EXAMPLE OF CALCULATING A LOCAL TWISTED ROOT NUMBER OF AN ELLIPTIC CURVE WITH WILD RAMIFICATION

MARIA SABITOVA

Abstract. In this paper we study a local twisted root number attached to an elliptic curve E with wild ramification over a local field K of characteristic zero and of residual characteristic 3. The main result is a formula for the root number attached to E and the representation of $\mathrm{Gal}(\overline{K}/K)$ induced by the trivial representation of a finite Galois extension of K.

Introduction

The main object of the paper is the local root number $W(E,\tau)$ attached to an elliptic curve E over a finite extension K of $\mathbb{Q}_p$ and a complex orthogonal (continuous) representation τ of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K. It can be proved that under these assumtions on τ we have $W(E,\tau)=\pm 1$ (see e.g, [R96], p. 315).

Explicit formulas for $W(E,\tau)$ in terms of τ and the representation σ'_E of the Weil–Deligne group of K attached to E have been obtained by D. Rohrlich [R96] in the case when E has potential multiplicative reduction over K and under the additional assumption $p \geq 5$ in the case when E has potential good reduction over K. Assuming that E has potential good reduction over K (so that $\sigma'_E = \sigma_E$ is a representation of the Weil group of K), other results in this direction include formulas for $W(E,\tau)$ in terms of σ_E by K. Kramer and J. Tunnell [KT82] in the case when τ is the trivial representation 1_K of $\mathrm{Gal}(\overline{K}/K)$ and σ_E is induced by a character of an unramified quadratic extension H of K, by D. Rohrlich [R93], [R95] in the case when $\tau = 1_K$ in terms of the coefficients of an arbitrary generalized Weierstrass equation of E, by S. Kobayshi [Ko02] when $p=3$ and $\tau = 1_K$ in terms of the coefficients of a certain Weierstrass equation of E, by T. Dokchitser and V. Dokchitser [DD08] as well as D. Whitehouse [W] when $p=2$ and $\tau = 1_K$ in terms of the coefficients of a Weierstrass equation of E. There are also some partial results with additional assumptions on E when $p=2,3$ (e.g., E has good reduction over K). However, the cases $p=2,3$, τ is arbitrary, and E has potential good reduction over K such that σ_E is irreducible still remain untreated.

To calculate $W(E,\tau)$ one can use the approach used by D. Rohrlich, i.e, to employ Serre's induction theorem, which asserts that a complex orthogonal representation τ of

Date: May 7, 2012.

Supported by NSF grant DMS-0901230 and by grants 60091-40 41, 64620-00 42 from The City University of New York PSC-CUNY Research Award Program.

$\mathrm{Gal}(\overline{K}/K)$ is a linear combination with integer coefficients of representations of the form $\mathrm{Ind}_{\mathrm{Gal}(\overline{K}/F)}^{\mathrm{Gal}(\overline{K}/K)}\pi$ (denoted by $\mathrm{Ind}_K^F\pi$), where $F\subset\overline{K}$ is a finite extension of K and π is either the trivial representation 1_F of $\mathrm{Gal}(\overline{K}/F)$, or π is a one-dimensional representation of $\mathrm{Gal}(\overline{K}/F)$ of order 2, or $\pi=\chi\oplus\overline{\chi}$, where χ is a one-dimensional representation of $\mathrm{Gal}(\overline{K}/F)$ of finite order ≥ 3, or π is dihedral (i.e., a two-dimensional complex irreducible orthogonal representation of $\mathrm{Gal}(\overline{K}/F)$ with finite image). Thus, one can first try to find formulas for $W(E,\mathrm{Ind}_K^F\pi)$, where F is a finite extension of K and π is one of the types described above, and then take into account that root numbers are multiplicative in short exact sequences. The case $\pi=\chi\oplus\overline{\chi}$ follows immediately from the properties of root numbers and the case of a one-dimensional representation π of $\mathrm{Gal}(\overline{K}/F)$ of order 2 can be reduced to the case $\pi=1_F$. Hence, two main instances to consider is when π is trivial and π is dihedral. In this paper we focus on the case $p=3$, $\pi=1_F$, and F satisfies an additional condition that it is Galois over K. Under these assumptions we give a formula for $W(E,\tau)$ in terms of σ_E and τ in the form analogous to the one used by D. Rohrlich with extra terms specific to our situation. The main results of the paper are contained in Proposition 2.1 (when σ_E is induced by a character of an unramified quadratic extension H of K) and in Proposition 3.1 together with Theorem 3.2 (when H is ramified over K).

The paper is organized in the following way: Section 1 contains a list of general facts and notation used in the paper as well as some preliminary results on the structure of the representation σ_E when H is ramified over K. Section 2 treats the case when H is unramified over K, whereas Sections 3 and 4 treat the case when H is ramified over K. Appendix A describes representations arising in the calculation, namely, symplectic representations of groups of the form $G=(A\rtimes B)\rtimes C$, where A, B are finite cyclic groups of coprime orders, and C is an infinite cyclic group. Appendix B contains the rest of the proof of Theorem 3.2 (when H is ramified over K and the ramification index of F over K is odd). Finally, Appendix C contains specific examples showing that our formula for $W(E,\tau)$ becomes more complicated without the assumption that F is Galois over K.

Acknowledgements. I would like to thank Kenneth Kramer and David Rohrlich for their interest in this work and useful inspiring discussions. I am also very grateful to Shinichi Kobayashi for answering a question regarding his paper [Ko02].

1. General facts and notation

In what follows K is a local non-archimedean field of zero characteristic with the ring of integers $\mathcal{O}_K$, the maximal ideal $\mathfrak{p}_K\subset\mathcal{O}_K$, a uniformizer ϖ_K, and the residue field $\hat{K}$ of characteristic p and cardinality q. Equivalently, K is a finite extension of $\mathbb{Q}_p$. We denote by $\mathfrak{D}(K/\mathbb{Q}_p)$ the absolute different of K and by $\overline{K}$ a fixed algebraic closure of K. We also fix a valuation on K satisfying $\mathrm{val}_K\varpi_K=1$.

We call a continuous non-trivial homomorphism $\lambda: K\longrightarrow\mathbb{C}^\times$ of absolute value 1 *an (additive) character of* K and we call a continuous homomorphism $\mu: K^\times\longrightarrow\mathbb{C}^\times$ of finite order *a (multiplicative) character of* $K^\times$. For an additive character λ of K we denote by $n(\psi)$ the largest integer n such that ψ is trivial on $\varpi_K^{-n}\mathcal{O}_K$. Throughout the paper we will identify one-dimensional complex (continuous) representations of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K with characters of $K^\times$ via the local class field theory. We also denote by $\chi_{H/K}$ the quadratic character of $K^\times$ with kernel $N_{H/K}(H^\times)$ or, equivalently, $\chi_{H/K}$ is the one-dimensional representation of $\mathrm{Gal}(\overline{K}/K)$ of order 2 with kernel $\mathrm{Gal}(\overline{K}/H)$.

Let $\Phi_K \in \mathrm{Gal}(\overline{K}/K)$ be a preimage of the Frobenius automorphism under the decomposition map, which we will call *a Frobenius of* $\mathrm{Gal}(\overline{K}/K)$. Let ω denote the unramified one-dimensional representation of $\mathrm{Gal}(\overline{K}/K)$ satisfying

$$\omega(\Phi_K) = q.$$

By definition, the Weil group $\mathcal{W}(\overline{K}/K)$ of K is a subgroup of $\mathrm{Gal}(\overline{K}/K)$ equal to $\mathrm{Gal}(\overline{K}/K^{unr}) \rtimes \langle \Phi_K \rangle$, where $K^{unr} \subset \overline{K}$ denotes the maximal unramified extension of K contained in $\overline{K}$, $\langle \Phi_K \rangle$ denotes the infinite cyclic group generated by Φ_K, and $I_K = \mathrm{Gal}(\overline{K}/K^{unr})$ is the inertia group of K.

Let $F \subset \overline{K}$ be a finite extension of K and let $\tau = \mathrm{Ind}_K^F 1_F$ denote the representation of $\mathrm{Gal}(\overline{K}/K)$ induced by the trivial representation 1_F of the subgroup $\mathrm{Gal}(\overline{K}/F)$. Given an elliptic curve E over K we are interested in calculating the twisted root number $W(E, \tau)$ in the case when $p = 3$ and E has potential good reduction over K. Thus from now on we assume that both conditions hold. Let l be a rational prime different from p, let $T_l(E)$ be the l-adic Tate module of E, and let σ_E denote the (2-dimensional) representation of $\mathcal{W}(\overline{K}/K)$ associated to the representation $\sigma_{E,l,\imath}$ of $\mathrm{Gal}(\overline{K}/K)$ on $(T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)^* \otimes_\imath \mathbb{C}$, where $\imath$ is an embedding of $\mathbb{Q}_l$ into $\mathbb{C}$. It is known that σ_E is the restriction of $\sigma_{E,l,\imath}$ to $\mathcal{W}(\overline{K}/K)$, which does not depend on the choice of l and $\imath$. We have by definition

$$W(E, \tau) = W(\sigma_E \otimes \tau),$$

where τ is considered as a representation of $\mathcal{W}(\overline{K}/K)$ via the restriction. By properties of root numbers,

$$W(\sigma_E \otimes \tau) = W(\sigma_E \otimes \omega^{1/2} \otimes \tau),$$

where $\sigma = \sigma_E \otimes \omega^{1/2}$ is symplectic (see e.g., [R94], Proposition on p. 150).

In the next few paragraphs we collect facts concerning elliptic curves that will be needed later.

Let $\Delta \in K$ denote a fixed discriminant of E, $N = K(\Delta^{1/4}, E[2])$, $H = K(\Delta^{1/2})$, $M = K(E[2])$, and $S = K(\Delta^{1/4})$. It is known that $H \subset M$, M is a finite Galois extension of K with $\mathrm{Gal}(M/K)$ being isomorphic to a subgroup of the symmetric group S_3 on 3 letters, $N^{unr} = K^{unr}(\Delta^{1/4}, E[2])$ is a finite Galois extension of K^{unr}, and N^{unr} is the minimal extension of K^{unr} over which E has good reduction ([Kr90], p. 362). From now on we assume that σ_E is irreducible. Then H is a quadratic extension of K and σ_E is induced by a one-dimensional representation of $\mathcal{W}(\overline{K}/H)$ (see e.g., [Ko02], p. 613, Prop. 3.3ii). By Lemma A.1 (see Appendix A below), σ has finite image and hence it is induced by a character ϕ of $H^\times$. We make an additional assumption that ϕ is wildly ramified, so that $\mathrm{Gal}(M/K) \cong S_3$.

If H is unramified over K, then $\mathrm{Gal}(N^{unr}/K^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$ or $\mathrm{Gal}(N^{unr}/K^{unr}) \cong \mathbb{Z}/6\mathbb{Z}$, $\mathrm{Gal}(S^{unr}/K^{unr}) \cong \mathbb{Z}/2\mathbb{Z}$.

If H is ramified over K, then

$$\mathrm{Gal}(N^{unr}/K^{unr}) \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$$

with the uniquely defined non-trivial action of $\mathbb{Z}/4\mathbb{Z}$ on $\mathbb{Z}/3\mathbb{Z}$, so that $\mathrm{Gal}(S^{unr}/K^{unr}) \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{Gal}(N^{unr}/S^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$. Let $a \in \mathrm{Gal}(N^{unr}/S^{unr})$ be an element of order 3 and let $b \in \mathrm{Gal}(N^{unr}/K^{unr})$ be an element of order 4 that maps onto a generator of $\mathrm{Gal}(S^{unr}/K^{unr})$ under the quotient map. We will need the following

Lemma 1.1. *Let F be a finite Galois extension of K contained in $\overline{K}$ such that $F \cap H = K$ and let $L = FH$. Then $L^{unr} \cap M^{unr} = H^{unr}$ and if $e(H/K) = 2$, then in addition $L^{unr} \cap N^{unr} = H^{unr}$.*

Proof. Assume that $M^{unr} \subseteq L^{unr}$. Let F_t be the maximal tamely ramified extension of K contained in F and let $L_t = F_t H$, $T = L_t M$. Since $[M : H] = e(M/H) = 3$, we have $L_t \cap M = H$, $L_t^{unr} \cap M^{unr} = H^{unr}$, and $T^{unr} \subseteq L^{unr}$. The restriction map gives the surjection $f : \mathrm{Gal}(L^{unr}/L_t^{unr}) \twoheadrightarrow \mathrm{Gal}(T^{unr}/L_t^{unr})$. Note that there are natural isomorphisms $\mathrm{Gal}(L^{unr}/L_t^{unr}) \cong \mathrm{Gal}(L/L_t)$ and $\mathrm{Gal}(T^{unr}/L_t^{unr}) \cong \mathrm{Gal}(T/L_t)$, which are induced by the restriction maps. These together with f give the surjection $g : \mathrm{Gal}(L/L_t) \twoheadrightarrow \mathrm{Gal}(T/L_t)$, which commutes with the natural action of $\mathrm{Gal}(\overline{K}/F_t)$. On the other hand, $\mathrm{Gal}(T/F_t) \cong \mathrm{Gal}(T/L_t) \rtimes \mathbb{Z}/2\mathbb{Z} \cong S_3$ and $\mathrm{Gal}(L/F_t) \cong \mathrm{Gal}(L/L_t) \times \mathbb{Z}/2\mathbb{Z}$. This implies that there exists an element γ in $\mathrm{Gal}(\overline{K}/F_t)$ with $\gamma|_{L_t} \neq \mathrm{id}_{L_t}$ that acts trivially on $\mathrm{Gal}(L/L_t)$ and non-trivially on $\mathrm{Gal}(T/L_t)$. This gives a contradiction with the existence of g.

