Root Numbers of 5-adic Curves of Genus Two Having Maximal Ramification

Lukas Melninkas

Abstract. The formulas for local root numbers of abelian varieties of dimension one are known. In this paper we treat the simplest unknown case in dimension two by considering a curve of genus 2 defined over a 5-adic field such that the inertia acts on the first \( \ell \)-adic cohomology group through the largest possible finite quotient, isomorphic to \( C_5 \times C_8 \). We give a few criteria to identify such curves and prove a formula for their local root numbers in terms of invariants associated to a Weierstrass equation.

Mathematics Subject Classification. Primary 11G10, 11G20; Secondary 14H25, 11G40.

Introduction

Let \( A \) be an abelian variety defined over a number field \( \mathcal{K} \). Its global root number \( w(A/\mathcal{K}) \) is the sign appearing in the conjectural functional equation of its completed \( L \)-function. Granting the Birch–Swinnerton–Dyer conjecture, \( w(A/\mathcal{K}) = -1 \) exactly when the Mordell–Weil rank is odd. Deligne \[10\] gives an unconditional definition of \( w(A/\mathcal{K}) \) relying on the local root numbers \( w(A_v/\mathcal{K}_v) \) of the completed abelian varieties at each place \( v \) of \( \mathcal{K} \).

For each infinite place we have \( w(A_v/\mathcal{K}_v) = (-1)^{\dim A} \). If \( A \) has good reduction at a finite place \( v \), then \( w(A_v/\mathcal{K}_v) = 1 \). This allows to define
\[
w(A/\mathcal{K}) = \prod_v w(A_v/\mathcal{K}_v),
\]
the product being taken over all places of \( \mathcal{K} \). The local root numbers at places of bad reduction are signs \( \pm 1 \) and are defined in a general way as follows.

Let \( p \) be a prime number, let \( \mathcal{K}/\mathbb{Q}_p \) be a finite extension with an algebraic closure \( \overline{\mathcal{K}} \), and let \( A/\mathcal{K} \) be an abelian variety. We choose another prime number \( \ell \neq p \) and consider the \( \ell \)-adic Galois representation \( \rho_\ell \) on the étale cohomology group \( H^1_{\text{ét}}(A_{\overline{\mathcal{K}}}, \mathbb{Q}_\ell) \). Applying Grothendieck’s monodromy construction we obtain a complex Weil–Deligne representation \( \text{WD}(\rho_\ell) \), whose isomorphism class does not
depend on $\ell$ (see, e.g., [29, Cor. 1.15]). Next, following Deligne, after choosing an additive character $\psi$ on $K$ and a Haar measure $dx$ on $K$, we consider the $\epsilon$-factor $\epsilon(\text{WD}(\rho_\ell), \psi, dx) \in \mathbb{C}$. The local root number is then defined as

$$w(A/K) := \frac{\epsilon(\text{WD}(\rho_\ell), \psi, dx)}{|\epsilon(\text{WD}(\rho_\ell), \psi, dx)|}.$$ 

We note that $w(A/K)$ does not depend on $\ell$, $\psi$, or $dx$, see [26, §11, §12].

It follows (see, e.g., [7, Prop. 3.1]) from the semi-stable reduction theorems and the theory of $p$-adic uniformization that there exists an abelian variety $B/K$ with potentially good reduction and an extension $S$ of $B$ by a torus $T$ such that the rigid analytification of $A$ is a quotient of the analytification of $S$ by a lattice. Then, it follows from the result of Sabitova [29, Prop. 1.10] that $w(A/K)$ can be determined by computing $w(B/K)$ and the Galois action on $T$. In this paper we treat the case when $A/K$ itself has potentially good reduction. This condition is equivalent to $T = 0$ and, by the criterion of Néron–Ogg–Shafarevich, to the condition that the image of inertia via $\rho_\ell$ is finite. By Serre–Tate [32, p. 497, Cor. 2] the representation $\rho_\ell$ is at most tamely ramified whenever $p > 2 \dim(A) + 1$.

If $A/K$ is an elliptic curve with potentially good reduction, formulas for root numbers have been given by Rohrlich [27] when $p \geq 5$, by Kobayashi [14] when $p = 3$, and by the Dokchitsers [9] when $p = 2$. The case of Jacobians having semistable reduction have been studied by Brumer–Kramer–Sabitova [5]. For general abelian varieties, the case when $\rho_\ell$ is tamely ramified has been studied by Bisatt [3].

0.1. The Main Setup and Results

We consider a curve $C$ of genus 2 defined over a 5-adic field $K$. Let $J(C)/K$ be its Jacobian surface. Our aim is to produce a formula for $w(C/K) := w(J(C)/K)$ in terms of other invariants of $C/K$. We suppose that $J(C)/K$ has potentially good reduction and that the associated Galois representation $\rho_\ell$ is wildly ramified. In general, the root number depends tightly on the decomposition of $\rho_\ell$ into irreducible factors, which is rather difficult determine from higher-level geometric or arithmetic invariants of $C/K$. In order to overcome this we suppose further that $\rho_\ell$ has the maximal possible inertia image, isomorphic to the semi-direct product $C_5 \rtimes C_8$ where $C_8$ acts on $C_5$ via $C_8 \rightarrow \text{Aut}(C_5)$. We will show that this setting can be detected from the Artin conductor, the 2-torsion of $J(C)$, or the discriminant of $C/K$, and that in this case $\rho_\ell$ is always irreducible.

