place v then $W(E/F_v, \tau_v) = 1$ by Theorem 2, while if condition (b) holds then $W(E/F_v, \tau_v) = 1$ by part (iii) of Proposition 8. Hence under the hypothesis of part (ii) of Theorem 3 we have $W(E/F_v, \tau_v) = 1$ for every v, and therefore $W(E, \tau) = 1$.

5. Examples

We say that a finite group D is a Galois group over $\mathbb{Q}_p$ if D is isomorphic to $\mathrm{Gal}(K/\mathbb{Q}_p)$ for some Galois extension K of $\mathbb{Q}_p$, or equivalently, if there is a surjective homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to D$. Here 'homomorphism' means 'continuous homomorphism', where D is given the discrete topology.

Proof of Proposition B

Proposition B of the introduction is a consequence of Theorem 3 and the following proposition. Recall that if τ is a representation of a group G and D a subgroup of G then τ_D denotes the restriction of τ to D.

PROPOSITION 13. *Let τ be the 4-dimensional irreducible representation of A_5 and D a subgroup of A_5.*

(i) *If D is isomorphic to A_4, S_3, or $(\mathbb{Z}/2\mathbb{Z})^2$, then $\langle 1, \tau_D \rangle = 1$.*

(ii) *Suppose that D is a Galois group over $\mathbb{Q}_p$ for some $p \leqslant \infty$ but is not isomorphic to one of the groups mentioned in (i). Then D is either cyclic or isomorphic to D_5. Furthermore:*

(a) *If $D \cong D_5$ then τ_D is the direct sum of the two faithful irreducible representations of D, and $p \geqslant 5$.*

(b) *If D is cyclic then τ_D is symplectic.*

Proof. (i) The following three assertions comprise a more precise version of the statement to be proved:

(1) If $D \cong A_4$ then $\tau_D \cong 1 \oplus \pi$, where π is the 3-dimensional irreducible representation of D.

(2) If $D \cong S_3$ then $\tau_D \cong 1 \oplus \epsilon \oplus \sigma$ where σ is the 2-dimensional irreducible representation and ϵ the quadratic character of D.

(3) If $D \cong (\mathbb{Z}/2\mathbb{Z})^2$ then $\tau_D \cong 1 \oplus \delta_1 \oplus \delta_2 \oplus \delta_3$, where the δ_i are the three quadratic characters of D.

Assertion (1) is a consequence of the fact that τ_D is faithful and $\det \tau_D$ real-valued. Then (3) follows because every subgroup of A_5 which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ is contained in a subgroup isomorphic to A_4. As for (2), if $D \cong S_3$ then the fact that τ_D is faithful and $\det \tau_D$ trivial implies that $\tau_D \cong \sigma \oplus \epsilon \oplus 1$ or $\tau_D \cong \sigma \oplus \sigma$. To exclude the latter possibility, observe that the restriction of τ_D to the subgroup of order 3 in D contains the trivial representation (this follows from (1)).

(ii) Since A_5 is not solvable it is not itself a Galois group over $\mathbb{Q}_p$. Furthermore, any maximal proper subgroup of A_5 is isomorphic to A_4, D_5, or S_3. Hence if D is not isomorphic to one of the groups mentioned in (i) then D is either cyclic or isomorphic to D_5.

(a) If $D \cong D_5$ then τ_D is the direct sum of the two 2-dimensional irreducible representations of D: indeed at least one occurs because τ_D is faithful, and then both occur because $\operatorname{tr} \tau$ is rational-valued.

Since 5 does not divide $2^2 - 1$ or $3^2 - 1$, no quadratic extension of $\mathbb{Q}_2$ or $\mathbb{Q}_3$ has a ramified cyclic extension of degree 5. It follows that D_5 is not a Galois group over $\mathbb{Q}_2$ or $\mathbb{Q}_3$.

(b) If D is cyclic then τ_D is symplectic by the following lemma.