Assume now that $e(H/K) = 2$ and $S^{unr} \subseteq L^{unr}$. Thus the restriction map gives the surjection

$$h : \mathrm{Gal}(L^{unr}/K^{unr}) \twoheadrightarrow \mathrm{Gal}(S^{unr}/K^{unr}),$$

where $\mathrm{Gal}(L^{unr}/K^{unr}) \cong \mathrm{Gal}(L^{unr}/H^{unr}) \times \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Gal}(S^{unr}/K^{unr}) \cong \mathbb{Z}/4\mathbb{Z}$. This is a contradiction, since h induces a surjection of the exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(L^{unr}/H^{unr}) \arrow[r] \arrow[d, two heads] & \mathrm{Gal}(L^{unr}/K^{unr}) \arrow[r] \arrow[d, two heads] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, two heads] & 1 \\
1 \arrow[r] & \mathrm{Gal}(S^{unr}/H^{unr}) \arrow[r] & \mathrm{Gal}(S^{unr}/K^{unr}) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 1,
\end{tikzcd}$$

the first of which splits and the second does not. □

Lemma 1.2. *Let E be an elliptic curve over K with potential good reduction over K and let $N \subset \overline{K}$ be a finite extension of K such that $N^{unr} \subset \overline{K}$ is the minimal extension of K^{unr} over which E has good reduction. Assume that σ_E is irreducible and induced by a wildly* *ramified character of a totally ramified quadratic extension H of K. Let $\Phi_N \in \mathrm{Gal}(\overline{K}/N)$ be a Frobenius considered as a Frobenius of $\mathrm{Gal}(\overline{K}/K)$ and $c = \Phi_N$. Then*

$$\mathcal{W}(\overline{K}/K)/I_N \cong (\langle a\rangle \rtimes \langle b\rangle) \rtimes \langle c\rangle,$$

where $|a| = 3$, $|b| = 4$, $b^{-1}ab = a^2$, $ac = ca$, $c^{-1}bc = b^r$, and $r = (-1)^{f(H/\mathbb{Q}_3)}$. Moreover, there exist a root of unity η satisfying $\eta^2 = (-1)^{f(H/\mathbb{Q}_3)}$, a primitive third root of unity ξ, and a one-dimensional representation ϕ of the subgroup $\mathcal{W}(\overline{K}/H)/I_N \cong \langle a, b^2, c\rangle$ such that $\phi(a) = \xi$, $\phi(b^2) = -1$, $\phi(c) = \eta$, and $\sigma = \sigma_E \otimes \omega^{1/2}$ is induced by ϕ. Thus, in a suitable basis we have

$$\sigma(a) = \begin{pmatrix} \xi & 0 \\ 0 & \xi^2 \end{pmatrix}, \quad \sigma(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \sigma(c) = \eta \begin{pmatrix} 1 & 0 \\ 0 & (-1)^{f(H/\mathbb{Q}_3)} \end{pmatrix}.$$

Proof. First, note that $\mathcal{W}(\overline{K}/K)/I_N \cong \mathrm{Gal}(N^{unr}/K^{unr}) \rtimes \langle \Phi_N\rangle$. It is easy to check that $\Phi_N^{-1} \circ a \circ \Phi_N = a$. Also, let $\xi_4 \in \overline{K}$ be the forth-root of unity such that $b(\Delta^{1/4}) = \xi_4 \Delta^{1/4}$. Then for $r = (-1)^{f(K/\mathbb{Q}_3)}$ we have

$$\Phi_N^{-1} \circ b \circ \Phi_N(\Delta^{1/4}) = \Phi_N^{-1} \circ b(\Delta^{1/4}) = \Phi_N^{-1}(\xi_4)\Delta^{1/4} = \xi_4^r \Delta^{1/4} = b^r(\Delta^{1/4})$$

and hence $\Phi_N^{-1} \circ b \circ \Phi_N \circ b^{-r} = a^t$ for some $t \in \{0, 1, 2\}$. For any $\alpha \in E[2]$ we have $b^{1-r}(\alpha) = a^t(\alpha)$, since $\Phi_N(\alpha) = \alpha$. If $r = 1$, then $t = 0$. If $r = -1$, then $b^2(\alpha) = a^t(\alpha)$. Since the order of a is 3 and the order of b is 4, we have $t = 0$ in this case as well.

Denote $G = (\langle a\rangle \rtimes \langle b\rangle) \rtimes \langle c\rangle$. Note that σ can be considered as an irreducible symplectic representation of G. Thus we can apply Proposition A.7 (see Appendix A below) to σ, so that σ is obtained from a one-dimensional representation ψ_1 of A. Note that if ψ_1 is trivial, then σ_E is tame, which contradicts the assumption. Hence ψ_1 is a primitive third root of unity ξ. Then in the notation of Proposition A.7, $\Gamma = A \rtimes \langle b^2\rangle$ and ψ_2 is a one-dimensional representation of $\langle b^2\rangle$, i.e., $\psi_2(b^2) = \pm 1$. Let $\phi = \psi_1 \otimes \psi_2$, where ψ_1 and ψ_2 are considered as representations of Γ. The stabilizer of $\mathrm{Ind}_\Gamma^{A\rtimes\langle b\rangle} \phi$ is G and the stabilizer F of ϕ in G is $\langle A, b^2, c\rangle$. Thus $\sigma \cong \mathrm{Ind}_F^G \mu$, where μ is an extension of ϕ to F such that $\mu(b^2) = -1$ and $\mu_b = \bar{\mu}$. In particular,

$$\mu(c)^{-1} = \bar{\mu}(c) = \mu_b(c) = (-1)^{\frac{1-r}{2}} \mu(c),$$

which implies the second part of the lemma. $\square$

We will also need a character θ of $H^\times$ such that $(\phi \otimes \theta)|_{K^\times} = 1_K$, where ϕ is considered as a character of $H^\times$ via the local class field theory.

Lemma 1.3. *In the notation of Lemma 1.2 let θ be a character of $H^\times$ given by $\theta(a) = 1$, $\theta(b^2) = -1$, and $\theta(c) = \gamma$ for a root of unity γ satisfying $\gamma^2 = (-1)^{f(H/\mathbb{Q}_3)}$. Then*

$$\theta|_{K^\times} = \chi_{H/K}, \quad (\phi \otimes \theta)|_{K^\times} = 1_K, \quad \textit{and} \quad a(\theta) = 1.$$

Proof. Interpreting the condition $(\phi\otimes\theta)|_{K^\times}=1_K$ in terms of Weil groups via the local class field theory we need to show that $(\phi\otimes\theta)\circ tr:\mathcal{W}(\overline{K}/K)^{ab}\longrightarrow\mathbb{C}^\times$ is trivial, where $tr:\mathcal{W}(\overline{K}/K)^{ab}\longrightarrow\mathcal{W}(\overline{K}/H)^{ab}$ is the transfer map. In the notation of Lemma 1.2 let $G=\langle a,b,c\rangle$ and $M=\langle a,b^2,c\rangle$. Since ϕ is trivial on I_N, it is enough to show that $\phi\otimes\theta$ composed with the transfer map $tr:G^{ab}\longrightarrow M^{ab}$ is trivial (here both ϕ and θ are considered as one-dimensional representations of M). By calculating the transfer map explicitly and using the definition of ϕ given in Lemma 1.2 it is easy to verify that $\theta|_{K^\times}=\phi|_{K^\times}=\chi_{H/K}$. Since the restriction of θ to the inertia group I_H has order two, we have $a(\theta)=1$. (See also [R96], p. 316, Prop. 1 for a proof that $\phi|_{K^\times}=\chi_{H/K}$.) □

To calculate the root number $W(E,\tau)$ we will follow the approach of D. Rohrlich developed in [R96]. Let $\tau=\operatorname{Ind}_K^F\pi$, where $F\subset\overline{K}$ is a finite extension of K, π is a continuous complex finite-dimensional representation of $\operatorname{Gal}(\overline{K}/F)$ with real-valued character, and $\operatorname{Ind}_K^F\pi$ denotes the representation of $\operatorname{Gal}(\overline{K}/K)$ induced by π from the subgroup $\operatorname{Gal}(\overline{K}/F)$. We will need the following formula ([R96], p. 321):

$$W(E,\tau)=W(\sigma\otimes\tau)=W((\operatorname{Res}_K^F\sigma)\otimes\pi)\frac{\det\tau(-1)}{\det\pi(-1)},\tag{1.1}$$

where $\operatorname{Res}_K^F\sigma$ denotes the restriction of σ onto the subgroup $\operatorname{Gal}(\overline{K}/F)$ of $\operatorname{Gal}(\overline{K}/K)$.

Lemma 1.4. *Let $\tau=\mathit{Ind}_K^F\pi$. If π has a real-valued character and $H\subseteq F$, then*

$$W(E,\tau)=(-1)^\delta\det\tau(-1),\quad \delta=\begin{cases}\frac{\dim\tau}{2}f(K/\mathbb{Q}_3), & H/K\ \textit{ramified},\\ 0, & H/K\ \textit{unramified}.\end{cases}\tag{1.2}$$

Proof. The calculation is the same as on p. 321 in [R96], which we repeat for the sake of completeness. Recall that by assumption $\sigma=\operatorname{Ind}_K^H\phi$. We have $\operatorname{Res}_K^F\sigma=\tilde\phi\oplus\tilde\phi^{-1}$ with $\tilde\phi=\operatorname{Res}_H^F\phi$, since σ is symplectic. Since π has real-valued character, using properties of root numbers we have

$$W((\operatorname{Res}_K^F\sigma)\otimes\pi)=\det(\pi\otimes\tilde\phi)(-1)=\det\pi(-1)\phi(-1)^{[F:H]\dim\pi},$$

where $\phi(-1)=\chi_{H/K}(-1)$ and $\chi_{H/K}(-1)=(-1)^{f(K/\mathbb{Q}_3)}$ if H/K is ramified, $\chi_{H/K}(-1)=1$ if H/K is unramified. Hence (1.2) follows from (1.1). □

From now on we assume that $F\cap H=K$ and $\tau=\operatorname{Ind}_K^F 1_F$. Let $L=FH$, $\lambda=\operatorname{Res}_H^L\phi$, and let ψ_F be an additive character of F. Then by the results on p. 322 in [R96],

$$W(E,\tau)=W(\lambda,\psi_L)W(\chi_{L/F},\psi_F)\det\tau(-1),\tag{1.3}$$

where $\psi_L=\psi_F\circ\operatorname{Tr}_{L/F}$.

Remark 1.5. If μ is a continuous complex finite-dimensional representation of $\mathcal{W}(\overline{K}/K)$, then the definition of root number $W(\mu)$ of μ depends on the choice of an additive character ψ_K of K. It turns out that $W(\operatorname{Res}_K^F\sigma)$ does not depend on the choice of an additive character of F, since σ (and hence $\operatorname{Res}_K^F \sigma$) is symplectic ([R96], p. 315). This explains why ψ_F is arbitrary in (1.3), because in (1.1)

$$W(\operatorname{Res}_K^F \sigma) = W(\operatorname{Res}_K^F \sigma, \psi_F) = W(\lambda, \psi_F \circ \operatorname{Tr}_{L/F}) W(\chi_{L/F}, \psi_F)$$

by the properties of root numbers.

2. The case when H/K is unramified

We keep the notation of Section 1. In this section we assume that H/K is unramified. Let $\operatorname{Gal}(N^{unr}/H^{unr}) = \langle a \rangle$, where the order $|a|$ of a is 3 or 6, and let ϕ be a one-dimensional representation of $\mathcal{W}(\overline{K}/H)$ such that $\ker(\phi|_{I_H}) = I_N$, so that $\phi(a)$ is a primitive 3rd root of unity if $|a| = 3$ and $\phi(a)$ is a primitive 6th root of unity if $|a| = 6$ (such ϕ exists because σ is induced by a character of $H^\times$ and $\ker(\sigma_E|_{I_K}) = I_N$). Note that by Proposition 1 on p. 316 in [R96] we have $\phi|_{K^\times} = \chi_{H/K}$.

Proposition 2.1. *Assume that H is an unramified quadratic extension of K, $\sigma = \operatorname{Ind}_K^H \phi$, and ϕ is wildly ramified. Let $H = K(u_{H/K})$, where $u_{H/K} \in \mathcal{O}_H^\times$, $u_{H/K}^2 \in \mathcal{O}_K$, and let θ be a character of $H^\times$ satisfying $a(\theta) \leq 1$ and $\theta|_{K^\times} = \chi_{H/K}$. Denote $\chi = \chi_{H/K}$, $\hat{\sigma} = \operatorname{Ind}_K^H(\phi \otimes \theta)$. If $\tau = Ind_K^F 1_F$ and F is Galois over K, then*

$$W(E, \tau) = (-1)^A \phi(u_{H/K})^{\dim \tau} \det \tau(-1), \tag{2.1}$$

where

$$A = (a(\phi) - e(H/K)) \dim \tau + \langle \tau, \chi \rangle + \langle \tau, 1 \rangle + \langle \tau, \hat{\sigma} \rangle.$$

Proof. By Proposition 3 on p. 319 in [R96] we have

$$W(E, \tau) = (-1)^{a(\lambda)} \phi(u_{H/K})^{\dim \tau} \det \tau(-1). \tag{2.2}$$

Let $\tilde{\theta} = \operatorname{Res}_H^L \theta$ and $\lambda = \operatorname{Res}_H^L \phi$. Using Frobenius reciprocity we have $\langle \tau, 1 \rangle = 1$, $\langle \tau, \chi \rangle = 0$, and

$$\langle \tau, \hat{\sigma} \rangle = \langle 1_F, \operatorname{Ind}_F^L(\lambda \otimes \tilde{\theta}) \rangle = \langle 1_L, \lambda \otimes \tilde{\theta} \rangle. \tag{2.3}$$

Here $a(\lambda) > 1$, since $M^{unr} \not\subseteq L^{unr}$ by Lemma 1.1, and $a(\tilde{\theta}^{-1}) \leq 1$. Thus $\lambda \neq \tilde{\theta}^{-1}$, $\langle \tau, \hat{\sigma} \rangle = 0$, and

$$\langle \tau, \chi \rangle + \langle \tau, 1 \rangle + \langle \tau, \hat{\sigma} \rangle = 1. \tag{2.4}$$

Assume now that $\operatorname{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$, so that $N^{unr} = M^{unr}$. We consider the following three cases.

i) Let F_t be the maximal tamely ramified extension of K contained in F, let $L_t = F_t H$, and let λ_t be the restriction of ϕ to L_t. Denote $e_t = e(L_t/H) = e(F_t/K)$. By Lemma B.2 (see Appendix B below), since $a(\phi) > 1$, we have $a(\lambda_t) = (a(\phi) - 1)e_t + 1$. Since $p = 3$ and $f(F/K)$ is odd, we have $e_t \equiv [F : K] \equiv \dim \tau \bmod 2$, so that

$$a(\lambda_t) \equiv (a(\phi) - 1) \dim \tau + 1 \bmod 2.$$

ii) Assume that F is a totally ramified Galois extension of K of degree 3. We will show that $a(\lambda) \equiv a(\phi) \bmod 2$. Indeed, let $T = LM$. We have the following diagram of field extensions:

$$\begin{tikzcd} L \arrow[r, dash, "3"] & T \\ H \arrow[u, dash, "3"] \arrow[r, dash, "3"] & M \arrow[u, dash, "3"'] \end{tikzcd}$$

Let $G = \mathrm{Gal}(T/H) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Ramification groups of G have the form

$$G = G_0 = G_1 = \cdots = G_t \supset G_{t+1} = \{1\} \quad \text{or} \tag{2.5}$$

$$G = G_0 = G_1 = \cdots = G_t \supset G_{t+1} = \cdots = G_{t+s} \supset G_{t+s+1} = \{1\}, \tag{2.6}$$

where $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$. It is easy to see that depending on the embedding of G_{t+1} into G we have either

(1) $a(\phi) = a(\lambda)$, or
(2) $a(\phi) = 1 + t + \frac{s}{3}$, $a(\lambda) = 1 + t + s$, or
(3) $a(\phi) = 1 + t + \frac{s}{3}$, $a(\lambda) = 1 + t$.