After choosing a Weierstrass equation for $C/K$ we may compute its discriminant $\Delta \in K^\times$, whose class in $K^\times/(K^\times)^2$ does not depend on the choice of the equation, see 2.3.

Let $k_K$ be the residue field of $K$. We denote by $(\frac{\cdot}{k_K})$ the Legendre symbol on $k_K^\times$ and by $(\cdot, \cdot)/K$ the quadratic Hilbert symbol on $K^\times \times K^\times$. We consider $v_K$ the normalized valuation of $K$ such that $v_K(K^\times) = \mathbb{Z}$. Let $F_5$ denote the Frobenius group on 5 elements, defined as the semi-direct product $F_5 = C_5 \rtimes C_4$ where $C_4$ acts faithfully on $C_5$.

**Theorem 0.1.1.** [Prop. 2.10.1, Proposition 4.0.4, Theorem 5.0.1] Let $C/K$ be a smooth projective curve of genus 2 defined over a 5-adic field $K$. We suppose that
the associated $\rho_\ell$ has finite inertia image of order divisible by 5. There exists an
equation $Y^2 = P(X)$ defining $C/K$ with unitary, irreducible $P \in K[X]$ of degree 5
having integral coefficients and a constant term $a_6$ such that $5 \nmid v_K(a_6)$.

The image of inertia of $\rho_\ell$ is the maximal possible, i.e. isomorphic to $C_5 \rtimes C_8$,
if and only if any of the following equivalent conditions is verified:

1. For any discriminant $\Delta$ of $C/K$ the valuation $v_K(\Delta)$ is odd;
2. The $\mathbb{F}_2$-linear Galois representation on the 2-torsion points $J(C)[2]$ has inertia
image isomorphic to the Frobenius group $F_5$;
3. The Artin conductor $a(C/K)$ of $\rho_\ell$ is odd.

In this case, the root number is given by

$$w(C/K) = (-1)^{[k_K: \mathbb{F}_5]} + 1 \cdot \left(\frac{v_K(a_6)}{k_K}\right) \cdot (\Delta, a_6)_K.$$

Remark 0.1.1. The setting of Theorem 0.1.1 is a particular case of the study by
Coppola [8], where a description of $\rho_\ell$ is given. Very recently, building on Coppola’s
results, Bisatt [4, Thm. 2.1] produced similar formulas of root numbers of hyperel-
liptic curves. Our article proposes a slightly different method with an emphasis on
geometry of curves.

0.2. Structure of the Paper

In Sect. 1 we recall some theory of $\epsilon$-factors of one-dimensional Weil representations
and give formulas for root numbers in some wild ramification cases by using explicit
local class field theory. In Sect. 2 we present some properties of genus 2 curves
with wild ramification. In Sect. 3 we employ the Artin–Schreier theory in order to
study $\rho_\ell$ via the automorphisms of curves over finite fields. In Sect. 4 we prove
a few characterizations of the maximal ramification case and exploit some of its
implications. Section 5 is dedicated to proving the formula of Theorem 0.1.1, where
we connect the results of Sect. 1 to a particular Weierstrass equation.

Notation and Conventions

Let $p$ be a prime number, and let $K/\mathbb{Q}_p$ be a finite extension. We adopt the con-
vention that every algebraic extension of $K$ used in this text is a subfield of $\overline{K}$. We
fix the following notation.

By a Weil representation on a complex vector space $V$ we mean a group ho-
momorphism $\rho : W_K \to \text{GL}(V)$ such that $\rho(I_K)$ is finite. For any $s \in \mathbb{C}^\times$, its Tate
twist is $\rho(s) := \rho \otimes \chi_{\text{ur}}^s$.

Let $\theta_K : K^\times \cong W_K^{\text{ab}}$ be Artin’s reciprocity map normalized to send a uni-
formizer to the class of a geometric Frobenius lift. The map $|| \cdot ||_K := \chi_{\text{ur}} \circ \theta_K$
is the non-Archimedean norm on $K$ induced by $v_K$. For every finite Galois extension
$L/K$, the map $\theta_K$ induces an isomorphism $\theta_{L/K} : K^\times / N_{L/K}(L^\times) \cong \text{Gal}(L/K)^{\text{ab}}$,
where $N_{L/K} : L^\times \to K^\times$ is the norm map.

Given schemes $X$, $S$, $S'$ as well as morphisms $X \to S$ and $S' \to S$, we will write
$X_{S'} := X \times_S S'$, and also $X_{R'} := X \times_R R'$ if $S' = \text{Spec } R'$ and $S = \text{Spec } R$
are affine.
The valuation of $K$ normalized by $v_K(K^\times) = \mathbb{Z}$

$O_K$ The ring of integers

$m_K$ The maximal ideal

$\varpi_K$ A uniformizer

$k_K$ The residue field

$q_K$ The order $|k_K|

m^n_K$ The subgroup $\varpi^n_K O_K \subset K$ for any $n \in \mathbb{Z}$

$U^n_K$ $1 + m^n_K$ for $n \geq 1$, and $U^n_K = O^n_K$

$(\cdot, \cdot)_{K}$ The Legendre symbol on $k_K^\times$

$(\cdot, \cdot)_{K}$ The quadratic Hilbert symbol on $K^\times \times K^\times$

$\bar{K}$ An algebraic closure of $K$

$\bar{k}_K$ The residue field of $\bar{K}$

$\Gamma_K$ The group $\text{Gal}(\bar{K}/K)$

$W_K$ The Weil subgroup of $\Gamma_K$

$I_K$ The inertia subgroup

$I^w_K$ The wild inertia subgroup

$\varphi_K$ A lift in $W_K$ of the geometric Frobenius

$\chi_{ur}$ The unramified (cyclotomic) character $W_{\mathbb{Q}_p} \to \mathbb{C}^\times$ with $\chi_{ur}(\varphi_K) = q_K^{-1}$ for every finite $K/\mathbb{Q}_p$

1. Root Numbers and Explicit Class Field Theory

Let $p > 2$ be a prime number and let $K/\mathbb{Q}_p$ be a finite extension.