LEMMA . *Let D be a finite group and τ a representation of D with real-valued character, even dimension, and trivial determinant. If D is cyclic or of odd order then τ is symplectic.*

Proof. Suppose first that D has odd order. If π is a nontrivial irreducible representation of D then $\pi \ncong \pi^*$, but π and π^* have the same multiplicity in τ because $\operatorname{tr} \tau$ is real-valued. Hence τ is a direct sum of representations of the form $\pi \oplus \pi^*$ plus some number of copies of the trivial representation. Since $\dim \tau$ is even the multiplicity of the trivial representation is also even, whence τ is symplectic. A similar argument applies if D is cyclic of even order: τ is a direct sum of representations of the form $\chi \oplus \overline{\chi}$, where χ is a character of order $\geqslant 3$, plus some number of copies of the trivial character and of the unique quadratic character ϵ. Since $\det \tau$ is trivial the multiplicity of ϵ is even, and then the multiplicity of the trivial character is also even because $\dim \tau$ is even.

Buhler's field of conductor 800

Let K be the splitting field over $\mathbb{Q}$ of the polynomial $x^5 + 10x^3 - 10x^2 + 35x - 18$. Then $\operatorname{Gal}(K/\mathbb{Q}) \cong A_5$, and the ramified primes are 2 and 5 with decomposition groups isomorphic to A_4 and $\mathbb{Z}/5\mathbb{Z}$ respectively ([1], p. 47). Let τ be the 4-dimensional irreducible representation of $\operatorname{Gal}(K/\mathbb{Q})$ and E any elliptic curve over $\mathbb{Q}$ with split multiplicative reduction at 2. By Proposition 12,

$$W(E, \tau) = W(E/\mathbb{Q}_2, \tau_2) W(E/\mathbb{Q}_5, \tau_5).$$

On the other hand, part (i) of Proposition 13 and part (ii) of Theorem 2 imply that $W(E/\mathbb{Q}_2, \tau_2) = -1$, while part (ii)(b) of Proposition 13 and part (iii) of Proposition 8 imply that $W(E/\mathbb{Q}_5, \tau_5) = 1$. Therefore $W(E, \tau) = -1$.

Proof of Proposition C

Proposition C follows from Theorem 3 and the next result.

PROPOSITION 14. (1) *Let $\tau = \tau^{(6)}$ be the 6-dimensional irreducible representation of* $\mathrm{PSL}(2, \mathbb{F}_7)$ *and D a subgroup of* $\mathrm{PSL}(2, \mathbb{F}_7)$.

(i) *If D is isomorphic to S_4 or A_4 then $\langle 1, \tau_D\rangle = 1$; if D is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ then $\langle 1, \tau_D\rangle = 3$; and if D is isomorphic to D_4 then there is a quadratic character χ of D such that $\langle \chi, \tau_D\rangle = 1$.*

(ii) *If D is a Galois group over $\mathbb{Q}_p$ for some $p \leqslant \infty$ but is not isomorphic to one of the groups mentioned in (i) then τ_D is symplectic.*

(2) *Let $\tau = \tau^{(8)}$ be the 8-dimensional irreducible representation of* $\mathrm{PSL}(2, \mathbb{F}_7)$ *and D a subgroup of* $\mathrm{PSL}(2, \mathbb{F}_7)$.

(i) *If D is isomorphic to D_4 or S_3 then $\langle 1, \tau_D\rangle = 1$. If D is isomorphic to S_4 and ρ is the 2-dimensional irreducible representation of D then $\langle \rho, \tau_D\rangle = 1$, and if $\iota : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to D$ is any surjective homomorphism then $p = 2$ and $\rho \circ \iota$ coincides with the representation $\hat{\sigma}_3$ of* $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$.