Since $a(\phi)$ is an integer, $a(\phi) \equiv a(\lambda) \bmod 2$ in cases (1) and (2). Case (3) occurs when ramification groups of G have form (2.6) and G_{t+1} embeds diagonally into G. Assume that this is the case. Let a denote a generator of $\mathrm{Gal}(M/H)$, let b denote a generator of $\mathrm{Gal}(L/H)$. Then we can identify G with $\langle a \rangle \times \langle b \rangle$ via the natural isomorphism given by restrictions and without loss of generality we can assume that $G_{t+1} = \langle ab \rangle$. Let $c = \Phi_K$ be a Frobenius of $\mathrm{Gal}(\overline{K}/K)$. Since under our assumptions $\mathrm{Gal}(M/K) \cong S_3$ and $\mathrm{Gal}(L/K) \cong \mathbb{Z}/6\mathbb{Z}$, we have $cac^{-1} = a^{-1}$ and $cbc^{-1} = b$. Denote $\Gamma = \mathcal{W}(\overline{K}/K)/I_T$ and $\Lambda = \mathcal{W}(\overline{K}/H)/I_T$. Then

$$\Gamma \cong (\langle a \rangle \times \langle b \rangle) \rtimes \langle c \rangle, \quad \Lambda \cong (\langle a \rangle \times \langle b \rangle) \times \langle c^2 \rangle.$$

Let ψ denote a one-dimensional representation of Λ given by $\psi(a) = \xi$ for a primitive third root of unity ξ, $\psi(b) = \psi(c^2) = 1$, let μ be a one-dimensional representation of Γ given by $\mu(a) = \mu(c) = 1$, $\mu(b) = \xi$, and let $\rho = \mathrm{Ind}_\Lambda^\Gamma \psi = \mathrm{Ind}_K^H \psi$, so that

$$\rho(a) = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then it is easy to check that on one hand, $a(\rho \otimes \mu) = 2(t+1) + \frac{s}{3}$ and on the other hand,

$$a(\rho \otimes \mu) = a(\mathrm{Ind}_K^H(\psi \otimes \mathrm{Res}_K^H \mu)) = 2a(\psi \otimes \mathrm{Res}_K^H \mu),$$

which implies that s is even and hence $a(\phi) \equiv a(\lambda) \bmod 2$ in case (3) as well.

iii) General case: F is an arbitrary Galois extension of K. If F is tame over K, then (2.1) follows from case *i*) above together with (C.3) and (2.4). Otherwise, since $\mathrm{Gal}(F/F_t)$ is a 3-group, there exists a totally ramified Galois extension F' of F_t contained in F such that F is a totally ramified Galois extension of F' of degree 3. Using the results of case *ii*) together with the induction on the degree of F over F_t, we get $a(\lambda) \equiv a(\lambda_t) \bmod 2$.

Finally, using the results of case *i*), (C.3), and (2.4), this proves (2.1) in the case when $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$.

Assume now that $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/6\mathbb{Z}$. Since $M^{unr} \not\subseteq L^{unr}$ by Lemma 1.1, λ is wildly ramified, hence $a(\lambda^2) = a(\lambda)$ and we can apply the results for the case $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$ above. Thus

$$a(\lambda) \equiv (a(\phi^2) - 1) \dim \tau + 1 \mod 2,$$

where $a(\phi^2) = a(\phi)$. Hence, (2.1) follows from (C.3) together with (2.4). $\square$

Remark 2.2. Note that if Φ_K is a Frobenius of $\mathrm{Gal}(\overline{K}/K)$, then $\Phi_K^2 \in \mathrm{Gal}(\overline{K}/H)$ is a Frobenius of H. Let θ_1 be the unramified one-dimensional representation of $\mathcal{W}(\overline{K}/H)$ such that $\theta_1(\Phi_K^2) = -1$. If $|a| = 6$, let θ_2 be the one-dimensional representation of $\mathcal{W}(\overline{K}/H)/I_N = \langle a \rangle \rtimes \langle \Phi_K^2 \rangle$ given by $\theta_2(a) = \theta_2(\Phi_K^2) = -1$ and considered as a representation of $\mathcal{W}(\overline{K}/H)$ via the natural projection. It is easy to check that $\theta_1|_{K^\times} = \theta_2|_{K^\times} = \chi_{H/K}$. Then in Proposition 2.1 we can take θ_1 as θ in both cases $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$ and $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/6\mathbb{Z}$ and we can take θ_2 as θ in the case when $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/6\mathbb{Z}$.

Remark 2.3. If $a(\phi)$ is odd, then (2.1) agrees with the formula for $W(E,\tau)$ given by D. Rohrlich in the case when ϕ is tamely ramified and F is an arbitrary finite extension of K ([R96], p. 318, Thm. 1). However, if in Proposition 2.1 we drop the assumption that F is Galois over K, then there appears an extra term in (2.1). See Lemma C.1 in Appendix C below for a specific example.

3. The case when H/K is ramified

We keep the notation of Section 1. In this section we assume that H/K is ramified. We distinguish two cases: L is unramified over F (equivalently, the ramification index $e(F/K)$ of F over K is even) and L is ramified over F (equivalently, $e(F/K)$ is odd). Proposition 3.1 below treats the first case and Theorem 3.2 below treats the second.

Proposition 3.1. *Let H be ramified over K, $H = K(\alpha)$, where $\alpha \in \mathcal{O}_H$, $\alpha^2 \in \mathcal{O}_K$, and $\mathrm{val}_H\, \alpha = 1$. Let L be unramified over F (equivalently, $e(F/K)$ is even). If $\tau = Ind_K^F 1_F$, then*

$$W(E,\tau) = (-1)^{a(\lambda)} \phi(\alpha)^{\dim \tau} (-1)^{\frac{e(F/K)}{2}} \det \tau(-1). \tag{3.1}$$

Moreover, let θ be a character of $H^\times$ satisfying $a(\theta) \leq 1$ and $\theta|_{K^\times} = \chi_{H/K}$ (e.g., θ given by Lemma 1.3). Denote $\hat{\sigma} = Ind_K^H(\phi \otimes \theta)$ and $\chi = \chi_{H/K}$. If F is Galois over K, then

$$W(E,\tau) = (-1)^A \phi(\alpha)^{\dim \tau} \det \tau(-1), \tag{3.2}$$

where

$$A = (a(\phi) - e(H/K)) \dim \tau + \langle \tau, \chi \rangle + \langle \tau, 1 \rangle + \langle \tau, \hat{\sigma} \rangle.$$

Proof. Let ϖ_F be a uniformizer of F. Since $e(F/K)$ is even, we have $\alpha = u\varpi_F^k$ for $k = \frac{e(F/K)}{2}$, $u \in \mathcal{O}_L^\times$, $u^2 \in \mathcal{O}_F^\times$. Then $L = F(u)$ and by Propositions 1 and 3 in [R96], we have

$$W(\lambda, \psi_L) \cdot W(\chi_{L/F}, \psi_F) = (-1)^{a(\lambda)} \cdot \lambda(u).$$

Here $\lambda(u) = \lambda(\alpha)\lambda(\varpi_F)^{-k}$. Note that $\lambda|_{F^\times} = \chi_{L/F}$ (it follows from Prop. 1 on p. 316 in [R96]), hence $\lambda(\varpi_F) = \chi_{L/F}(\varpi_F) = -1$ and (3.1) follows from (1.3).

The proof of (3.2) can be reduced to the case treated in Proposition 2.1 as follows. Let F_t be the maximal tamely ramified extension of K contained in F, let $L_t = F_tH$, and let λ_t be the restriction of ϕ to L_t. Also, let $\tau_t = \mathrm{Ind}_{F_t}^F 1_F$ and $\sigma_t = \mathrm{Res}_K^{F_t}\sigma = \mathrm{Ind}_{F_t}^{L_t}\lambda_t$. On one hand, by (1.3) applied to $W(\sigma_t \otimes \tau_t)$ we have

$$W(\sigma_t \otimes \tau_t) = W(\lambda, \psi_L)W(\chi_{L/F}, \psi_F)\det \tau_t(-1). \tag{3.3}$$

On the other hand, since L_t is unramified over F_t, by Proposition 2.1 we have

$$W(\sigma_t \otimes \tau_t) = (-1)^B \lambda_t(u)^{\dim \tau_t} \det \tau_t(-1), \tag{3.4}$$

where $L_t = F_t(u)$ for some $u \in \mathcal{O}_{L_t}^\times$ such that $u^2 \in \mathcal{O}_{F_t}^\times$. As in the proof of (3.1) above we have

$$\lambda_t(u) = \phi(\alpha)^{[L_t:H]}(-1)^{e_t},$$

where $e_t = \frac{e(F_t/K)}{2} = e(L_t/H)$. Moreover, note that $\dim \tau_t = e(F/F_t)$ is a power of 3, i.e., odd. Thus, combining (1.3) with (3.3) and (3.4) we get

$$W(E, \tau) = (-1)^{B+e_t}\phi(\alpha)^{\dim \tau}\det \tau(-1). \tag{3.5}$$

We now explain what B in (3.5) is. Let χ_t denote the quadratic character χ_{L_t/F_t} corresponding to the extension L_t/F_t and let $\theta_t = \mathrm{Res}_H^{L_t}\theta$ so that $\chi_t = \mathrm{Res}_K^{F_t}\chi$, $a(\theta_t) \le 1$, and $\theta_t|_{F_t^\times} = \chi_t$. Finally, denote

$$\begin{aligned} \hat{\sigma}_t &= \mathrm{Ind}_{F_t}^{L_t}(\lambda_t \otimes \theta_t), \\ C &= \langle \tau_t, \chi_t\rangle + \langle \tau_t, 1\rangle + \langle \tau_t, \hat{\sigma}_t\rangle, \end{aligned}$$

where by the Frobenius reciprocity theorem

$$\langle \tau_t, \chi_t\rangle = \langle \tau, \chi\rangle, \quad \langle \tau_t, 1\rangle = \langle \tau, 1\rangle, \text{ and } \langle \tau_t, \hat{\sigma}_t\rangle = \langle \tau, \hat{\sigma}\rangle.$$

Then, according to Proposition 2.1

$$B = (a(\lambda_t) - 1)\dim \tau_t + C = (a(\lambda_t) - 1)\dim \tau_t + \langle \tau, \chi\rangle + \langle \tau, 1\rangle + \langle \tau, \hat{\sigma}\rangle. \tag{3.6}$$

Note that by Lemma B.2 (see Appendix B below), $a(\lambda_t) = (a(\phi)-1)e_t+1 \equiv e_t+1 \mod 2$, since $a(\phi)$ is even by Lemma B.1 (see Appendix B below). Also, $\dim \tau_t = e(F/F_t)$ is a power of 3, i.e., $\dim \tau_t$ is odd. Thus, using (3.6), we get

$$\begin{aligned} B + e_t &\equiv \langle \tau, \chi\rangle + \langle \tau, 1\rangle + \langle \tau, \hat{\sigma}\rangle \equiv \\ &\equiv (a(\phi) - e(H/K))\dim \tau + \langle \tau, \chi\rangle + \langle \tau, 1\rangle + \langle \tau, \hat{\sigma}\rangle \mod 2, \end{aligned}$$

and (3.2) follows from (3.5). $\square$

Theorem 3.2. *Suppose $e(F/K)$ is odd, $\tau = \mathit{Ind}_K^F 1_F$, $\hat{\sigma} = \operatorname{Ind}_K^H(\phi \otimes \theta)$, and e_t is the ramification index of the maximal tamely ramified extension of K contained in F. Assume in addition that F is Galois over K. Then there exists $\alpha \in \mathcal{O}_H$ (that depends on E and does not depend on τ) such that $H = K(\alpha)$, $\alpha^2 \in \mathcal{O}_K$, $\operatorname{val}_H \alpha = 1$, and satisfying the following properties. If $f(K/\mathbb{Q}_3)$ is even then*

$$W(E,\tau) = (-1)^{\langle \tau,\chi\rangle + \langle \tau,1\rangle + \langle \tau,\hat{\sigma}\rangle} \eta^{\dim \tau} \phi(\alpha)^{\dim \tau} \det \tau(-1), \quad \eta = \pm 1. \tag{3.7}$$

If $f(K/\mathbb{Q}_3)$ is odd then

$$W(E,\tau) = (-1)^{\langle \tau,\chi\rangle + \langle \tau,1\rangle + \langle \tau,\hat{\sigma}\rangle + fa} \eta^{\dim \tau} \phi(\alpha)^{\dim \tau} \det \tau(-1), \tag{3.8}$$

where $f = f(F/K)$, $\eta^2 = -1$, and

$$a = \left(\frac{e_t}{3}\right)(-1)^{\frac{e_t - 1}{2}} = \begin{cases} 1, & e_t \equiv 5 \text{ or } 7 \bmod 12, \\ 0, & \text{otherwise.} \end{cases}$$

Corollary 3.3. *Assume $f(K/\mathbb{Q}_3)$ is even when $e(H/K) = 2$ and*

$$\tau = \sum_i n_i \operatorname{Ind}_K^{F_i} 1_{F_i},$$

where each F_i is Galois over K. Also, let $H = K(\beta)$, where $\beta \in \mathcal{O}_H^\times$, $\beta^2 \in \mathcal{O}_K$ if $e(H/K) = 1$ and $\beta = \alpha$ (from Theorem 3.2) if $e(H/K) = 2$. Then

$$W(E,\tau) = (-1)^A \eta^{\dim \tau} \phi(\beta)^{\dim \tau} \det \tau(-1), \tag{3.9}$$

where $\eta = 1$ if H is unramified over K, $\eta = \pm 1$ if H is ramified over K, and

$$A = (a(\phi) - e(H/K)) \dim \tau + \langle \tau, \chi \rangle + \langle \tau, 1 \rangle + \langle \tau, \hat{\sigma} \rangle.$$

Proof. Since (3.9) is multiplicative in τ it is enough to show that (3.9) holds for each τ of the form $\operatorname{Ind}_K^F 1_F$, where F is a finite Galois extension of K.