1.1. Choice of an Additive Character

By an additive character we mean a locally constant group homomorphism $\psi : K \to \mathbb{C}^\times$. By $n(\psi)$ we denote the largest integer $n$ such that $\psi$ is trivial on $m^n_K$, called the level of $\psi$. In order to simplify the computations of the root number we fix a particular character. Let $\psi_k$

$$\psi_k : O_K \to k \xrightarrow{\text{tr}_{k/\mathbb{F}_p}} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\exp\left(\frac{2\pi i \cdot}{p}\right)} \mathbb{C}^\times.$$ 

We see that $\psi_k$ is trivial on $m_K$. Since $\mathbb{C}^\times$ is divisible, $\psi_k$ can be extended non-uniquely to an additive character of $K$, which we again denote by $\psi_k$. Since $\text{tr}_{k/\mathbb{F}_p}$ is nontrivial, independently on the choice of the extension, we have $n(\psi_k) = -1$. Moreover, every additive character of level $-1$ is given by $x \mapsto \psi_k(cx)$ for some $c \in O_K^\times$.

1.2. $\psi$-Gauges of Weil Characters

Let $\chi : W_K \to \mathbb{C}^\times$ be a one-dimensional ramified Weil representation. We identify $\chi$ with a quasi-character of $K^\times$ via $\theta_K$. The Artin conductor $a(\chi)$ is the smallest integer $a$ such that $\chi$ is trivial on $U^a_K$. Let $n := \left\lfloor \frac{a(\chi)+1}{2} \right\rfloor$. The map $x \mapsto \chi(1 + x)$ defined for $x \in m^n_K$ is additive, trivial on $m^n_K$, and extends to an additive character $\psi_{\chi}$ of $K$ with $n(\psi_{\chi}) = a(\chi)$. Let $\varpi_K \in m_K$ be a uniformizer. Then $x \mapsto \psi_{\chi}(\varpi_K^{-a(\chi)-1} x)$ has level $-1$. Thus, there exists $c_\chi \in K^\times$, called a $\psi_k$-gauge of
\( \chi \), of valuation \(-a(\chi) + 1\), unique modulo \( m_K^{-n+1} \), such that for all \( x \in m_K^n \):

\[
\chi(1 + x) = \psi_k(c_\chi x). \tag{1.2.1}
\]

### 1.3. Epsilon Factors of Characters

In addition to the setting of 1.2, we fix a Haar measure \( dx \) on \( K \). We recall from \([10, (3.4.3.2)]\) that the \( \epsilon \)-factor of \( \chi \) relative to \( \psi_k \) and \( dx \) is defined as the integral

\[
\epsilon(\chi, \psi_k, dx) := \int_{\mathbb{A}_K^{a(\chi)+1} \mathcal{O}_K^\times} \chi^{-1}(x)\psi_k(x) \, dx. \tag{1.3.1}
\]

We will be mainly interested in the root number

\[
w(\chi, \psi_k) := \frac{\epsilon(\chi, \psi_k, dx)}{|\epsilon(\chi, \psi_k, dx)|},
\]

which does not depend on \( dx \).

For \( a, b \in \mathbb{C}^\times \) we will write \( a \approx b \) whenever \( ab^{-1} \) is contained in the subgroup of \( \mathbb{C}^\times \) generated by positive real numbers and the complex roots of unity of \( p \)-power orders. We note that if \( p \neq 2 \) and \( a, b \in \{-1, 1\} \) are such that \( a \approx b \), then \( a = b \).

### 1.4. Cyclic Ramification

The group \( \chi(I_K) \) is finite and cyclic, we denote its order by \( ep^r \) with \( e \) prime to \( p \). We view the restriction \( \chi|_{I_K} \) as a character of the group \( \text{Gal}(K^{ab}/K^{ur}) \). The group \( \ker(\chi|_{I_K}) \) cuts out an abelian extension \( L'/K \) containing \( K^{ur} \). The closure of the subgroup generated by \( \varphi_K \) in \( \text{Gal}(L'/K) \) cuts out a totally ramified abelian extension \( L/K \), such that \( L = LK^{ur} \). We then have canonical isomorphisms

\[
\text{Gal}(K^{ab}/K^{ur})/\ker(\chi|_{I_K}) \cong \text{Gal}(L'/K^{ur}) \cong \text{Gal}(L/K).
\]

The restriction \( \chi|_{I_K} \) induces a faithful complex one-dimensional representation of the finite group \( \text{Gal}(L/K) \), and thus \( \text{Gal}(L/K) \) must be cyclic. Let \( M/K \) be the unique subextension of \( L/K \) of degree \( p^r \). Then \( \chi^e|_{I_K} \) has order \( p^r \) and induces a faithful character of the cyclic group \( \text{Gal}(M/K) \).

The following is an alloy of some of the results of \([14]\) and \([1]\).