(ii) *If D is a Galois group over $\mathbb{Q}_p$ for some $p \leqslant \infty$ but is not isomorphic to one of the groups mentioned in (i), then τ_D is symplectic.*

Proof. (1) Before embarking on the verification of statements (i) and (ii) it is helpful to note the following facts:

(A) If C is a subgroup of $\mathrm{PSL}(2, \mathbb{F}_7)$ of order 2 then the trivial character of C occurs in τ_C with multiplicity 4 and the nontrivial character with multiplicity 2.

(B) If C is a subgroup of $\mathrm{PSL}(2, \mathbb{F}_7)$ of order 3 then all three characters of C occur in τ_C with multiplicity 2.

(C) Let $P \cong D_4$ be a 2-Sylow subgroup of S_4 and κ the 2-dimensional irreducible representation of P. Let ϵ be the quadratic character of S_4. Then $\epsilon_P \neq \det \kappa$.

The first two assertions can be read from a character table (see e.g. [9], p. 263). For the third, observe that ϵ is the sign character, hence nontrivial on 4-cycles.

(i) The statement to be proved is contained in the following more detailed assertions:

(1) If $D \cong S_4$ then $\tau_D \cong 1 \oplus \rho \oplus \tilde{\pi}$, where ρ is the 2-dimensional irreducible representation of D and $\tilde{\pi}$ the 3-dimensional irreducible representation with nontrivial determinant.

(2) If $D \cong A_4$ then $\tau_D \cong 1 \oplus \xi \oplus \overline{\xi} \oplus \pi$, where ξ is either of the cubic characters of D and π the 3-dimensional irreducible representation of D.

(3) If $D \cong (\mathbb{Z}/2\mathbb{Z})^2$ then $\tau_D \cong 1 \oplus 1 \oplus 1 \oplus \delta_1 \oplus \delta_2 \oplus \delta_3$, where the δ_i are the distinct quadratic characters of D.

(4) If $D \cong D_4$ then $\tau_D \cong 1 \oplus 1 \oplus \chi_1 \oplus \chi_2 \oplus \kappa$, where κ is the 2-dimensional irreducible representation of D and χ_1 and χ_2 are the two quadratic characters of D distinct from $\det \kappa$.

First suppose that $D \cong (\mathbb{Z}/2\mathbb{Z})^2$. Then τ_D coincides with $1 \oplus 1 \oplus 1 \oplus \delta_1 \oplus \delta_2 \oplus \delta_3$ on each two-element subgroup of D, by (A). Since D is the union of its two-element subgroups, (3) follows. Next suppose that $D \cong A_4$. Since τ_D is faithful, π occurs in τ_D, whence either $\tau_D \cong \pi \oplus \xi \oplus \overline{\xi} \oplus 1$ or $\tau_D \cong \pi \oplus 1 \oplus 1 \oplus 1$ or $\tau_D \cong \pi \oplus \pi$. The second and third possibilities are inconsistent with (B) and (3) respectively, and we obtain (2). Turning to (1), suppose that $D \cong S_4$, and let $\epsilon = \det \tilde{\pi} = \det \rho$

be the quadratic character of D. Using the fact that $\det \tau_D$ is trivial, we deduce from (2) that $\tau_D \cong \tilde{\pi} \oplus \rho \oplus 1$ or $\tau_D \cong (\tilde{\pi} \otimes \epsilon) \oplus \rho \oplus \epsilon$. To exclude the latter possibility, choose an involution $g \in D$ such that $\epsilon(g) = -1$, and observe that $\tilde{\pi}(g)$ and $\rho(g)$ have eigenvalues $1, 1, -1$ and $1, -1$ respectively. We see that the hypothesis $\tau_D \cong (\tilde{\pi} \otimes \epsilon) \oplus \rho \oplus \epsilon$ is inconsistent with (A), and (1) follows. Finally, if $D \cong D_4$ then D is contained in a subgroup D' of $\mathrm{PSL}(2, \mathbb{F}_7)$ isomorphic to S_4, and if ρ is the 2-dimensional irreducible representation of D' then ρ_D is the direct sum of the trivial and a nontrivial character of D. Also κ occurs in τ_D because τ_D is faithful. Hence (4) follows by a straightforward argument from (1) and (C).