Assume first that $H \subseteq F$. Then $W(E,\tau) = \det \tau(-1)$ by Lemma 1.4. Also, it is easy to check that $\eta^{\dim \tau} = \phi(\beta)^{\dim \tau} = 1$ in both cases $e(H/K) = 1$ and $e(H/K) = 2$. Finally, $\langle \tau, \chi \rangle = \langle \tau, 1 \rangle = 1$ and we verify that $\langle \tau, \hat{\sigma} \rangle$ is even. Note that $\hat{\sigma}$ is orthogonal by Proposition 1(ii) on p. 317 in [R96]. Let $\mu = \operatorname{Res}_H^F(\phi \otimes \theta)$. Then

$$\langle \tau, \hat{\sigma} \rangle = \langle 1_F, \mu \rangle + \langle 1_F, \bar{\mu} \rangle = 2 \langle 1_F, \mu \rangle$$

and hence (3.9) holds in this case.

Assume that H is not contained in F. If H is unramified over K, then (3.9) follows directly from Proposition 2.1. If H is ramified over K, then $a(\phi)$ is even and (3.9) follows from Proposition 3.1 and Theorem 3.2. $\square$

4. Proof of Theorem 3.2

In the notation of Section 1 throughout this section we assume that H is ramified over K, L is ramified over F (equivalently, $e(F/K)$ is odd), and F is Galois over K. To prove Theorem 3.2 we will choose a special ψ_F and calculate separately $W(\chi_{L/F}, \psi_F)$ and $W(\lambda, \psi_L)$ in (1.3).

The root number $W(\chi_{L/F}, \psi_F)$. Let g be a generator of $\mathrm{Gal}(M/H)$ (recall that $M = K(E[2])$ and $\mathrm{Gal}(M/H) \cong \mathbb{Z}/3\mathbb{Z}$) and let α, β, γ denote the x-coordinates of the 2-torsion points on E such that $g(\alpha) = \beta$, $g(\beta) = \gamma$. Let $\Delta^{1/2}$ denote a fixed quadratic root of Δ satisfying

$$\Delta^{1/2} = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha),$$

let $\Delta^{1/4}$ denote a fixed quadratic root of $\Delta^{1/2}$, and let $N = K(E[2], \Delta^{1/4})$ with our choice of $\Delta^{1/4}$. We can extend g to an element of order 3 of $\mathrm{Gal}(N/H)$, then consider g as an element of $\mathrm{Gal}(N^{unr}/H^{unr})$ via the natural isomorphism $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathrm{Gal}(N/H)$ given by the restriction, and finally regard g as an element of $\mathcal{W}(\overline{K}/H)/I_N$ via the natural embedding $\mathrm{Gal}(N^{unr}/H^{unr}) \hookrightarrow \mathcal{W}(\overline{K}/H)/I_N$. In particular, $g(\Delta^{1/4}) = \Delta^{1/4}$. Let ψ_K denote a character of K whose restriction to $\mathcal{O}_K$ is given by

$$\psi_K(x) = \phi(g)^{-\mathrm{Tr}_{\hat{K}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_K,$$

where $\bar{x}$ denotes the image of x in $\hat{K}$ under the quotient map.

Let $\sigma_F = \mathrm{Res}^F_K \sigma = \mathrm{Ind}^L_F \lambda$, so that σ_F is the analogue of σ for the elliptic curve over F obtained from E by extension of scalars. Denote $P = LM$ and $T = LN$. By Lemma 1.1, the natural restriction map

$$\mu : \mathrm{Gal}(T^{unr}/L^{unr}) \longrightarrow \mathrm{Gal}(N^{unr}/H^{unr})$$

is an isomorphism, which implies that σ_F is irreducible (by Prop. 1(i) on p. 316 in [R96]). Let $\tilde{g} \in \mathrm{Gal}(T^{unr}/L^{unr})$ be the preimage of g under μ. We consider $\tilde{g}$ as an element of $\mathcal{W}(\overline{K}/L)/I_T$ via the natural embedding $\mathrm{Gal}(T^{unr}/L^{unr}) \hookrightarrow \mathcal{W}(\overline{K}/L)/I_T$. Thus $T = F(E[2], \Delta^{1/4})$ with the above choice of $\Delta^{1/4}$, $\tilde{g}$ fixes each element of F^{unr}, $\tilde{g}(\alpha) = \beta$, $\tilde{g}(\beta) = \gamma$, $\tilde{g}(\Delta^{1/4}) = \Delta^{1/4}$, and $\lambda(\tilde{g}) = \phi(g)$. Let ψ denote a character of F whose restriction to $\mathcal{O}_F$ is given by

$$\psi(x) = \phi(g)^{-\mathrm{Tr}_{\hat{F}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_F,$$

and let ψ_F be a character of F given by

$$\psi_F(x) = \psi(e_t x). \tag{4.1}$$

(Recall that e_t is the ramification index of the maximal tamely ramified extension F_t of K contained in F.) Let $\Phi_T \in \mathcal{W}(\overline{K}/T)$ be a Frobenius. Then by the properties of root numbers combined with the results on pp. 617 – 619 in [Ko02] we have

$$W(\chi_{L/F}, \psi_F) = \chi_{L/F}(e_t) W(\chi_{L/F}, \psi) = -\chi_{L/F}(e_t)\lambda(\Phi_T).$$

Note that since $\mathrm{Gal}(\overline{K}/T^{unr})$ is in the kernel of λ, $\lambda(\Phi_T)$ does not depend on the choice of Φ_T. Let $f = f(T/N) = f(F/K)$ and let $\Phi_N \in \mathrm{Gal}(\overline{K}/N)$ be a fixed Frobenius. There exists $d \in I_N$ such that $\Phi_T = \Phi_N^f d$, hence $\lambda(\Phi_T) = \phi(\Phi_N)^f = \eta^f$ and

$$W(\chi_{L/F}, \psi_F) = -\chi_{L/F}(e_t)\eta^f. \tag{4.2}$$

Given $L_t = F_t H$ we also define characters ψ_H and ψ_L of H and L, respectively, via

$$\psi_H \;=\; \psi_K \circ \mathrm{Tr}_{H/K}, \quad \psi_L = \psi_F \circ \mathrm{Tr}_{L/F}\,.$$

Note that

$$\begin{aligned}
\psi_F(x) &= \phi(g)^{-e_t \mathrm{Tr}_{\hat{F}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_F,\\
\psi_H(x) &= \phi(g)^{-2\, \mathrm{Tr}_{\hat{H}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_H,\\
\psi_L(x) &= \phi(g)^{-2e_t \mathrm{Tr}_{\hat{L}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_L,
\end{aligned}$$

so that $n(\psi_K) = n(\psi_F) = n(\psi_H) = n(\psi_L) = -1$ and

$$\begin{aligned}
\psi_L(x) &= \psi_H \circ \mathrm{Tr}_{L_t/H}(x), \quad x \in \mathcal{O}_{L_t},\\
\psi_F(x) &= \psi_K \circ \mathrm{Tr}_{F_t/K}(x), \quad x \in \mathcal{O}_{F_t}.
\end{aligned}$$

Clearly, Φ_N is a Frobenius of both $\mathrm{Gal}(\overline{K}/H)$ and $\mathrm{Gal}(\overline{K}/K)$. We fix uniformizers ϖ_H and ϖ_K of H and K, respectively, corresponding to Φ_N via the local class field theory. Analogously, we fix uniformizers ϖ_L and ϖ_F of L and F, respectively, corresponding to Φ_T via the local class field theory. In particular, we have

$$\varpi_K = N_{H/K}\varpi_H, \quad \varpi_F = N_{L/F}\varpi_L$$

and

$$\tilde{\theta}(\varpi_L) = \theta(\varpi_H)^f = \gamma^f, \quad f = f(F/K) = f(L/H), \tag{4.3}$$

where θ is defined by Lemma 1.3 and $\tilde{\theta} = \mathrm{Res}_H^L\,\theta$. In particular,

$$\tilde{\theta}(\varpi_L)^2 = \gamma^{2f} = (-1)^{f(L/\mathbb{Q}_3)}.$$

The root number $W(\lambda, \psi_L)$. Let $H = K(\alpha)$ for some $\alpha \in \mathcal{O}_H$ such that $\alpha^2 \in \mathcal{O}_K$ and $\mathrm{val}_H\,\alpha = 1$, and let $e = e(F/K)$. By Lemma 1.1, λ is not tame and hence by Lemma B.1 (see Appendix B below), $a(\lambda)$ and $a(\phi)$ are even. We denote $a(\lambda) = \kappa$, $a(\phi) = m$. To calculate $W(\lambda, \psi_L)$ we follow Rohrlich's approach, namely make use of the Fröhlich–Queyrut's formula as follows. Note that $L = F(\alpha)$. Since θ was chosen so that $(\phi \otimes \theta)|_{K^\times} = 1_K$, we have $(\lambda \otimes \tilde{\theta})|_{F^\times} = 1_F$ and hence

$$W(\lambda \otimes \tilde{\theta}, \psi_L) = \lambda(\alpha)\tilde{\theta}(\alpha) = \phi(\alpha)^{[F:K]} \cdot \theta(\alpha)^{[F:K]},$$

where the first equality follows from Theorem 3 on p. 130 in [FQ73]. On the other hand, since $a(\tilde{\theta}) = 1$ and $n(\psi_L) = -1$, by the results on p. 546 in [D72], we have

$$W(\lambda \otimes \tilde{\theta}, \psi_L) = \tilde{\theta}(z)^{-1} W(\lambda, \psi_L),$$

where $z \in L^\times$ satisfies $\mathrm{val}_L(z) = 1 - \kappa$ and

$$\lambda(1+b) = \psi_L(zb), \quad \text{for any } b \in L \text{ with } \mathrm{val}_L(b) \geq \kappa/2. \tag{4.4}$$

Hence,

$$W(\lambda, \psi_L) = \phi(\alpha)^{[F:K]} \cdot \theta(\alpha)^{[F:K]} \cdot \tilde{\theta}(z). \tag{4.5}$$

Let $y \in H^\times$ with $\mathrm{val}_H(y) = 1 - m$ satisfy

$$\phi(1+a) = \psi_H(ya), \quad \text{for any } a \in H \text{ with } \mathrm{val}_H(a) \geq m/2. \tag{4.6}$$

Then by Lemma B.3 (see Appendix B below) we have

$$\tilde{\theta}(z) = \theta(y)^{e_t f}. \tag{4.7}$$

Let $n = a(\phi)/2$. Note that $\phi^{-1}(1 + \alpha\varpi_K^{n-1} b)$ is an additive character in $b \in \mathcal{O}_K$ and hence there exists $u \in K^\times$ such that

$$\phi^{-1}(1 + \alpha\varpi_K^{n-1} b) = \psi_K(ub), \quad \forall b \in \mathcal{O}_K.$$

Moreover, $\mathrm{val}_K u = 0$, so that $u \in \mathcal{O}_K^\times$. Thus there exists $\alpha \in H$ depending on ϕ, ψ_K, and our choice of ϖ_K such that $H = K(\alpha)$, $\alpha^2 \in \mathcal{O}_K$, $\mathrm{val}_H \alpha = 1$, and

$$\phi^{-1}(1 + \alpha\varpi_K^{n-1} b) = \psi_K(b), \quad \forall b \in \mathcal{O}_K. \tag{4.8}$$

In particular, it follows from our choices of ψ_K and ϖ_K that α in (4.8) depends on E and does not depend on τ. Taking into account that $\mathrm{val}_H\left(\alpha\varpi_K^{n-1} b\right) \geq n$ for any $b \in \mathcal{O}_K$, by the definition of y we have

$$\psi_H(b) = \phi(1 + \alpha\varpi_K^{n-1} b) = \psi_H(y\alpha\varpi_K^{n-1} b),$$

which implies $y\alpha\varpi_K^{n-1} \equiv 1 \bmod \mathfrak{p}_H$ (since $n(\psi_H) = -1$). Thus $\theta(y) = \theta(\alpha)^{-1}$. This together with (4.5) and (4.7) yields

$$W(\lambda, \psi_L) = \phi(\alpha)^{[F:K]} \cdot \theta(\alpha)^{[F:K] - e_t f}. \tag{4.9}$$

Proof of Theorem 3.2. Note first that $\langle \tau, 1 \rangle = 1$, $\langle \tau, \chi \rangle = 0$, and it follows from (2.3) that $\langle \tau, \hat{\sigma} \rangle = 0$, since λ is wildly ramified.

It follows from (1.3), (4.2), and (4.9) that

$$W(E, \tau) = -\eta^f \chi_{L/F}(e_t) \phi(\alpha)^{[F:K]} \theta(\alpha)^{[F:K] - e_t f} \det \tau(-1). \tag{4.10}$$

Let $\alpha = u\varpi_H$ for some $u \in \mathcal{O}_H^\times$. Note that $\theta(\varpi_H) = \gamma$, $\theta|_{\mathcal{O}_H^\times}$ has order 2, and $[F:K] - e_t f$ is even, so that

$$\theta(\alpha)^{[F:K] - e_t f} = \gamma^{[F:K] - e_t f}. \tag{4.11}$$

Assume $f(K/\mathbb{Q}_3)$ is odd and $f(F/K)$ is even or $f(K/\mathbb{Q}_3)$ is even. Then $\chi_{L/F}(e_t) = 1$. Also, using Lemmas 1.2 and 1.3, it is easy to check that $\gamma^{[F:K] - e_t f} = 1$ and $\eta^f = \eta^{\dim \tau}$, so that (3.7) and (3.8) follow from (4.10) together with (4.11).