**Theorem 1.4.1.** Let \( \psi_k \) be as in 1.1. Let \( \chi : W_K \to \mathbb{C}^\times \) be a Weil character such that \( |\chi(I_K^\times)| = p \). Let \( ep = |\chi(I_K)| \) with \( e \) prime to \( p \). Let \( M/K \) be as in 1.4. We denote by \( \sigma \in \text{Gal}(M/K) \) the generator that is sent to \( \exp(\frac{2\pi i}{p}) \) via \( \chi \). Let \( \varpi_M \) be a uniformizer of \( M \), and let \( \delta_\chi := \mathcal{N}_{M/K}(1 - \frac{\sigma(\varpi_M)}{\varpi_M^p}) \). Let us write \( \delta_\chi = u \varpi_K^{\nu_K(\delta_\chi)} \) with \( u \in \mathcal{O}_K^\times \), whose class in \( k_K^\times \) we denote by \( \varpi \).

1. If \( a(\chi) \) is even, then \( \epsilon(\chi, \psi_k, dx) \approx \chi(\delta_\chi) \);
2. If \( a(\chi) \) is odd, and \( p \equiv 1 \mod 4 \), then

\[
\epsilon(\chi, \psi_k, dx) \approx -\chi(\delta_\chi) \cdot \left( \frac{2\varpi}{k_K} \right) \cdot (-1)^{[k_K : F_p]}.
\]

**Lemma 1.4.1.** We have \( v_K(\delta_\chi) = a(\chi) - 1 \) and \( c_\chi \delta_\chi \in U_K^1 \). In particular, \( \chi^{-1}(c_\chi) \approx \chi(\delta_\chi) \).
Proof. The lemma is essentially proved in [14, p. 618]. We shall repeat Kobayashi’s argument in our setting.

Let \( t \) be the largest integer such that the \( t \)-th ramification subgroup \( G_t \) of \( \text{Gal}(M/K) \) is nontrivial. We then have \( G^t = G_{t'} = \text{Gal}(M/K) \) and \( G^t = \{ \} \) for \( t' > t \), see [31, V.\$3]. The reciprocity map (see [31, XV.\$2]) and \( \chi \) induce a commutative diagram

\[
\begin{array}{ccc}
U_K^t / U_K^{t+1} N_{M/K} (U_M^t) & \xrightarrow{\sim} & G^t = \text{Gal}(M/K) \\
& & \xrightarrow{\chi^e | I_K} \mathbb{C}^\times \\
U_K^t & \xrightarrow{\chi^e | I_K} & \text{Gal}(K^{ab}/K^{ur}) \xrightarrow{\chi | I_K} \mathbb{C}^\times.
\end{array}
\] (1.4.1)

As \( e \) is prime to \( p \) we observe that \( a(\chi) = a(\chi^e) \) and that \( a(\chi^e) = t + 1 \). Since \( \sigma \in G_t \setminus G_{t+1} \), by using [31, IV.Prop. 5] we obtain

\[
v_K(\delta \chi) = v_M(1 - \sigma(\omega_M) / \omega_M) = t = a(\chi) - 1.
\] (1.4.2)

Applying [31, XV.\$3, Exercise 1] shows that for all \( v \in U_K^t \),

\[
\theta_{M/K}(v) = \sigma^{tr_{K/F}}((v-1)/\delta \chi \mod m_K).
\] (1.4.3)

For every \( x \in m_K^{a(\chi)-1} \subseteq m_K^a \), taking the image of (1.4.3) by \( \chi \), we obtain \( \chi^e(1 + x) = \psi_k(e\delta^{-1}x) \), and taking the \( e \)-th power of (1.2.1) gives \( \chi^e(1 + x) = \psi_k(ec \chi x) \). We note that \( e\delta^{-1}m_K^{a(\chi)-1} = \mathcal{O}_K \). Thus,

\[
\psi_k((1 - \delta \chi c \chi) \mathcal{O}_K) = \psi_k((e\delta^{-1} - ec \chi)m_K^{a(\chi)-1}) = 1.
\]

Therefore, we must have \( 1 - \delta \chi c \chi \in m_K^{-n(\psi_k)} = m_K \). The last part of the lemma follows from the fact that \( \chi(U_K^t) \) is a finite \( p \)-group. \( \square \)

Proof of Theorem 1.4.1. We shall apply [1, Prop. 8.7, (ii)] which allows to express the epsilon factor using a refined \( \psi_k \)-gauge \( c \) of \( \chi \). Abbes–Saito proves that there exists an element \( c \in K \), unique modulo \( m_K^{-n+1} \), such that for every \( x \in m_K^{a(\chi)-n} \) we have

\[
\chi \left( 1 + x + \frac{x^2}{2} \right) = \psi_k(cx).
\]

Let \( \tau : k_K \to K \) be the Teichmüller lift. The quadratic Gauss sum

\[
G_{\psi_k} := \sum_{x \in k_K} \psi_k(\tau(x)^2)
\]

satisfies well-known formulas \( G_{\psi_k} = \sum_{x \in k_K} \left( \frac{x}{k_K} \right) \psi_k(\tau(x)) \) and \( G_{\psi_k}^2 = \left( \frac{-1}{k_K} \right) q_K \) (see, e.g., [2, \$1.1]). The Abbes–Saito formula\(^1\) [1, (8.7.3)] can be rewritten as

\[
\epsilon(\chi, \psi_k, dx) \approx \chi^{-1}(c) \psi_k(c) \left( \frac{-1}{k_K} \right) \left( \frac{a(\chi)}{2} \right) G_{\psi_k}^{-a(\chi)} \times \begin{cases} 1 & \text{if } a(\chi) \text{ is even}, \\ (-2c, \omega_K)_K & \text{if } a(\chi) \text{ is odd}. \end{cases}
\] (1.4.4)