(ii) If D is a solvable subgroup of $\mathrm{PSL}(2, \mathbb{F}_7)$ and is not isomorphic to one of the groups mentioned in (i) then D is either cyclic, or isomorphic to $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$, or isomorphic to S_3. In the first two cases τ_D is symplectic by the previous lemma. If $D \cong S_3$ then we deduce from (B) and the triviality of $\det \tau_D$ that $\tau_D \cong \lambda \oplus \lambda \oplus \delta \oplus \delta$, where λ is the two-dimensional irreducible representation of D and δ a character of D with $\delta^2 = 1$ (actually $\delta = 1$ by (A)). Therefore τ_D is symplectic in this case as well.

(2) Again it is helpful to make some preliminary observations:

(A) Let θ be either of the 3-dimensional irreducible representations of $\mathrm{PSL}(2, \mathbb{F}_7)$. Then $\theta \otimes \theta^* \cong 1 \oplus \tau$.

(B) Let π be the 3-dimensional irreducible representation of A_4. Then $\pi \otimes \pi \cong \pi \oplus \pi \oplus \xi \oplus \overline{\xi} \oplus 1$, where ξ is either of the cubic characters of A_4.

(C) Let $\check{\pi}$ and $\tilde{\pi}$ be the 3-dimensional irreducible representations of S_4 with trivial and nontrivial determinants respectively. Then $\check{\pi} \otimes \check{\pi} \cong \check{\pi} \oplus \tilde{\pi} \oplus \rho \oplus 1$, where ρ is the 2-dimensional irreducible representation of S_4.

To verify (A) note that $\langle 1, \theta \otimes \theta^* \rangle = 1$ by Schur's Lemma. Since the dimensions of the nontrivial irreducible representations of $\mathrm{PSL}(2, \mathbb{F}_7)$ different from τ are 3, 6, and 7, a comparison of dimensions gives $\theta \otimes \theta^* \cong 1 \oplus \tau$. A similar argument applies to (B): we have $\langle 1, \pi \otimes \pi \rangle = \langle 1, \pi \otimes \pi^* \rangle = 1$ by Schur's Lemma, whence $\pi \otimes \pi \cong 1 \oplus (*) \oplus (**)$ with $(*)$ equal to a direct sum of copies of π and $(**)$ equal to a direct sum of copies of $\xi \oplus \overline{\xi}$. Since $\pi \otimes \pi$ has odd dimension, we see that $(*)$ is actually a direct sum of copies of $\pi \oplus \pi$: furthermore, $(*)$ is not the empty direct sum because a tensor product of faithful representations of a group with trivial center is faithful. Comparing dimensions, we conclude that $(*) = \pi \oplus \pi$, and (B) follows. Finally, (C) follows from (B) and Schur's Lemma.

(i) If D is isomorphic to S_3 or D_4 then $\theta_D \cong \mu \oplus \det \mu$, where μ is the 2-dimensional irreducible representation of D. In particular, θ_D is the direct sum of two inequivalent irreducible representations. Therefore $\langle 1, (\theta \otimes \theta^*)_D \rangle = 2$ by Schur's Lemma, whence (A) gives $\langle 1, \tau_D \rangle = \langle 1, (\theta \otimes \theta^*)_D \rangle - \langle 1, 1 \rangle = 1$. Next suppose that $D \cong S_4$. Then θ_D coincides with the 3-dimensional irreducible representation of D with trivial determinant. Hence $\langle \rho, \tau_D \rangle = 1$ by (A) and (C). Furthermore, if $P \triangleleft I \triangleleft D$ is a tower of normal subgroups such that D/I and I/P are cyclic and P is a p-group then I is isomorphic to A_4 and P is the 2-Sylow

subgroup of I. Hence if $\iota : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to D$ is a surjective homomorphism then $p = 2$ and $\rho \circ \iota = \hat{\sigma}_3$.