Assume $f(F/\mathbb{Q}_3)$ is odd, so that both $f(F/K)$ and $f(K/\mathbb{Q}_3)$ are odd. Then $\eta^2 = -1$ and we choose $\gamma = \eta$, which gives

$$\eta^{f+[F:K]-e_t f} = (-1)^{\frac{e_t-1}{2}} \eta^{\dim \tau}.$$

Calculating $(-1)^{\frac{e_t-1}{2}}$ and $\chi_{L/F}(e_t) = \left(\frac{e_t}{3}\right)$ explicitly, we get (3.8).

Appendix A. Representation theoretic facts

The goal of the appendix is to study symplectic representations of semidirect products G of the form $G = (A \rtimes B) \rtimes C$, where A, B are finite cyclic groups of coprime orders and C is an infinite cyclic group. The appendix is organized as follows: in Lemma A.1 we show that without loss of generality we can assume that C is finite. In Section A.1 we consider the case when A is a finite abelian group and C is finite with all the other assumptions on G remaining the same. Here we use Theorem A.2 describing representations of a finite group G via representations of a fixed normal subgroup. Finally, in Section A.2 we specialize to the case when A is cyclic (Proposition A.7).

Lemma A.1. *Let $C = \langle c \rangle$ be an infinite cyclic group generated by an element c and let E be a finite group. Let $G = E \rtimes C$ be a semi-direct product, where C acts on E via a homomorphism $\alpha : C \longrightarrow \mathrm{Aut}(E)$, and let $\mathrm{Ker}\,\alpha = \langle c^l \rangle$ for some $l \in \mathbb{N}$. Then every irreducible representation λ of G has the following form:*

$$\lambda = \lambda_0 \otimes \phi,$$

where λ_0 is an irreducible representation of G trivial on $\langle c^l \rangle$ and ϕ is a one-dimensional representation of G. In particular, every symplectic irreducible representation of G has finite image.

Proof. Since c^l is contained in the center of G and λ is an irreducible complex representation, by Schur's lemma $\lambda(c^l)$ acts as a scalar $a \in \mathbb{C}^\times$. Define a one-dimensional representation ϕ of G as follows: ϕ is trivial on E and $\phi(c)$ equals an l-th root of a. Then $\lambda_0 = \lambda \otimes \phi^{-1}$ is trivial on $\langle c^l \rangle$ and $\lambda = \lambda_0 \otimes \phi$.

Assume now that λ is symplectic. Then λ and its contragredient representation have the same character, which implies that for any $g \in G$ we have

$$\phi(g) \cdot \mathrm{tr}\,\lambda_0(g) = \phi(g)^{-1} \cdot \mathrm{tr}\,\lambda_0(g^{-1}).$$

Taking into account that λ_0 is trivial on $\langle c^l \rangle$, the above equation for $g = c^l$ gives $\phi(c^{2l}) = 1$, i.e., λ can be considered as an irreducible symplectic representation of the finite group $H = G/\langle c^{2l} \rangle \cong E \rtimes C/\langle c^{2l} \rangle$. □

A.1. **The case of an abelian A.** Let G be a finite group and let $N \subseteq G$ be a normal subgroup. The group G acts on the set $\hat{N}$ of isomorphism classes of complex irreducible representations σ of N in the following way: if $\sigma : N \longrightarrow \mathrm{GL}_m(\mathbb{C})$, then $g\sigma : N \longrightarrow \mathrm{GL}_m(\mathbb{C})$ is given by

$$g\sigma(n) = \sigma(g^{-1}ng), \; g \in G, \; n \in N.$$

For $\sigma \in \hat{N}$ we denote by G_σ the stabilizer of σ in G, i.e.,

$$G_\sigma = \{g \in G \mid g\sigma \cong \sigma\}\,.$$

Theorem A.2 (Mackey method of small subgroups (cf. [D00], p. 153, Thm. 6.2))**.** *Let $\sigma \in \hat{N}$ and let $\tau \in \hat{G}_\sigma$ be an irreducible component of $\operatorname{Ind}_N^{G_\sigma} \sigma$. Then $\operatorname{Ind}_{G_\sigma}^G \tau$ is an irreducible representation of G. Moreover, any irreducible representation of G can be obtained in this way. More precisely, let $\lambda \in \hat{G}$ and let $\sigma \in \hat{N}$ be an irreducible component of $\operatorname{Res}_N^G \lambda$. Then there exists an irreducible component $\tau \in \hat{G}_\sigma$ of $\operatorname{Ind}_N^{G_\sigma} \sigma$ such that $\lambda \cong \operatorname{Ind}_{G_\sigma}^G \tau$.*

Proof. Let us show first that $\operatorname{Ind}_{G_\sigma}^G \tau$ is irreducible or, equivalently, $\langle \operatorname{Ind}_{G_\sigma}^G \tau, \operatorname{Ind}_{G_\sigma}^G \tau\rangle = 1$, where $\langle \cdot\,, \cdot\rangle$ denotes the inner product of representations. Using the Frobenius reciprocity theorem we have $\langle \operatorname{Ind}_{G_\sigma}^G \tau, \operatorname{Ind}_{G_\sigma}^G \tau\rangle = \langle \tau, \operatorname{Res}_{G_\sigma}^G \left(\operatorname{Ind}_{G_\sigma}^G \tau\right)\rangle$ and we need to show that τ appears only once in the decomposition of $\mu = \operatorname{Res}_{G_\sigma}^G \left(\operatorname{Ind}_{G_\sigma}^G \tau\right)$ into irreducibles. Let W and V denote representation spaces of μ and τ, respectively, and assume that $W = V^n \oplus V'$, where $n \geq 2$ and V' is a $\mathbb{C}[G_\sigma]$-submodule of W.

Let $h_1, \ldots, h_s \in G$ denote a set of left coset representatives of G_σ in G with $h_1 = 1$. Then $W = h_1 V \oplus \cdots \oplus h_s V$ and

$$h_1 V \oplus \cdots \oplus h_s V = V^n \oplus V', \quad n \geq 2. \tag{A.1}$$

Let U be a representation space of σ and let $g_1, \ldots, g_t \in G_\sigma$ be a set of left coset representatives of N in G_σ. Then $\operatorname{Ind}_N^{G_\sigma} \sigma = g_1 U \oplus \cdots \oplus g_t U$. Note that each $g_i U$ is an N-module and it follows from the definition of G_σ that as N-modules all $g_i U$ are isomorphic to each other. Since τ is a subrepresentation of $\operatorname{Ind}_N^{G_\sigma} \sigma$, this implies $\operatorname{Res}_N^{G_\sigma} \tau \cong \sigma^r$ for some $r \geq 1$. Thus from (A.1) we get $h_1 U^r \oplus \cdots \oplus h_s U^r \cong U^{rn} \oplus V'$, where each $h_j U$ is an N-module and this is an isomorphism of N-modules. Since $n \geq 2$ and $h_1 = 1$, by the uniqueness of decomposition of a module into simple modules we conclude that there exists $h_k \neq 1$ such that $h_k U \cong U$ and hence $h_k \in G_\sigma$. This contradicts the assumptions that h_k is a representative of G_σ in G and $h_k \neq 1$.

Assume now that $\lambda \in \hat{G}$ and $\sigma \in \hat{N}$ is an irreducible component of $\operatorname{Res}_N^G \lambda$. Then by the Frobenious reciprocity theorem $\langle \operatorname{Res}_{G_\sigma}^G \lambda, \operatorname{Ind}_N^{G_\sigma} \sigma\rangle = \langle \operatorname{Res}_N^G \lambda, \sigma\rangle \neq 0$ and hence $\operatorname{Res}_{G_\sigma}^G \lambda$ and $\operatorname{Ind}_N^{G_\sigma} \sigma$ have a common irreducible component $\tau \in \hat{G}_\sigma$. By the previous paragraph $\operatorname{Ind}_{G_\sigma}^G \tau$ is irreducible and $\langle \operatorname{Ind}_{G_\sigma}^G \tau, \lambda\rangle = \langle \tau, \operatorname{Res}_{G_\sigma}^G \lambda\rangle \neq 0$. Since λ is irreducible, this implies $\lambda \cong \operatorname{Ind}_{G_\sigma}^G \tau$. $\square$

Lemma A.3. *Let A be a finite abelian group of order e, let $B = \langle b\rangle$ be a finite cyclic group of order k prime to e, and let $C = \langle c\rangle$ be a finite cyclic group. Let $E = A \rtimes B$ be a semi-direct product with B acting on A and let $G = E \rtimes C$ be a semi-direct product, where C acts on E. Let ψ_1 be a (one-dimensional) representation of A, let $\Gamma = A \rtimes \langle b^x\rangle$ denote the stabilizer of ψ_1 in E, and let ψ_2 be a (one-dimensional) representation of $\langle b^x\rangle$. Then both ψ_1 and ψ_2 can be extended to representations of Γ and denote $\phi = \psi_1 \otimes \psi_2 \in \hat{\Gamma}$.*

Let $E \rtimes \langle c^s\rangle$ be the stabilizer of $\operatorname{Ind}_\Gamma^E \phi$ in G. Then there exist i and a one-dimensional representation μ of $F = \langle A, b^x, c^s b^i\rangle$ such that

- $c^s b^i \phi = \phi$,
- $\operatorname{Res}_\Gamma^F \mu = \phi$,
- $\sigma = \operatorname{Ind}_F^G \mu$ *is irreducible, and*
- $|\overline{c^s b^i}| = |c^s|$, *where $\overline{c^s b^i}$ denotes the image of $c^s b^i$ in F/Γ or, equivalently,*
$$[E \rtimes \langle c^s\rangle : F] = x.$$

Moreover, every irreducible representation σ of G can be obtained in this way.

Proof. Note that since k is prime to e, A is normal in G. Let λ be an irreducible representation of $E = A \rtimes B$. Using Theorem A.2, λ can be constructed from one-dimensional representation ψ_1 of A in the following way. Let Γ denote the stabilizer of ψ_1 in E. Then $\Gamma = A \rtimes \langle b^x\rangle$ for some x and let ψ_2 be a one-dimensional representation of $\langle b^x\rangle$. Then ψ_1 and ψ_2 can be extended to representations of Γ via
$$\begin{aligned} \psi_1(b^{xv}a) &= \psi_1(a), \quad a \in A, \\ \psi_2(b^{xv}a) &= \psi_2(b^{xv}), \end{aligned}$$
and $\lambda = \operatorname{Ind}_\Gamma^E(\psi_1 \otimes \psi_2)$ ([S77], p. 62, Prop. 25). Let $\phi = \psi_1 \otimes \psi_2$ and let G_λ denote the stabilizer of λ in G. Then $G_\lambda = E \rtimes \langle c^s\rangle$ for some s, i.e., $c^s\lambda \cong \lambda$ or, equivalently, $\langle c^s\lambda, \lambda\rangle = 1$. Note that Γ is normal in G and $\{1, b, \dots, b^{x-1}\}$ is a system of representatives for the left cosets of Γ in E. Hence
$$\operatorname{Res}_\Gamma^E(c^s\lambda) \cong c^s\phi \oplus c^s b\phi \oplus \cdots \oplus c^s b^{x-1}\phi$$
and by the Frobenius reciprocity theorem we have
$$1 = \langle c^s\lambda, \lambda\rangle = \langle \operatorname{Res}_\Gamma^E(c^s\lambda), \phi\rangle = \sum_{i=0}^{x-1} \langle c^s b^i\phi, \phi\rangle.$$
This implies that there exists i such that $c^s b^i$ is in the stabilizer of ϕ in G_λ. Denote by F the stabilizer of ϕ in G_λ. Thus $\langle A, b^x, c^s b^i\rangle \subseteq F$ and it is easy to check that the reverse inclusion also holds. Consequently, $F = \langle A, b^x, c^s b^i\rangle$ and as a result F/Γ is cyclic. We will make use of the following lemma:

Lemma A.4 ([I94], p. 97, Exc. (6.17))**.** *Let N be a normal subgroup of a finite group G such that G/N is cyclic. If $\sigma \in \hat{N}$ and $G_\sigma = G$, then σ can be extended to an irreducible representation of G.*

By Lemma A.4 there exists a one-dimensional representation μ of F such that $\operatorname{Res}_\Gamma^F \mu = \phi$ and μ is an irreducible component of $\operatorname{Ind}_\Gamma^F \phi$. First, applying Theorem A.2 to G_λ with a normal subgroup Γ, $\phi \in \hat{\Gamma}$, and an irreducible component μ of $\operatorname{Ind}_\Gamma^F \phi$, we conclude that $\operatorname{Ind}_F^{G_\lambda} \mu$ is irreducible. Second, applying Theorem A.2 to G with a normal subgroup E, $\lambda \in \hat{E}$, and an irreducible component $\operatorname{Ind}_F^{G_\lambda} \mu$ of $\operatorname{Ind}_E^{G_\lambda} \lambda$, we conclude that $\operatorname{Ind}_F^G \mu = \operatorname{Ind}_{G_\lambda}^G \operatorname{Ind}_F^{G_\lambda} \mu$ is also irreducible.

Conversely, let $\sigma \in \hat{G}$ and let λ be an irreducible component of $\operatorname{Res}^G_E \sigma$. Then in the notation of the proof used above, $\lambda = \operatorname{Ind}^E_\Gamma \phi$ and it is enough to show that there exists an extension μ of ϕ to F such that $\sigma \cong \operatorname{Ind}^G_F \mu$. Note that by Lemma A.4 there exists $\tilde{\lambda} \in \hat{G}_\lambda$ that extends λ and hence every irreducible component of $\operatorname{Ind}^{G_\lambda}_E \lambda$ has the form $\tilde{\lambda} \otimes \psi$, where ψ is a one-dimensional representation of $\langle c^s \rangle$ considered as a representation of G_λ via inflection. By Theorem A.2, without loss of generality we can assume that $\sigma \cong \operatorname{Ind}^G_{G_\lambda} \tilde{\lambda}$. Now we will use Theorem A.2 applied to G_λ with the normal subgroup Γ and $\tilde{\lambda}$. Namely, note that every irreducible component of $\operatorname{Res}^{G_\lambda}_\Gamma \tilde{\lambda}$ has the form $b^j \phi$ and every irreducible component of $\operatorname{Ind}^F_\Gamma \phi$ has the form $\mu \otimes \kappa$, where κ is a one-dimensional representation of $\langle \overline{c^s b^i} \rangle$ considered as a representation of F via inflection. By Theorem A.2, without loss of generality we can assume that $\tilde{\lambda}$ is obtained from ϕ and μ via $\tilde{\lambda} \cong \operatorname{Ind}^{G_\lambda}_F \mu$ and hence $\sigma \cong \operatorname{Ind}^G_F \mu$. Moreover, it follows that $x = \dim \tilde{\lambda} = [G_\lambda : F]$, hence $[F : \Gamma] = [G_\lambda : E]$ and $|\overline{c^s b^i}| = |c^s|$. $\square$

Remark A.5. Note that if A is cyclic, then F is normal in G (see the subsection below). This is not true for a general abelian A. For example, let $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $B \cong \mathbb{Z}/3\mathbb{Z}$, and $C \cong \mathbb{Z}/2\mathbb{Z}$. Denote by a_1, a_2 generators of A with the group operation written multiplicatively and define

$$\begin{aligned} c^{-1}bc &= b^2, \\ b^{-1}a_1 b &= a_2, \quad b^{-1}a_2 b = a_1 a_2, \\ c^{-1}a_1 c &= a_1, \quad c^{-1}a_2 c = a_1 a_2, \\ \psi_1(a_1) &= 1, \quad\ \ \psi_1(a_2) = -1. \end{aligned}$$

It is easy to check that $G = (A \rtimes B) \rtimes C$ is well defined, $\Gamma = A$ and $c\psi_1 = \psi_1$. Thus $F = \langle A, c \rangle$ and F is not normal in G. Indeed, $bcb^{-1} = cb \notin F$.