\(^1\)The formula is stated for the \( \epsilon_0 \)-factor of \( \chi \), which is equal to the \( \epsilon \)-factor when \( \chi \) is ramified.
Since $c$ is also a $\psi_k$-gauge of $\chi$, we have $\chi^{-1}(c) \approx \chi(\delta_k)$ by Lemma 1.4.1. For $r \in \mathbb{Z}$ large enough, $\psi_k(p^r c) = 1$, so $\psi_k(c) \approx 1$. If $a(\chi)$ is even, then it is straightforward to verify that (1) holds.

We now assume the hypotheses of (2). Then $\psi_k(c) = 1$, and $G \approx -(-1)[K:F_p]$, see [2, Thm. 11.5.4]. We also have $-2, \varpi_K \psi_k(c) \approx \chi^{-1}(c)$ by Lemma 1.4.1. For $r$ large enough, $\psi_k(\chi^{-1}(c)) = 1$, so $\psi_k(c) \approx 1$. If $a(\chi)$ is even, then it is straightforward to verify that (1) holds.

**Proposition 1.4.1.** We continue in the situation of Theorem 1.4.1. Let $\alpha \in \mathcal{O}_M$ be such that $p \nmid v_M(\alpha)$, and let $D_{\alpha,\chi} := N_{M/K} \left(1 - \frac{v_M(\alpha)}{\alpha}\right)$. Then

$$D_{\alpha,\chi} \equiv v_M(\alpha) \theta_K \mod U_K^1.$$  

**Proof.** A detailed proof when $p = 3$ can be found in [14, p. 614]. It generalizes for any $p > 2$ without significant modifications. □

**Corollary 1.4.1.** If $a(\chi)$ is even and $\alpha \in \mathcal{O}_M$ is such that $p \nmid v_M(\alpha)$, then

$$\epsilon(\chi, \psi_k, dx) \approx \chi \circ \theta_K \left(\frac{D_{\alpha,\chi}}{v_M(\alpha)}\right).$$

**Proof.** Follows from Theorem 1.4.1. (1) and Proposition 1.4.1. □

### 2. Curves of Genus 2 and Wild Ramification

#### 2.1. Generalities

Let $K$ be a $p$-adic local field with $p \neq 2$, and let $C/K$ be a smooth, projective, and geometrically connected curve of genus 2 defined over $K$. The curve $C/K$ is hyperelliptic (see [20, 7, Prop. 4.9]), and there exists an open affine subvariety $C_{\text{aff}}$ of $C$ which is defined by a single Weierstrass equation

$$Y^2 = P(X),$$

where $P \in K[X]$ has simple roots and has degree 5 or 6.

#### 2.2. Discriminants

Following [19, §2] we define the discriminant of an equation (2.1.1) in terms of the discriminant of the polynomial $P$: let $a_0$ be the leading coefficient of $4P$, then

$$\Delta(P) := \begin{cases} 2^{-12} \text{disc}(4P) & \text{if } \deg P = 6, \\ 2^{-12} a_0^2 \text{disc}(4P) & \text{if } \deg P = 5. \end{cases}$$

In particular, if $P(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)(X - \alpha_5)$, then

$$\Delta(P) = 2^8 \prod_{1 \leq i < j \leq 5} (\alpha_i - \alpha_j)^2.$$
We note that $\Delta(P) \neq 0$ since $C$ is non-singular.

2.3. Change of Variables

The Eq. (2.1.1) is unique up to a transformation

$$X' = \frac{aX + b}{cX + d}, \quad Y' = \frac{eY}{(cX + d)^3}$$

(2.3.1)

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(K)$ and $e \in K^\times$. If $Y'^2 = P'(X')$ is obtained from (2.1.1) via (2.3.1), then the new discriminant is

$$\Delta(P') = e^{20} \left| \begin{pmatrix} a \\ c \end{pmatrix} \right|^3 \Delta(P).$$

(2.3.2)

As an immediate consequence, the class of a discriminant in $K^\times/(K^\times)^2$ does not depend on the choice of a Weierstrass equation.

2.4. Root Numbers and Semi-stable Reduction

Let $C/K$ be as in 2.1 and let $J(C)/K$ be its Jacobian. We denote by $J(C/K)^\circ_k$ the neutral component of the special fiber of the Néron model of $J(C)/K$. Let $\ell \neq p$ be a prime number. We have an isomorphism of $\ell$-adic $\Gamma_K$-representations

$$H^1_{\text{ét}}(C_K, \mathbb{Q}_\ell) \cong H^1_{\text{ét}}(J(C)_K, \mathbb{Q}_\ell),$$

we denote either of them by $\rho_\ell$. The root number $w(C/K) := w(\rho_\ell)$ is defined via the the complex Weil–Deligne representation associated to $\rho_\ell$ (see, e.g., [26]). Let $L/K$ be a finite extension over which $C$ has stable reduction. Then $J(C_L)/L$ has semi-stable reduction, i.e. that $J(C_L/L)^\circ_k$ is an extension of an abelian variety by a torus. Using Sabitova’s decomposition [29, Prop. 1.10] we can separate the contributions to $w(C/K)$ coming from the abelian and the toric parts of $J(C_L/L)^\circ_k$.