(ii) If D is cyclic or of odd order then τ_D is symplectic by the lemma. If $D \cong A_4$ then θ_D is the 3-dimensional irreducible representation of D, whence τ_D is symplectic by (A) and (B). Finally, if $D \cong (\mathbb{Z}/2\mathbb{Z})^2$ then θ_D is the direct sum of the three nontrivial characters of D, so that the trivial character of D has multiplicity 3 in $(\theta \otimes \theta^*)_D$ and each nontrivial character multiplicity 2. Hence τ_D is symplectic by (A).

The example of Trinks

Let us return to the example of Trinks mentioned in the introduction: $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}(2, \mathbb{F}_7)$ with K equal to the splitting field of $x^7 - 7x + 3$. We claim that of the groups S_4, A_4, D_4, $(\mathbb{Z}/2\mathbb{Z})^2$, and S_3, only S_3 occurs as a decomposition subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. Hence Proposition C implies that there is an elliptic curve E over $\mathbb{Q}$ for which $W(E, \tau^{(8)}) = -1$ but none for which $W(E, \tau^{(6)}) = -1$.

Since $x^7 - 7x + 3$ has discriminant $3^8 7^8$, the decomposition subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ at a prime $p \neq 3, 7$ are cyclic. Furthermore, since $(x+4)^7 - 7(x+4) + 3$ is an Eisenstein polynomial at 7, the decomposition subgroups at 7 have order divisible by 7. Hence to verify our claim it suffices to see that the decomposition subgroups at 3 are isomorphic to S_3. Now the factorization

$$x^7 - 7x + 3 \equiv (x + 6)(x^3 - 3x^2 - 4)(x^3 - 3x^2 + 4) \pmod 9$$

over $\mathbb{Z}/9\mathbb{Z}$ lifts to a factorization over $\mathbb{Z}_3$, because for $A = \mathbb{Z}_3[x]$ we have

$$(x + 6)A + (x^3 - 3x^2 - 4)(x^3 - 3x^2 + 4)A = A$$

and

$$(x^3 - 3x^2 - 4)A + (x^3 - 3x^2 + 4)A = A.$$

Furthermore, if $f(x)$ is a lift of $x^3 - 3x^2 - 4$ then $f(x + 1)$ is an Eisenstein polynomial and

$$\mathrm{disc}(f) \equiv 3^3 \pmod{3^4},$$

whence the splitting field of f over $\mathbb{Q}_3$ is a totally ramified extension of $\mathbb{Q}_3$ with Galois group S_3. Thus if D is a decomposition subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ at 3 then D is isomorphic to a subgroup of $\mathrm{PSL}(2, \mathbb{F}_7)$ having S_3 as quotient group. Any such group is isomorphic to S_4 or to S_3 itself. Since S_4 is not a Galois group over $\mathbb{Q}_3$, we conclude that D is isomorphic to S_3, as claimed.

Suppose now that E is any elliptic curve over $\mathbb{Q}$ with split multiplicative reduction at 3. Then $W(E/\mathbb{Q}_3, \tau_3^{(8)}) = -1$ by part 2(i) of Proposition 14 and

part (ii) of Theorem 2, while $W(E/\mathbb{Q}_7, \tau_7^{(8)}) = 1$ by part 2(ii) of Proposition 14 and part (iii) of Proposition 8. Hence Proposition 12 gives

$$W(E, \tau^{(8)}) = W(E/\mathbb{Q}_3, \tau_3^{(8)}) W(E/\mathbb{Q}_7, \tau_7^{(8)}) = -1.$$

Proof of Proposition D

Finally, Theorem 3 applied to the following result yields Proposition D:

PROPOSITION 15. *Let $G = D_q \times D_r \times D_s \times D_t$ with distinct primes $q, r, s, t \geqslant 5$, and let τ be an irreducible 16-dimensional representation of G. Let D be a subgroup of G, and assume that D is a Galois group over $\mathbb{Q}_p$ for some $p \leqslant \infty$.*

(a) *Suppose that m divides $qrst$ and $m > 1$. If $D \cong D_m$ or $D \cong D_m \times (\mathbb{Z}/2\mathbb{Z})$ then τ_D is a direct sum of 2-dimensional irreducible representations, and $p \geqslant 5$.*

Next suppose that mn divides $qrst$ and $m, n > 1$. If $D \cong D_m \times D_n$ then τ_D is a direct sum of 4-dimensional irreducible representations, and again $p \geqslant 5$.

(b) *If D is not isomorphic to one of the groups mentioned in* (a), *then τ_D is symplectic.*

Proof. We merely sketch the argument, leaving the details as an exercise. The key point is that neither $(\mathbb{Z}/2\mathbb{Z})^3$ nor any group admitting $(\mathbb{Z}/2\mathbb{Z})^3$ as quotient is a Galois group over $\mathbb{Q}_p$ for $p \geqslant 3$, while neither $(\mathbb{Z}/2\mathbb{Z})^4$ nor any D_m (m an odd integer $\geqslant 5$) is a Galois group over $\mathbb{Q}_2$. Using these facts one finds that D is isomorphic to a group on the following list:

(1) D_m, where $m > 1$ and $m | qrst$.
(2) $D_m \times (\mathbb{Z}/2\mathbb{Z})$, where $m > 1$, $m | qrst$, and $m \neq qrst$.
(3) $D_m \times D_n$, where $m, n > 1$ and $mn | qrst$.
(4) $(\mathbb{Z}/2\mathbb{Z})^\nu$, where $0 \leqslant \nu \leqslant 3$.
(5) $H \times (\mathbb{Z}/\ell\mathbb{Z})$, where H is as in (1), (2), (3), or (4), $\ell > 1$, and either $\ell m | qrst$ (if H is as in (1) or (2)) or $\ell mn | qrst$ (if H is as in (3)) or $\ell | qrst$ and the number of primes dividing ℓ is at most $4 - \nu$ (if H is as in (4)).

Cases (1), (2), and (3) are the ones mentioned in part (a) of the proposition, and the stated decomposition of τ_D follows from the fact that τ is the exterior tensor product of irreducible 2-dimensional representations of the factors D_q, D_r, D_s, and D_t. Cases (4) and (5) correspond to part (b) of the proposition. In case (5), τ_D is symplectic because it is the exterior tensor product of an orthogonal representation of H and a symplectic representation of $\mathbb{Z}/\ell\mathbb{Z}$ (namely a representation of the form $\chi \oplus \overline{\chi}$ where χ is a character of $\mathbb{Z}/\ell\mathbb{Z}$). In case (4) the key point is that $\nu < 4$. Indeed if $P \cong (\mathbb{Z}/2\mathbb{Z})^4$ is any 2-Sylow subgroup of G then τ_P contains each character of P with multiplicity one. Hence if $D \cong (\mathbb{Z}/2\mathbb{Z})^\nu$ then τ_D contains each character of D with multiplicity $2^{4-\nu}$, and for $\nu \leqslant 3$ we conclude that τ_D is symplectic.

6. The Schur index

As before, F denotes a number field. If τ is an irreducible representation of $\mathrm{Gal}(\overline{F}/F)$ then τ factors through a finite quotient of $\mathrm{Gal}(\overline{F}/F)$ and therefore its Schur index $m(\tau)$ is defined.