A.2. **The case of a cyclic** A**.** In what follows we will write an action of a cyclic group $\langle b \rangle$ on a group A in the form $b^{-1}ab$, $a \in A$. Since B is cyclic, it is well defined, and it is more convenient for applications to representations. Thus we multiply elements in a semi-direct product $A \rtimes \langle b \rangle$ as follows

$$(a_1, b_1) \cdot (a_2, b_2) = (b_2^{-1} a_1 b_2 \cdot a_2, b_1 b_2), \quad a_1, a_2 \in A,\ b_1, b_2 \in \langle b \rangle.$$

Lemma A.6. *Let $E = A \rtimes B$, $A = \langle a \rangle$, $B = \langle b \rangle$, $|a| = e$, $|b| = k$, $(e,k) = 1$, and $b^{-1}ab = a^m$, where $m \in (\mathbb{Z}/e\mathbb{Z})^\times$ and $m^k \equiv 1 \bmod e$. Then any automorphism θ of E is defined by a triple (r,t,n) via*

$$\theta(a) = a^n, \quad \theta(b) = b^r a^t,$$

where $n \in (\mathbb{Z}/e\mathbb{Z})^\times$, $r \in (\mathbb{Z}/k\mathbb{Z})^\times$, $t \in \mathbb{Z}/e\mathbb{Z}$, $m^r \equiv m \bmod e$, and

$$t \cdot (1 + m + m^2 + \cdots + m^{k-1}) \equiv 0 \bmod e. \tag{A.2}$$

Moreover, if $\theta_1 = (r_1, t_1, n_1)$ and $\theta_2 = (r_2, t_2, n_2)$, then $\theta_1 \circ \theta_2 = (r_1 r_2, t_1 + t_2 n_1, n_1 n_2)$. Furthermore, $\theta^{-1} = (r', -n't, n')$ with $n' \equiv n^{-1} \bmod e$, $r' \equiv r^{-1} \bmod k$, and $\theta^s = (r^s, \alpha_s, n^s)$

with

$$\alpha_s = t\sum_{j=0}^{s-1} n^j. \tag{A.3}$$

Proof. Indeed, note that

$$1 = \theta(b)^k = (b^r a^t)^k = a^{tu},$$

where $u = 1 + m^r + m^{2r} + \cdots + m^{(k-1)r} \equiv 1 + m + m^2 + \cdots + m^{k-1} \; mod \; e$, which implies (A.2). Let y denote the order of m in $(\mathbb{Z}/e\mathbb{Z})^\times$. Then y divides both k and $r-1$, and from (A.2) we get

$$t\cdot(1+m+m^2+\cdots+m^{k-1}) \equiv t\cdot(1+m+m^2+\cdots+m^{y-1})\frac{k}{y} \equiv 0 \; mod \; e. \tag{A.4}$$

Since $(e,k)=1$, we conclude that $t\cdot(1+m+m^2+\cdots+m^{y-1}) \equiv 0 \; mod \; e$ and hence $t\cdot(1+m+m^2+\cdots+m^{r-1}) \equiv t \; mod \; e$ for any r satisfying $m^r \equiv m \; mod \; e$. To get formulas for $\theta_1 \circ \theta_2$ and θ^{-1} note that

$$\theta_1 \circ \theta_2(b) = b^{r_1 r_2} a^{u + t_2 n_1}, \tag{A.5}$$

where $u = t_1(1 + m^{r_1} + m^{2r_1} + \cdots + m^{(r_2-1)r_1}) \equiv t_1(1+m+m^2+\cdots+m^{r_2-1}) \equiv t_1 \; mod \; e$. Using (A.5), formula (A.3) can be easily proved by induction. $\square$

Proposition A.7. *Let $A = \langle a\rangle$ be a finite cyclic group of order e, let $B = \langle b\rangle$ be a finite cyclic group of order k prime to e, and let $C = \langle c\rangle$ be a finite cyclic group. Let $E = A \rtimes B$ be a semi-direct product with B acting on A via $b^{-1}ab = a^m$ for some $m \in (\mathbb{Z}/e\mathbb{Z})^\times$ and let $G = E \rtimes C$ be a semi-direct product, where C acts on E via $c^{-1}ac = a^n$, $n \in (\mathbb{Z}/e\mathbb{Z})^\times$, $c^{-1}bc = b^r a^t$, $r \in (\mathbb{Z}/k\mathbb{Z})^\times$, $t \in \mathbb{Z}/e\mathbb{Z}$. Let ψ_1 be a (one-dimensional) representation of A, let $\Gamma = A \rtimes \langle b^x\rangle$ denote the stabilizer of ψ_1 in E, and let ψ_2 be a (one-dimensional) representation of $\langle b^x\rangle$. Then both ψ_1 and ψ_2 can be extended to representations of Γ and denote $\phi = \psi_1 \otimes \psi_2 \in \hat{\Gamma}$. Let $E \rtimes \langle c^s\rangle$ be the stabilizer of $\mathrm{Ind}_\Gamma^E \phi$ in G. Then there exist a unique $i \in \{0,1,\ldots,x-1\}$ and a one-dimensional representation μ of $F = \langle A, b^x, c^s b^i\rangle$ such that*

- $c^s b^i \phi = \phi$,
- $\mathrm{Res}_\Gamma^F \mu = \phi$, *and*
- $\sigma = \mathrm{Ind}_F^G \mu$ *is irreducible.*

If, in addition, σ is symplectic, then there exist $g \in \{0,1,\ldots,s-1\}$ and $j \in \{0,1,\ldots,x-1\}$ such that $\overline{\mu} = \mu_{c^g b^j}$, $(c^g b^j)^2 \in F$, and $\mu((c^g b^j)^2) = -1$. Moreover, every irreducible symplectic representation σ of G can be obtained in this way.

Proof. We assume the results of Lemma A.3 and Lemma A.6. Note that $m^k \equiv 1 \; mod \; e$ and $m^r \equiv m \; mod \; e$. Then $\psi_1(a)$ is an e-th root of unity of order d in $\mathbb{C}^\times$ and $x = |m|$ in $(\mathbb{Z}/d\mathbb{Z})^\times$. Since d divides e, from $m^r \equiv m \; mod \; e$ we have $r \equiv 1 \; mod \; x$. This implies that the group $F = \langle A, b^x, c^s b^i\rangle$ is normal. Indeed, since A is normal in G, it is enough to show that F/A is normal in G/A. Denoting the images of a, b, and c in G/A again by a, b, and c, respectively, we have

$$\begin{aligned} c^{-1} \cdot b^x \cdot c &= b^{rx}, \\ b \cdot c^s b^i \cdot b^{-1} &= c^s b^i \cdot b^{r^s - 1}, \\ c^{-1} \cdot c^s b^i \cdot c &= c^s b^i \cdot b^{i(r-1)}. \end{aligned}$$

Thus by Lemma A.3 every irreducible representation of G is induced by a one-dimensional representation from a normal subgroup. Proposition A.7 then follows from Lemma A.8 below, which characterizes symplectic irreducible representations of a finite group induced by one-dimensional representations from normal subgroups. □

Lemma A.8. *Let G be a finite group with a normal subgroup F and let $\sigma = \operatorname{Ind}_F^G \mu$ be an irreducible representation of G induced by a one-dimensional representation μ of F. For $g \in G$ let μ_g denote the one-dimensional representation of F given by*

$$\mu_g(f) = \mu(g^{-1} f g), \quad f \in F.$$

Let $\overline{\mu}$ denote the contragredient representation of μ. Then σ is symplectic if and only if there exists $t \in G$ such that $\overline{\mu} = \mu_t$, $t^2 \in F$, and $\mu(t^2) = -1$.

Proof. Let χ denote the character of σ. By Proposition 39 on p. 109 in [S77], σ is symplectic if and only if

$$\frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = -1. \tag{A.6}$$

Let T denote a system of representatives of F in G. Note that $\operatorname{Res}_F^G \sigma = \bigoplus_{t \in T} \mu_t$ and $\chi(g) = 0$ if $g \notin F$. Thus

$$\sum_{y \in G} \chi(y^2) = \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{f \in F} \chi(t^2 \cdot t^{-1} f t \cdot f) = \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{f \in F} \sum_{t' \in T} \mu_{t'}(t^2) \mu_{t'}(t^{-1} f t) \mu_{t'}(f),$$

where $\sum_{f \in F} \mu_{t'}(t^{-1} f t) \mu_{t'}(f) = |F| \cdot \langle \mu_{(t')^{-1} t t'}, \overline{\mu} \rangle$. Hence

$$\frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = \frac{|F|}{|G|} \cdot \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{t' \in T} \mu_{t'}(t^2) \langle \mu_{(t')^{-1} t t'}, \overline{\mu} \rangle. \tag{A.7}$$

This implies that if σ is symplectic, then there exists $t_0 \in G$ such that ${t_0}^2 \in F$ and $\overline{\mu} = \mu_{t_0}$. Since σ is irreducible, all μ_t's are pairwise distinct and hence from (A.6) and (A.7) we get

$$-1 = \frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = \frac{|F|}{|G|} \cdot \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{t' \in T} \mu_{t'}(t^2) \langle \mu_{(t')^{-1} t t'}, \overline{\mu} \rangle = \mu({t_0}^2),$$

which implies that the conditions in Lemma A.8 are necessary and it follows from the proof that they are also sufficient. □

Remark A.9. By Proposition 39 on p. 109 in [S77], σ is orthogonal if and only if

$$\frac{1}{|G|}\cdot\sum_{y\in G}\chi(y^2)=1.$$

Thus it follows from the proof of Lemma A.8 that σ is orthogonal if and only if there exists $t\in G$ such that $\overline{\mu}=\mu_t$, $t^2\in F$, and $\mu(t^2)=1$. In particular, if σ is orthogonal, then either μ is real-valued or the order of G/F is even.

Appendix B

Lemma B.1. *Let H be a ramified quadratic extension of K and let ϕ be a character of $H^\times$ such that $\phi|_{K^\times}=\chi_{H/K}$. Then either $a(\phi)=1$ or $a(\phi)$ is positive and even.*

Proof. Since $a(\phi)\neq 0$, assume $a(\phi)=2m+1$ for some $m\neq 0$. Since H is ramified over K, $\mathcal{O}_H=\mathcal{O}_K[\varpi_H]$ for a uniformizer ϖ_H of H such that $\varpi_H^2\in\mathcal{O}_K$. Let $y=1+x\varpi_H^{2m}$, $x\in\mathcal{O}_H$. Then $x=a+b\varpi_H$ for $a,b\in\mathcal{O}_K$, $y=1+a\varpi_H^{2m}+b\varpi_H^{2m+1}$, and $\phi(y)=\chi_{H/K}(1+a\varpi_H^{2m})=1$, since $a(\chi_{H/K})=1$. Thus ϕ is trivial on $1+\mathfrak{p}_H^{2m}$ which contradicts $a(\phi)=2m+1$. $\square$

Lemma B.2. *Let H be a local non-archimedean field of zero characteristic and let L be a tamely ramified Galois extension of H. Let ϕ be a character of $H^\times$, $\lambda=\operatorname{Res}_H^L\phi$, and $e_t=e(L/H)$. If $a(\phi)>1$, then*

$$a(\lambda)=(a(\phi)-1)e_t+1. \tag{B.1}$$

Proof. Let N be a finite Galois extension of H such that $\mathrm{Gal}(\overline{K}/N^{unr})$ is contained in the kernel of ϕ. Since $a(\phi)>1$, $a(\phi^k)=a(\phi)$ for any k not divisible by p. Thus without loss of generality we can assume that $A=\mathrm{Gal}(N^{unr}/H^{unr})$ is a p-group and hence $N^{unr}\cap L^{unr}=H^{unr}$. Let $T=L^{unr}N^{unr}$, $B=\mathrm{Gal}(T/H^{unr})$, $C=\mathrm{Gal}(T/L^{unr})$, where $C\cong A$. Then $a(\phi)=1+\frac{1}{e_t}\alpha$, where α depends on whether ϕ is trivial on the higher ramification groups B_i's of B, $i\geq 1$. On the other hand, $a(\lambda)=1+\beta$, where β depends on whether ϕ is trivial on the higher ramification groups C_i's of C, $i\geq 1$. Since $C_i=C\cap B_i=B_i$, we have $\alpha=\beta$ and hence (B.1). $\square$

Lemma B.3. *Let $e_t=e(F_t/K)$, $f=f(F/K)$, and let z, y be given by (4.4), (4.6), respectively. Then*

$$\tilde{\theta}(z)=\theta(y)^{e_tf}.$$

Proof. We consider three cases: 1) F is tamely ramified over K (equivalently, L is tamely ramified over H), 2) F is a totally ramified Galois extension of K of degree 3 (hence, L is a totally ramified Galois extension of H of degree 3), and 3) the general case.