2.5. Hypotheses

We suppose from now on that $J(C_L)/L$ has good reduction or, equivalently, that $J(C)/K$ has potentially good reduction. It follows from the semi-stable reduction theorems that this happens exactly when $\rho_\ell(I_K)$ is finite. In this case we write $|\rho_\ell(I_K)| = ep^r$ with $e$ coprime to $p$. We further suppose that $r \geq 1$, i.e. $\rho_\ell$ is wildly ramified. Due to Serre–Tate [32, p. 497, Cor. 2], necessarily, $p \leq 5$. We will later suppose that $p = 5$.

2.6. Inertially Minimal Extensions

It follows from the Néron–Ogg–Shafarevich criterion that $J(C)$ attains good reduction over $L' := \overline{K}_{\ker \rho_\ell|_K}$ and that $L'/K_{\text{ur}}$ is the minimal such extension. We call an algebraic extension $L/K$ inertially minimal (IM) for $J(C)/K$ if $I_L = I_{L'} = \ker \rho_\ell|_{I_K}$. In other words, $L/K$ is IM if and only if $J(C)$ has good reduction over $L$ and has bad reduction over every proper subextension of $K_{\text{ur}}L/K_{\text{ur}}$. 
2.7. Good Reduction and Torsion

For $m \geq 1$ we denote by $J(C)[m]$ the subgroup of $m$-torsion points of $J(C)(\overline{K})$ and by $K(J(C)[m])$ the smallest regular model $C_L$ over $K$ is strictly Henselian and (with kernel $C$). For $m \geq 3$ coprime to $p$, it follows from Serre–Tate [32, Cor. 3, p. 498] that the extension $K(J(C)[m])/K$ is IM for $J(C)/K$. Similarly, for $p \neq 2$, Serre [30] shows that $|\rho(I_K(J(C)[2]))| \leq 2$. Thus, if $K(J(C)[2])/K$ is not an IM extension, then there is a totally ramified quadratic extension $L/K(J(C)[2])$ such that $L/K$ is IM for $J(C)/K$. Therefore, if $p \neq 2$, then the groups $\rho(I_K^{w})$ and $I^w(K(J(C)[2])/K)$ are isomorphic.

2.8. We Suppose for the Rest of Section 2 that $p = 5$

The groups $\rho(I_K)$ associated to abelian surfaces have been classified by Silverberg–Zarhin [34, Thm. 1.7]. In our case $\rho(I_K)$ is one of the four groups (in the notation of [11]) satisfying the inclusions $C_5 \subset C_{10} \subset \text{Dic}_5 \subset C_5 \rtimes C_8$. More precisely, the group $\rho(I_K)$ has the form $C_5 \rtimes C_{2^i}$ where $C_{2^i}$ is a subgroup of $C_8$ acting on $C_5$ with kernel $C_2 \cap C_{2^i} \subset C_8$.

Recall the Frobenius group $F_5 = C_5 \rtimes C_4$ where $C_4$ acts faithfully on $C_5$. In particular, $F_5$ and $\text{Dic}_5$ are not isomorphic.

**Proposition 2.8.1.** Suppose that $\rho_\ell$ is wildly ramified and let $L/K$ be a finite extension. If $J(C)$ has semi-stable reduction over $L$, then $C$ has good reduction over $L$, i.e. the minimal regular model $C'/O_L$ is smooth.

**Proof.** From classical theorems we know that $C$ has semi-stable reduction over $L$, and that there exists a stable (flat) model $C'_{\text{can}}/O_L$ of $C_L/C$. The ring $R := O_{K^{ur}/L}$ is strictly Henselian and $(C'_{\text{can}})_R$ is a stable model of $C_{K^{ur}/L}/K^{ur}$. Wild ramification of $\rho_\ell$ implies that $5$ divides $[K^{ur}/L : K^{ur}]$. By studying the possible orders of automorphisms of stable curves Liu [16, Cor. 4.1.(4)] showed that $(C'_{\text{can}})_{\overline{L}/\overline{K}}$ must be smooth. Thus $(C'_{\text{can}})_{\overline{L}/\overline{K}}$ and hence $C'_{\text{can}}/O_L$ are smooth. We may then use [20, 10, Prop. 1.21] to conclude that $C'/O_L$ is smooth. \qed

**Remark 2.8.1.** The hypotheses that $\rho_\ell$ is wildly ramified and that $K$ is $5$-adic are essential. The curve $C_L/L$ might have bad reduction even if $J(C)$ has good reduction over $L$. On the other hand, [6, Example 8, p. 246] shows that the non-rational irreducible components of $C'_{k_L}$ correspond to nontrivial abelian varieties as quotients of $J(C_L/L)^{\circ}_{k_L}$. Then, it can be shown in general that if $J(C_L/L)^{\circ}_{k_L}$ is a simple abelian variety, then $C_L/L$ has good reduction.

2.9. An Explicit IM Extension

The notation fixed in this section will be used throughout the text. Let $Y^2 = P(X)$ be a hyperelliptic equation defining $C/K$. Generalizing the results of Kraus [15], Liu [18, §5.1] provides an explicit description in terms of invariants of $P$ of the tame part of the minimal extension $L'/K^{ur}$ over which $C$ has stable reduction. By Proposition 2.8.1, this extension is precisely the IM extension for $J(C)/K$ defined in 2.6. Liu [18, §2.1] defines a so-called affine invariant $A_5$. After Proposition 2.10.1 we will always have $A_5 = 1$. We define

$$\beta := -A_5^{-6}\Delta(P),$$
fix one of its 8th roots $\beta^{1/8} \in \overline{K}$, and denote $\beta^{1/4} := (\beta^{1/8})^2$ and $\nu := v_K(\beta)$. Let $\zeta_8 \in \overline{K}$ be some fixed primitive 8th root of unity.