PROPOSITION 16. *Let τ be an irreducible representation of $\mathrm{Gal}(\overline{F}/F)$ with real-valued character. Assume that τ_v is symplectic whenever v is a place of F dividing 2 or 3. If $m(\tau) = 2$ then $W(E, \tau) = 1$ for every elliptic curve E over F.*

Proof. Let v be a place of F not dividing 2 or 3. It suffices to verify that τ_v satisfies condition (a) in part (ii) of Theorem 3. Suppose then that $\rho \in R_v$ is given, and choose a finite Galois extension K of F such that τ factors through the group $G = \mathrm{Gal}(K/F)$ and ρ factors through a decomposition subgroup D of G at v. Identify τ_v with τ_D and write ρ^G for the representation of G obtained by inducing ρ from D. Since ρ is realizable over $\mathbb{Q}$ so is ρ^G, and consequently $m(\tau)$ divides $\langle \rho^G, \tau \rangle$. Hence if $m(\tau) = 2$ then $\langle \rho, \tau_D \rangle$ is even by Frobenius reciprocity.

To deduce Proposition E of the introduction we use:

LEMMA . *Let G be a finite group, D an abelian subgroup, and τ an irreducible representation of G with real-valued character. If $m(\tau) = 2$ then τ_D is symplectic.*

Proof. We must check that if χ is a character of D such that $\chi^2 = 1$, then $\langle \chi, \tau_D \rangle$ is even. This follows from Frobenius reciprocity, because $m(\tau)$ divides $\langle \chi^G, \tau \rangle$.

Since it is not yet known whether an arbitrary finite simple group can be realized as a Galois group over $\mathbb{Q}$, it may be premature to inquire too deeply about the corresponding irreducible representations. Nevertheless, in light of Theorem 3 the following question seems natural:

Question. Given a nonabelian finite simple group G and an irreducible even-dimensional representation τ of G with real-valued character and Schur index 1, does there exist a subgroup D of G and a one-dimensional character χ of D with $\chi^2 = 1$ such that D is a Galois group over $\mathbb{Q}_p$ for some $p < \infty$ and $\langle \chi, \tau_D \rangle$ is odd?

Of course Proposition D shows that for an arbitrary finite group the answer is negative in general, even if one formulates the question in such a way as to allow the representations $\hat{\sigma}_e$.

7. A final remark

In conclusion, we point out that just as the inverse problem of Galois theory becomes easy if in place of the base field $\mathbb{Q}$ we allow number fields of arbitrarily

large degree, so also the realization problem for Galois representations becomes easy if in place of elliptic curves we allow abelian varieties of arbitrarily large dimension:

PROPOSITION 17. *Let K be a finite Galois extension of $\mathbb{Q}$ and τ any representation of* $\mathrm{Gal}(K/\mathbb{Q})$. *Then there exists an abelian variety A over $\mathbb{Q}$ such that τ is equivalent to a subrepresentation of the natural representation of* $\mathrm{Gal}(K/\mathbb{Q})$ *on* $\mathbb{C} \otimes_{\mathbb{Z}} A(K)$.

Proof. Choose an elliptic curve E over $\mathbb{Q}$ with positive Mordell-Weil rank, view E as an elliptic curve over K, and put

$$A = \mathrm{Res}_{K/\mathbb{Q}} E$$

(restriction of scalars from K down to $\mathbb{Q}$). It will suffice to show that the regular representation of $\mathrm{Gal}(K/\mathbb{Q})$ occurs as a subrepresentation of $\mathbb{C} \otimes A(K)$, for then τ occurs as a subrepresentation of $\mathbb{C} \otimes A^m(K)$ for some m.

Put $G = \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ and write n for the cardinality of G. We make the identification

$$E^n(\overline{\mathbb{Q}}) \cong E(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Z}[G],$$

writing elements of $E^n(\overline{\mathbb{Q}})$ as formal sums

$$\sum_{g \in G} e_g \otimes g$$

with $e_g \in E(\overline{\mathbb{Q}})$. Given $g \in G$, let $\tilde{g}$ denote any extension of g to an automorphism of $\overline{\mathbb{Q}}$. According to the definition of restriction of scalars ([19], p. 5), there is a map $\theta : A \to E$ defined over K such that the associated map $\Theta : A \to E^n$ given on $\overline{\mathbb{Q}}$-points by

$$a \mapsto \sum_{g \in G} \tilde{g}\theta(\tilde{g}^{-1}a) \otimes g \tag{7.1}$$

is a K-isomorphism.