L **is tamely ramified over** H**.** Note that in this case we have $L=L_t$ and hence $\psi_L=\psi_H\circ\mathrm{Tr}_{L/H}$ on $\mathcal{O}_L$. Since by assumption $a(\phi)$ is not tame, by Lemma B.2 we have $\kappa=(m-1)e_t+1$. This implies

$$\mathrm{val}_L\,y=\mathrm{val}_L\,z=(1-m)e_t.$$

For any $b \in L$ with $\mathrm{val}_L(b) \geq (m-1)e_t$ using (4.4) we have

$$\psi_L(zb) = \lambda(1+b) = \phi(\mathrm{N}_{L/H}(1+b)) = \phi(1 + \mathrm{Tr}_{L/H}(b) + b'), \quad b' \in H, \tag{B.2}$$

where $\mathrm{val}_L(\mathrm{Tr}_{L/H}(b)) \geq me_t/2$ and $\mathrm{val}_L(b') \geq me_t$. Thus

$$\mathrm{val}_H(\mathrm{Tr}_{L/H}(b)) \geq m/2, \quad \mathrm{val}_H(b') \geq a(\phi), \text{ and } yb \in \mathcal{O}_L,$$

hence by (4.6)

$$\phi(1 + \mathrm{Tr}_{L/H}(b) + b') = \psi_H(y \,\mathrm{Tr}_{L/H}(b)) = \psi_H(\mathrm{Tr}_{L/H}(yb)) = \psi_L(yb). \tag{B.3}$$

Therefore, comparing (B.2) and (B.3) we get $\psi_L(zb) = \psi_L(yb)$ or, equivalently,

$$\psi_L((z-y)b) = 1.$$

Since the last equation holds for all $b \in \mathfrak{p}_L^{(m-1)e_t}$, we conclude that

$$\mathrm{val}_L((z-y)\varpi_L^{(m-1)e_t}) \geq 1. \tag{B.4}$$

Let $y = u\varpi_L^{\mathrm{val}\, y}$, $z = v\varpi_L^{\mathrm{val}\, y}$ for $u, v \in \mathcal{O}_L^\times$. Then (B.4) implies $u \equiv v \mod \mathfrak{p}_L$ and hence

$$\tilde{\theta}(z) = \tilde{\theta}(\varpi_L)^{\mathrm{val}_L y} \cdot \tilde{\theta}(u) = \tilde{\theta}(y) = \theta(y)^{[L:H]}. \tag{B.5}$$

L is a totally ramified Galois extension of H of degree 3. Let $T = LN$. We first study the relation between $a(\phi)$ and $a(\lambda)$. In particular, we will show that $a(\lambda) \geq a(\phi)$. For that we analyze the higher ramification groups of $\mathrm{Gal}(T^{unr}/H^{unr})$. Denote

$$\begin{aligned} P &= \mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\ Q &= \mathrm{Gal}(L^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}, \\ G &= \mathrm{Gal}(T^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \\ C &= \mathrm{Gal}(T^{unr}/L^{unr}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

(here we used Lemma 1.1). The higher ramification groups of P are

$$P = P_0 \supset P_1 = \cdots = P_n \supset P_{n+1} = \{1\},$$

where $P_1 \cong \mathbb{Z}/3\mathbb{Z}$, n is even (as follows from the results on the action of inertia groups on higher ramification groups), $m = 1 + n/2$, and since m is even, we have $n/2$ is odd. Let $R = \mathrm{Gal}(L^{unr}/K^{unr}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Then the higher ramification groups of R are

$$R = R_0 \supset R_1 = \cdots = R_\alpha \supset R_{\alpha+1} = \{1\},$$

where $R_1 \cong \mathbb{Z}/3\mathbb{Z}$ and α is even. Then the higher ramification groups Q_i of Q have the form $Q_i = Q \cap R_i$, so that

$$Q = Q_0 = \cdots = Q_\alpha \supset Q_{\alpha+1} = \{1\},$$

where α is even. Finally, the higher ramification groups of C are

$$C = C_0 \supset C_1 = \cdots = C_\delta \supset C_{\delta+1} = \{1\},$$

where $C_1 \cong \mathbb{Z}/3\mathbb{Z}$, δ is even, $\kappa = 1 + \delta/2$, and since κ is even, we have $\delta/2$ is odd. Since $L^{unr} \cap N^{unr} = H^{unr}$, the restriction maps give the isomorphism

$$\mu : G \xrightarrow{\cong} \mathrm{Gal}(N^{unr}/H^{unr}) \times \mathrm{Gal}(L^{unr}/H^{unr}),$$

so that $G \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$ is an abelian group of order 18. As a result, the higher ramification groups of G can have two forms:

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \{1\}, \tag{B.6}$$

where $G_1 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, t is even, or

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \cdots = G_{t+s} \supset G_{t+s+1} = \{1\}, \tag{B.7}$$

where $G_1 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$, t is even, and s is divisible by 6. We will show, in particular, that (B.6) does not occur.

Assume that (B.6) holds. By comparing the higher ramification groups of G with the higher ramification groups of its quotients Q and P, it is not hard to see that in this case we have $\alpha = t/2$, $n = t$, which is a contradiction, since by above α is even and $n/2$ is odd.

Assume that (B.7) holds. There are three sub-cases depending on the embedding of $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$ into $G_t \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $S \subseteq N$ be a quadratic extension of H such that S^{unr}/H^{unr} is the maximal tamely ramified subextension of N^{unr}/H^{unr}. Again, as in the previous paragraph, by comparing the higher ramification groups of G with the higher ramification groups of its subgroup C and quotients Q and P, it is not hard to see that

$$\begin{array}{llll} \alpha = \frac{t}{2} + \frac{s}{6}, & n = t, & \delta = t, & \text{if } \mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr}), \\ \alpha = \frac{t}{2}, & n = t + \frac{s}{3}, & \delta = t + s, & \text{if } \mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr}), \\ \alpha = \frac{t}{2} + \frac{s}{6}, & n = t + \frac{s}{3}, & \delta = t, & \qquad\text{otherwise.} \end{array} \tag{B.8}$$

Thus, in the third sub-case in (B.8) we get $\alpha = n/2$, which is a contradiction, since by above α is even and $n/2$ is odd. Hence $\mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr})$ or $\mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr})$.

Remark B.4. It turns out that both first two cases in (B.8) can occur. Explicit examples of elliptic curves over $K = \mathbb{Q}_3$ can be found in [Ki03].

Note that since L is wildly ramified over H, by our choice $\psi_H = \psi_L$ on $\mathcal{O}_H$. Let $x \in L$ with $\mathrm{val}_L(x) \geq \kappa - 1$. Then

$$\psi_L(zx) = \lambda(1+x) = \phi\left(\mathrm{N}_{L/H}(1+x)\right). \tag{B.9}$$

By [S79] (p. 83, Lem. 4 and 5), we have

$$\begin{array}{rcll} \mathrm{N}_{L/H}(1+x) & \equiv & 1 + \mathrm{Tr}_{L/H}(x) + \mathrm{N}_{L/H}(x) \mod \mathfrak{p}_H^{l_1}, & l_1 = \left[\frac{2}{3}(\kappa+\alpha)\right], \\ \mathrm{Tr}_{L/H}(x) & \equiv & 0 \mod \mathfrak{p}_H^{l_2}, & l_2 = \left[\frac{\kappa + 2\alpha + 1}{3}\right]. \end{array} \tag{B.10}$$

(Here, for $r \in \mathbb{R}$ the symbol $[r]$ denotes the largest integer $\leq r$.) In both cases when $\mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr})$ or $\mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr})$, using formulas (B.8) and $a(\lambda) = \kappa = 1 + \delta/2$, $a(\phi) = m = 1 + n/2$, it is easy to check that $l_1 \geq m$. Let

$$x = a\varpi_L^{\kappa-1},\ z = w\varpi_L^{1-\kappa},\ y = u\varpi_L^{3(1-m)}, \quad a \in \mathcal{O}_L,\ w, u \in \mathcal{O}_L^\times.$$

Assume that $\mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr})$. In this case we have $\kappa = m$, $l_2 \geq m$, and $\mathrm{val}_H \mathrm{N}_{L/H}(x) \geq \kappa - 1 = m - 1 \geq m/2$. Thus using (B.9) and (B.10) we get

$$\psi_L(zx) = \phi\left(1 + \mathrm{N}_{L/H}(x)\right) = \psi_L(y\,\mathrm{N}_{L/H}(x)). \tag{B.11}$$

Note that the group $\mathrm{Gal}(L/H)$ coincides with its α-th ramification subgroup, where $\alpha \geq 1$, so that $g(\varpi_L)\varpi_L^{-1} \equiv 1 \bmod \mathfrak{p}_L$ for any $g \in \mathrm{Gal}(L/H)$. Then easy calculation shows that

$$y\,\mathrm{N}_{L/H}(x) = y\,\mathrm{N}_{L/H}(a)\,\mathrm{N}_{L/H}(\varpi_L)^{\kappa-1} \equiv ua^3 \bmod \mathfrak{p}_L.$$

Thus, (B.11) implies $aw - ua^3 \in \ker\psi_L$. Let $f = f(L/\mathbb{Q}_3)$. We have $u^{3^f} \equiv u \bmod \mathfrak{p}_L$ and

$$ua^3 \equiv u^{3^f}a^3 - u^{3^{f-1}}a + u^{3^{f-1}}a \equiv u^{3^{f-1}}a \bmod \ker\psi_L,$$

since it follows from the definition of ψ_L that $u^{3^f}a^3 - u^{3^{f-1}}a \in \ker\psi_L$. This implies $a\cdot(w - u^{3^{f-1}}) \in \ker\psi_L$ for all $a \in \mathcal{O}_L$ and hence $w \equiv u^{3^{f-1}} \bmod \mathfrak{p}_L$ (because $n(\psi_L) = -1$). Since the restriction of $\tilde\theta$ to $\mathcal{O}_L^\times$ has order 2, we have

$$\tilde\theta(y) = \tilde\theta(u)\tilde\theta(\varpi_L)^{3(1-\kappa)} = \tilde\theta(w)\tilde\theta(\varpi_L)^{3(1-\kappa)} = \tilde\theta(w)^3\tilde\theta(\varpi_L)^{3(1-\kappa)} = \tilde\theta(z)^3.$$

On the other hand, $\tilde\theta(y) = \theta(y)^3$, since $y \in H^\times$. Finally, recall that $\theta(\beta)^4 = 1$ for any $\beta \in \mathcal{W}(\overline{K}/H)$, hence

$$\tilde\theta(z) = \theta(y). \tag{B.12}$$

Assume now that $\mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr})$. In this case $l_2 = m - 1 \geq m/2$ and $\mathrm{val}_H \mathrm{N}_{L/H}(x) \geq \kappa - 1 \geq m$. Hence, using (B.9) and (B.10) we get

$$\psi_L(zx) = \phi\left(1 + \mathrm{Tr}_{L/H}(x)\right) = \psi_L(y\,\mathrm{Tr}_{L/H}(x)). \tag{B.13}$$

Note that without loss of generality we can assume $w \in \mathcal{O}_H^\times$. Indeed, since L is totally ramified over H, there exists $w_0 \in \mathcal{O}_H^\times$ such that $w - w_0 \in \mathfrak{p}_L$. Then $\psi_L(zx) = \psi_L(w_0\varpi_L^{1-\kappa}x)$ (because $n(\psi_L) = -1$) and $\tilde\theta(z) = \tilde\theta(w_0\varpi_L^{1-\kappa})$ (because $a(\tilde\theta) = 1$). For any $a \in \mathcal{O}_H$ the equation (B.13) yields

$$a\cdot(w - y\,\mathrm{Tr}_{L/H}(\varpi_L^{\kappa-1})) \in \mathcal{O}_H \cap \ker\psi_L$$

and hence $w \equiv y\,\mathrm{Tr}_{L/H}(\varpi_L^{\kappa-1}) \bmod \mathfrak{p}_H$. Our next step is to calculate $y\,\mathrm{Tr}_{L/H}(\varpi_L^{\kappa-1})$. Denote $\varpi_L = \varpi$, $\kappa - 1 = j$, and let g be a generator of $\mathrm{Gal}(L/H)$, so that

$$\mathrm{Tr}_{L/H}(\varpi^j) = \varpi^j + g(\varpi)^j + g^2(\varpi)^j.$$

Note that $\mathrm{val}_L(y) + j + 2\alpha = 0$. We have $g(\varpi) = \varpi(1 + c\varpi^\alpha)$ for some $c \in \mathcal{O}_L^\times$ and $g(c) \equiv c \bmod \mathfrak{p}_L^{\alpha+1}$. Using this, it is easy to check that

$$\begin{aligned} \mathrm{Tr}_{L/H}(\varpi^j) &= \varpi^j + \varpi^j(1 + c\varpi^\alpha)^j + g(\varpi)^j(1 + g(c)g(\varpi)^\alpha)^j \equiv \\ &\equiv \varpi^j(3 + 3cj\varpi^\alpha + c^2 j(\alpha + j)\varpi^{2\alpha}) \bmod \mathfrak{p}_L^{j+2\alpha+1}. \end{aligned} \tag{B.14}$$

Let $b = e(H/\mathbb{Q}_3)$. Then $e(N/\mathbb{Q}_3) = 6b$ and $e(L/\mathbb{Q}_3) = 3b$. It is known (see e.g., [S79], p. 72, Exc. 3c) that

$$n \leq \frac{1}{2}e(N/\mathbb{Q}_3) \quad \text{and} \quad \alpha \leq \frac{1}{2}e(L/\mathbb{Q}_3),$$

which implies $t + \frac{s}{3} \leq 3b$ and since $s \neq 0$, we conclude that $2\alpha = t < 3b$. In other words, $\mathrm{val}_L 3 > 2\alpha$ and it follows from (B.14) that

$$y\,\mathrm{Tr}_{L/H}(\varpi^j) \equiv uc^2 j(\alpha + j) \bmod \mathfrak{p}_L.$$

Recall that in this case $j = \kappa - 1 = \frac{\delta}{2} = \frac{t}{2} + \frac{s}{2}$, $\alpha = \frac{t}{2}$ and since $s \equiv 0 \bmod 3$, we have

$$w \equiv y\,\mathrm{Tr}_{L/H}(\varpi^j) \equiv 2c^2t^2u \bmod \mathfrak{p}_L.$$

Since w is a unit, we see that t is not divisible by 3 and since the restriction of $\tilde{\theta}$ to $\mathcal{O}_L^\times$ has order 2, we have

$$\tilde{\theta}(z) = \tilde{\theta}(w)\tilde{\theta}(\varpi_L)^{1-\kappa} = \theta(2)\tilde{\theta}(u)\tilde{\theta}(\varpi_L)^{1-\kappa}.$$