Let $L'_t/K^{ur}$ be the maximal tamely ramified subextension of $L'/K^{ur}$, then $L'/L'_t$ is totally wildly ramified of degree 5. Liu proves that

$$L'_t = K^{ur}(\beta^{1/8}).$$  \hspace{1cm} (2.9.1)

We define the following field extensions of $K$:

$$M := K(J(C)[2]), \quad N := K(\beta^{1/8}), \quad H := K(\beta^{1/4}), \quad \text{and} \quad L := MN.$$  

We recall from [23, 3.39, Cor. 2.11] that $M$ is the splitting field of $P$. The extension $M/K$ is finite Galois. The extension $L/K$ is finite but not necessarily Galois.

**Proposition 2.9.1.** The extension $L/K$ is IM for $J(C)/K$ or, equivalently, $L' = K^{ur}L$. The extension $L(\zeta_8)/K$ is Galois. In particular, if the residual degree $f(K/\mathbb{Q}_5)$ is even, then $L/K$ is Galois. The extension $L/H$ is always Galois.

**Proof.** From 2.7 we have $|\rho_t(I_M)| \leq 2$, so $\rho_t|_{I_M}$ is at most tamely ramified. It now follows from (2.9.1) that $J(C)$ has good reduction over $LK^{ur}$, so $L' \subset LK^{ur}$. On the other hand, we have $L' \supset L'_t = NK^{ur}$, and $I_{L'}$ acts trivially on $J(C)[2]$ by the Néron–Ogg–Shafarevich criterion, so $L' \supset LK^{ur}$. Therefore, $I_{L'} = I_L$.

The Galois closure of $N/K$ is $N(\zeta_8)/K$, so $L(\zeta_8)/K$ is Galois. Since $\mathbb{Q}_5$ contains the 4th roots of unity and no primitive 8th roots of unity, $K$ contains $\zeta_8$ if and only if $f(K/\mathbb{Q}_5)$ is even.

The extension $HM/K$ is Galois since $H/K$ and $M/K$ are such. Thus, $L/H$ is Galois as the compositum of $HM/H$ and $N/H$. \hfill \square

**Proposition 2.9.2.** The group $\text{Gal}(M/K)$ is isomorphic to a subgroup of $F_5$ (as in 2.8). As a consequence, the polynomial $P$ has an irreducible factor over $K$ of degree 5.

**Proof.** We recall that $\text{deg } P = 5$ or 6, so we may view $\text{Gal}(M/K) = \text{Gal}(P)$ as a subgroup of $S_5$ or $S_6$, respectively. Since the wild inertia subgroup of $\text{Gal}(P)$ is normal of order 5, the group $\text{Gal}(P)$ must be a subgroup of a normalizer subgroup $G$ of a 5-cycle in $S_5$ or $S_6$. We naturally have $F_5 \subseteq G$ and, in fact, an equality holds because for $n = 5, 6$ we have

$$|G| = \frac{|S_n|}{\#\{\text{5-Sylow’s in } S_n\}} = \frac{n!}{4 \cdot 5 \cdot (n-5)!} = 20.$$  

If $P$ was irreducible over $K$ and had degree 6, then $\text{Gal}(P)$ would have a subgroup of index 6, which is impossible. On the other hand, since $\text{Gal}(P)$ contains a 5-cycle, $P$ must have an irreducible factor of degree at least 5. \hfill \square

**Proposition 2.9.3.** The group $\rho_t(I_K)$ is isomorphic to $C_5 \rtimes C_8$, $\text{Dic}_5$, $C_{10}$, or $C_5$ if and only if $\nu \equiv 1 \mod 2$, $\nu \equiv 2 \mod 4$, $\nu \equiv 4 \mod 8$, or $\nu \equiv 0 \mod 8$, respectively. In particular, by denoting the ramification index of $L/K$ by $e(L/K)$ we have $40 \mid e(L/K) \cdot \nu$. 
Proof. By (2.9.1) and Proposition 2.9.1, the tame ramification index of \( L/K \) is determined by the the residue \( \nu \) mod 8 and is exactly the maximal prime-to-5 divisor of \( |\rho_{\ell}(I_K)| \). The group \( \rho_{\ell}(I_K) \) can then be identified from the classification in 2.8. \( \square \)

**Proposition 2.9.4.** Let \( \sigma \in I_K^\nu \) and let \( \tau \in \Gamma_K \) denote a lift of a topological generator of the tame inertia group \( I_K^\nu \). Let \( \varphi_L \in \Gamma_L \) and \( \varphi_{L(\zeta_8)} \in \Gamma_{L(\zeta_8)} \) be lifts of the geometric Frobenii. Then:

1. The images \( \rho_{\ell}(\sigma) \), \( \rho_{\ell}(\tau^4) \), and \( \rho_{\ell}(\varphi_L) \) commute;
2. The images \( \rho_{\ell}(\tau) \) and \( \rho_{\ell}(\varphi_{L(\zeta_8)}) \) commute.

In particular, \( \rho_{\ell}(\varphi_{L(\zeta_8)}) \) is central in \( \rho_{\ell}(\Gamma_K) \).