Define an action of G on $E^n(K)$ by the formula

$$h \cdot \left(\sum_{g \in G} e_g \otimes g \right) = \sum_{g \in G} h(e_g) \otimes hg \qquad (h \in G). \tag{7.2}$$

Note that this is *not* the natural action of G on $E^n(K)$ when E^n is regarded as a variety over $\mathbb{Q}$. For $a \in A(K)$, (7.1) and (7.2) give

$$\Theta(ha) = h\Theta(a).$$

It follows that $A(K)$ and $E^n(K)$ are isomorphic as G-modules. But $E^n(K)$ contains the G-submodule $E^n(\mathbb{Q})$, and as a G-module, $\mathbb{C} \otimes E^n(\mathbb{Q})$ is isomorphic to r copies of the regular representation, where $r > 0$ is the rank of $E(\mathbb{Q})$ (cf. (7.2)). This completes the proof.

References

1. Buhler, J.: Icosahedral Galois Representations, *Lect. Notes in Math.* 654, Springer-Verlag, 1978.
2. Deligne, P.: Les constantes des équations fonctionelles des fonctions L, Modular Functions of One Variable, II, *Lect. Notes in Math.* 349, Springer-Verlag, 1973, pp. 501–595.
3. Deligne, P.: Les constantes locales de l'équation fonctionelle de la fonction L d'Artin d'une représentation orthogonale, *Invent. Math.* 35 (1976) 299–316.
4. Fröhlich, A. and Queyrut, J.: On the functional equation for the Artin L-function for characters of real representations, *Invent. Math.* 20 (1973) 125–138.
5. Greenberg, R.: Non-vanishing of certain values of L-functions, Analytic Number Theory and Diophantine Problems, *Prog. in Math.* 70, Birkhauser, Boston, 1987, pp. 223–235.
6. Kramer, K. and Tunnell, J.: Elliptic curves and local ε-factors, *Compos. Math.* 46 (1982) 307–352.
7. LaMacchia, S. E.: Polynomials with Galois group PSL(2, 7), *Comm. in Algebra* 8 (1980) 983–992.
8. Manduchi, E.: Root numbers of fibers of elliptic surfaces, *Compos. Math.* (to appear).
9. Matzat, B. H.: Konstruktive Galoistheorie, *Lect. Notes in Math.* 1284, Springer-Verlag, 1987.
10. Rohrlich, D. E.: The vanishing of certain Rankin-Selberg convolutions, Automorphic Forms and Analytic Number Theory, *Les publications CRM*, Montreal, 1990, pp. 123–133.
11. Rohrlich, D. E.: Variation of the root number on families of elliptic curves, *Compos. Math.* 87 (1993) 119–151.
12. Rohrlich, D. E.: Elliptic curves and the Weil-Deligne group, Elliptic Curves and Related Topics, *CRM Proceedings & Lecture Notes Vol. 4, Amer Math. Soc., Providence*, 1994, pp. 125–157.
13. Serre, J-P.: Conducteurs d'Artin des caractères réels, *Invent. Math.* 14 (1971) 173–183.
14. Serre, J-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.
15. Serre, J-P.: Local Fields, GTM vol 67, Springer-Verlag, 1979.
16. Serre, J-P. and Tate, J.: Good reduction of abelian varieties, *Ann. Math.* 88 (1968) 492–517.
17. Silverman, J. H.: The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, 1985.
18. Tate, J.: Number theoretic background, Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math. Vol. 33 – Part 2, *Amer. Math. Soc.*, Providence, 1979.
19. Weil, A.: Adeles and Algebraic Groups, *Notes by M. Demazure and T. Ono*, Birkhauser-Boston, Boston, 1982.