Recall that $y = u\varpi_L^{3(1-m)}$. Also, $1 - \kappa - 3(1 - m) = t$, where $t = 2\alpha$ and α is even, so t is divisible by 4 and hence

$$\tilde{\theta}(\varpi_L)^{1-\kappa} = \tilde{\theta}(\varpi_L)^{3(1-m)}.$$

Thus,

$$\tilde{\theta}(z) = \theta(2)\tilde{\theta}(y) = \theta(2)\theta(y)^3.$$

Writing $y \in H^\times$ as the product of a unit in $\mathcal{O}_H^\times$ and $\varpi_H^{\mathrm{val}_H y}$ and taking into account that $\theta(2) = (-1)^{f(H/\mathbb{Q}_3)}$, $\theta(\varpi_H)^2 = (-1)^{f(H/\mathbb{Q}_3)}$, $\mathrm{val}_H y = 1 - m$ is odd, and the restriction of θ to $\mathcal{O}_H^\times$ has order two, we get $\theta(2)\theta(y)^2 = 1$. Therefore,

$$\tilde{\theta}(z) = \theta(y). \tag{B.15}$$

General case. We now assume that F is an arbitrary finite Galois extension of K. Let F_t be the maximal tamely ramified extension of K contained in F. Since the group $\mathrm{Gal}(F/F_t)$ is a p-group with $p = 3$, it has a quotient that is a cyclic group of order 3, hence, there exists a finite Galois extension F_1 of F_t contained in F with $\mathrm{Gal}(F_1/F_t) \cong \mathbb{Z}/3\mathbb{Z}$. We put $L_1 = F_1 H$, $L_t = L_0$ and for each $i \in \{0, 1\}$ denote $\phi_i = \mathrm{Res}_H^{L_i}\phi$, $\theta_i = \mathrm{Res}_H^{L_i}\theta$, $\psi_0 = \psi_H \circ \mathrm{Tr}_{L_t/H}$. Also, let ψ_1 be a character of L_1 such that $\psi_1 = \psi_L$ on $\mathcal{O}_{L_1}$ and let $z_i \in L_i^\times$ be the analogues of z for ϕ_i, i.e., we have

$$\phi_i(1 + a) = \psi_i(z_i a), \quad a \in L_i^\times,\ \mathrm{val}_{L_i}(a) \geq a(\phi_i)/2.$$

(Note that ψ_i is non-trivial and $a(\phi_i)$ is even by Lemma 1.1 and Lemma B.1 (see Appendix B below).) Using the inductive hypothesis on the order of $\mathrm{Gal}(L/L_t)$ together with (B.12) and (B.15), we get

$$\tilde{\theta}(z) = \theta_1(z_1) = \theta_0(z_0).$$

Finally, using (B.5) we have

$$\tilde{\theta}(z) = \theta_0(z_0) = \theta(y)^{[L_t:H]}.$$

□

Appendix C. An example of a non-Galois F/K.

We keep the notation of Section 1.

Lemma C.1. *Let H be unramified over K and let F be a degree 3 extension of K such that the Galois closure F^g of F over K is totally ramified over K. Denote $\tau = \mathrm{Ind}_K^F 1_F$. Then there exists $t \in \mathbb{N}$ such that*

$$W(E,\tau) = (-1)^A \phi(u_{H/K})^{\dim\tau} \det\tau(-1), \tag{C.1}$$

where $u_{H/K} \in \mathcal{O}_H^\times$, $u_{H/K}^2 \in \mathcal{O}_K$, $H = K(u_{H/K})$, and

$$A = \begin{cases} a(\phi), & \text{if } F/K \text{ is Galois},\\ a(\phi)+t, & \text{if } F/K \text{ is not Galois.}\end{cases} \tag{C.2}$$

Note that in the notation of Proposition 2.1

$$a(\phi) \equiv (a(\phi) - e(H/K))\dim\tau + \langle\tau,\chi\rangle + \langle\tau,1\rangle + \langle\tau,\hat{\sigma}\rangle \ mod\ 2,$$

so that (C.1) agrees with Proposition 2.1 when F is Galois over K. Furthermore, both cases t is even and t is odd can occur.

Proof. The case when F is Galois over K is done in Proposition 2.1. Suppose F is not Galois over K, so that $\mathrm{Gal}(F^g/K) \cong S_3$. By Proposition 4 and its proof on p. 320 in [R96] we have

$$W(E,\tau) = (-1)^{a(\sigma\otimes\tau)/2 - a(\tau)} \phi(u_{H/K})^{\dim\tau} \det\tau(-1). \tag{C.3}$$

Let S/K be the maximal tamely ramified subextension of F^g/K, i.e., $[S:K]=2$. Let $T = F^gM$, $\tilde{H} = SH$, $\tilde{L} = F^gH$, and $\tilde{M} = SM$. By Lemma 1.1 above, M is not contained in $\tilde{L}$ and hence we have the following diagrams of field extensions:

$$\begin{tikzcd}
F^g \arrow[r, dash, "2"] \arrow[d, dash, "3"'] & \tilde{L} \arrow[r, dash, "3"] \arrow[d, dash, "3"'] & T \arrow[d, dash, "3"'] \\
S \arrow[r, dash, "2"] \arrow[d, dash, "2"'] & \tilde{H} \arrow[r, dash, "3"] \arrow[d, dash, "2"'] & \tilde{M} \arrow[d, dash, "2"'] \\
K \arrow[r, dash, "2"] & H \arrow[r, dash, "3"] & M
\end{tikzcd}
\qquad
\begin{tikzcd}
(F^g)^{unr} \arrow[r, equal] \arrow[d, dash, "3"'] & \tilde{L}^{unr} \arrow[r, dash, "3"] \arrow[d, dash, "3"'] & T^{unr} \arrow[d, dash, "3"'] \\
S^{unr} \arrow[r, equal] \arrow[d, dash, "2"'] & \tilde{H}^{unr} \arrow[r, dash, "3"] \arrow[d, dash, "2"'] & \tilde{M}^{unr} \arrow[d, dash, "2"'] \\
K^{unr} \arrow[r, equal] & H^{unr} \arrow[r, dash, "3"] & M^{unr}
\end{tikzcd}$$

Let μ be a character of $S^\times$ such that $\ker\mu = \mathrm{Gal}(\overline{K}/F^g)$, let $\tilde{\mu} = \mathrm{Res}_S^{\tilde{H}}\mu$, $\tilde{\phi} = \mathrm{Res}_H^{\tilde{H}}\phi$. Then $a(\tilde{\phi}) = 2a(\phi) - 1$ by Lemma B.2 and hence $a(\tilde{\phi})$ is odd. Also, it is easy to check that $\mu|_{K^\times} = 1_K$ and hence $a(\mu) = a(\tilde{\mu})$ is even by Lemma 4 on p. 132 in [FQ73]. Let $G = \mathrm{Gal}(T^{unr}/H^{unr}) \cong S_3 \times \mathbb{Z}/3\mathbb{Z}$. Ramification groups of G have the form

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \{1\} \quad \text{or} \tag{C.4}$$

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \cdots = G_{t+s} \supset G_{t+s+1} = \{1\}, \tag{C.5}$$

where $G_1 = \mathrm{Gal}(T^{unr}/\tilde{H}^{unr}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and in (C.5) we have $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$. It is easy to see that in case (C.4) and in case (C.5) with G_{t+1} embedded diagonally into G_1, we have $a(\tilde{\phi}) = a(\tilde{\mu})$, which is a contradiction, since by above one number is odd and the other is even. Thus (C.4) does not occur and in (C.5) we have either $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{L}^{unr})$ or $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{M}^{unr})$. If $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{L}^{unr})$, then we have $a(\tilde{\phi}) = a(\tilde{\phi}\otimes\tilde{\mu}) = 1 + t + \frac{s}{3}$, $a(\tilde{\mu}) = 1 + t$. Since $a(\tilde{\phi})$ is odd and $a(\tilde{\mu})$ is even, we conclude that both t and $a(\tilde{\phi}\otimes\tilde{\mu})$ are odd. Analogously, if $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{M}^{unr})$, then $a(\tilde{\phi}) = 1 + t$, $a(\tilde{\mu}) = a(\tilde{\phi}\otimes\tilde{\mu}) = 1 + t + \frac{s}{3}$, so that both t and $a(\tilde{\phi}\otimes\tilde{\mu})$ are even.

On the other hand, $\tau = \mathrm{Ind}_K^F 1_F \cong 1_K + \mathrm{Ind}_K^S \mu$ and using the inductive properties of function $a(-)$ one can see that

$$a(\sigma\otimes\tau)/2 - a(\tau) \equiv a(\phi) + a(\tilde{\phi}\otimes\tilde{\mu}) \equiv a(\phi) + t \bmod 2,$$

so that using (C.3) we have $A \equiv a(\phi) + t \bmod 2$ in (C.2).

We now show that both cases t is even and t is odd can occur. Let $K = \mathbb{Q}_3$ and let $B = \mathrm{Gal}(F^g/K) \cong S_3$, $C = \mathrm{Gal}(M/H) \cong \mathbb{Z}/3\mathbb{Z}$. Then the ramification groups of B and C are

$$B = B_0 \supset B_1 = \cdots = B_\alpha \supset B_{\alpha+1} = \{1\}, \quad B_1 \cong \mathbb{Z}/3\mathbb{Z}, \tag{C.6}$$

$$C = C_0 = C_1 = \cdots = C_\beta \supset C_{\beta+1} = \{1\}. \tag{C.7}$$

Thus $a(\mu) = 1 + \alpha$ and $a(\phi) = 1 + \beta$. By the previous paragraph we also have two cases:

1. $a(\mu) = 1 + t$, $a(\phi) = 1 + \frac{1}{2}(t + \frac{s}{3})$ or
2. $a(\mu) = 1 + t + \frac{s}{3}$, $a(\phi) = 1 + \frac{t}{2}$.

On the other hand, $\alpha \le e(F^g/\mathbb{Q}_3)/2 = 3$, $\beta \le e(M/\mathbb{Q}_3)/2 = 1.5$ (see e.g., [S79], p. 72, Exc. 3c). Thus $\beta = 1$ and since $a(\mu)$ is even, $\alpha = 1$ or $\alpha = 3$. Furthermore, by comparing $a(\mu)$ and $a(\phi)$ in terms of α, β with those in terms of t, s, we have two cases

1. $\alpha = t$, $\beta = \frac{1}{2}(t + \frac{s}{3}) = 1$, hence $\alpha = t = 1$, or
2. $\alpha = t + \frac{s}{3}$, $\beta = \frac{t}{2} = 1$, hence $t = 2$, $\alpha = 3$.

Consider the following elliptic curves over $\mathbb{Q}_3$:

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5,$$
$$E_1 : y^2 + y = x^3,$$
$$E_2 : y^2 + y = x^3 - 1.$$

Let Δ, Δ_1, and Δ_2 denote the minimal discriminants of E, E_1, and E_2, respectively. It is shown in [Ki03] that E, E_1, and E_2 are of the Kodaira-Néron reduction type II, $\mathrm{val}_{\mathbb{Q}_3}(\Delta) = a(\sigma_E) = 4$, $\mathrm{val}_{\mathbb{Q}_3}(\Delta_1) = a(\sigma_{E_1}) = 3$, $\mathrm{val}_{\mathbb{Q}_3}(\Delta_2) = a(\sigma_{E_2}) = 5$. It is not hard to check that this implies, in particular, that E satisfies the hypothesis of Lemma C.1. Also, denote $M_i = \mathbb{Q}_3(E_i[2])$, $i = 1, 2$. Then one can check that $\mathrm{Gal}(M_i/\mathbb{Q}_3) \cong S_3$ and M_i is totally ramified over $\mathbb{Q}_3$. For $i \in \{1, 2\}$ let ϕ_i denote the analogue of ϕ for E_i (note that each ϕ_i is wildly ramified), M_i will play a role of F^g in our notation above, and let α_i denote the analogue of α for M_i. From $a(\sigma_{E_1}) = 3$ and $a(\sigma_{E_2}) = 5$ we can find $a(\phi_1) = 2$, $a(\phi_2) = 4$. Moreover, note that $a(\phi_i) = \alpha_i + 1$, so that $\alpha_1 = 1$, $\alpha_2 = 3$. Hence by cases (1) and (2) above there exist non-Galois cubic extensions $F_i/\mathbb{Q}_3 \subset M_i/\mathbb{Q}_3$ such that $t(F_1) = 1$ and $t(F_2) = 2$. $\square$

References

[D72] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 501–597. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[D00] Do Ngoc Diep, *Methods of noncommutative geometry for group C*-algebras.* Chapman & Hall/CRC Research Notes in Mathematics, 416. Chapman & Hall/CRC, Boca Raton, FL, 2000.

[DD08] T. Dokchitser, V. Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. 40 (2008), no. 3, 516–524.

[FQ73] A. Fröhlich, J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Invent. Math. 20 (1973), 125–138.

[I94] I. M. Isaacs, *Character theory of finite groups* (Dover Publications, Inc., New York, 1994).

[Ki03] M. Kida, *Variation of the reduction type of elliptic curves under small base change with wild ramification*, Cent. Eur. J. Math. 1 (2003), no. 4, 510–560.

[Ko02] S. Kobayashi, *The local root number of elliptic curves with wild ramification*, Math. Ann. 323 (2002), no. 3, 609–623

[KT82] K. Kramer, J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. 46 (1982), no. 3, 307–352.

[Kr90] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. 69 (1990), no. 4, 353–385.

[R93] D. E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. 87 (1993), no. 2, 119–151.

[R94] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics (CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994), 125–157.

[R95] D. E. Rohrlich, *Epsilon factors of elliptic curves over the rationals*, preprint (unpublished).

[R96] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compositio Math. 100 (1996), 311–349.

[S77] J.-P. Serre, *Linear representations of finite groups* (Springer-Verlag, New York-Heidelberg, 1977).

[S79] J.-P. Serre, *Local fields* (Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979).

[ST68] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) 88 (1968), 492–517.

[W] D. Whitehouse, *Root numbers of elliptic curves over 2-adic fields*, preprint (unpublished).

Department of Mathematics, CUNY Queens College, 65-30 Kissena Blvd., Flushing, NY 11367, USA
E-mail address: Maria.Sabitova@qc.cuny.edu