**Proof.** Proposition 2.9.1 shows that \( \rho_{\ell}|_{I_K} \) is trivial and that \( L' = LK^{ur} \). Thus, for (1) we only need to show that the classes \( \sigma I_L, \tau^4 I_L \), and \( \varphi_L I_L \) in \( \text{Gal}(L'/K) = \Gamma_K/I_L \) commute. From 2.8 we have \( \sigma^5 \in I_L \) and \( \tau^8 \in I_L \). We note that the subfield of \( L' \) fixed by \( \varphi_L I_L \) is \( L \).

Let \( F/K \) be the subextension of \( M/K \) fixed by the unique 5-Sylow subgroup of \( \text{Gal}(M/K) \). We claim that \( L/F \) is abelian. We observe that \( L/F \) is the compositum of the \( C_5 \)-extension \( M/F \) and the maximal at most tamely ramified subextension \( L_t/F \) of \( L/F \). By 2.7, the ramification index of \( L_t/F \) is at most 2, so \( L_t/F \) must be abelian. It follows that \( L/F \) is abelian. The extension \( L'/F \) is abelian as the compositum of \( L/F \) and \( K^{ur}F/F \).

We observe that the closure of the subgroup generated by \( \tau^4 I_K^\nu \) in \( I_K \) cuts out the unique extension of \( K^{ur} \) of degree 4, which contains \( F \) (we have \( [F:K] \mid 4 \) by Proposition 2.9.2). Thus, the class \( \tau^4 I_L \) is in \( \text{Gal}(L'/F) \). On the other hand, \( \sigma I_L \) and \( \varphi_L I_L \) are also in \( \text{Gal}(L'/F) \), so they all commute.

For (2) we first note that, for \( \gamma \in I_K \), we have \( \eta := \gamma \varphi_{L(\zeta_8)} \gamma^{-1} \varphi_{L(\zeta_8)}^{-1} \in I_K \).

Since \( L(\zeta_8)/K \) is Galois by Proposition 2.9.1, we have \( \gamma \varphi_{L(\zeta_8)} \gamma^{-1} \in \Gamma_{L(\zeta_8)} \), and thus \( \eta \in \Gamma_{L(\zeta_8)} \cap I_K = I_L \). Thus, \( \rho_{\ell}(\eta) \) is trivial, and hence (2) holds. \( \square \)

### 2.10. Particular Form of Hyperelliptic Equation

If \( \deg P = 6 \), then Proposition 2.9.2 shows that \( P \) has a root in \( K \). By applying a change of variables (2.3.1) that sends this root to the point at infinity, we may assume that the curve \( C/K \) is defined by a Weierstrass equation \( Y^2 = P(X) \) with \( P \) unitary and irreducible of degree 5. Applying Liu’s results [18, Prop. 5.1] gives the following

**Proposition 2.10.1.** There exist \( a_2, \ldots, a_6 \in \mathcal{O}_K \) such that the equation

\[
Y^2 = X^5 + a_2 X^4 + \ldots + a_6
\]

defines \( C/K \) and \( v_K(a_6) \in \{1, 2, 3, 4, 6, 7, 8, 9\} \). With respect to this equation, we have \( A_5 = 1 \).

**Remark 2.10.1.** Proposition 2.10.1 is an analogue of Tate’s algorithm for elliptic curves. Indeed, Liu also proved that the integer \( v_K(a_6) \) determines the geometric type of the minimal regular model of \( C/K \). These correspond to the Namikawa–Ueno [25] types [VIII-i] and [IX-i] for \( i = 1, 2, 3, 4 \).
3. Galois Action on the Special Fiber

Let \( k \) be a finite field of some characteristic \( p > 2 \). We denote by \( k(y) \) the field of rational functions in one variable over \( k \).

3.1. Artin–Schreier Curves

We briefly recall some basic Artin–Schreier theory. If \( f \in k(y) \) is not in the image of the map \( g \mapsto g^p - g \), then the equation \( x^p - x = f \) defines a smooth projective curve \( C_f \) over \( k \) together with a finite morphism \( \pi : C_f \to \mathbb{P}^1_k \) of degree \( p \). In other words, the function field \( k(C_f) = k(x, y) \) is a cyclic extension of \( k(y) \) of degree \( p \). Inversely, every cyclic extension of \( k(y) \) of order \( p \) is of this form. We may assume that \( f \) is in standard form, i.e. each pole of \( f \) is of order prime to \( p \), this is well-known, see [12, §2]. Then, \( f \) has poles at exactly the branch points of \( \pi \). In particular, if \( \pi \) has a unique branch point in \( \mathbb{P}^1_k \) which is the pole of \( y \), then \( f \) is a polynomial in \( y \). If this is the case, then the genus of \( C_f \) is given by \( g(C_f) = \frac{(\deg f - 1)(p-1)}{2} \), see, e.g., [33, 3.7.8.(d)].

For every \( a \in k^\times \) and \( c \in k \) we denote by \( C_{a,c} \) the Artin–Schreier curve given by the equation \( x^p - x - c = ay^2 \).

**Lemma 3.1.1.** Let \( p \equiv 1 \mod 4 \). On the curve \( C_{1,0}/\mathbb{F}_p \) we have the automorphisms \( \sigma_1 : (x, y) \mapsto (x + 1, y) \), \( \iota : (x, y) \mapsto (x, -y) \), and the endomorphism \( F : (x, y) \mapsto (x^p, y^p) \). They commute pairwise and, for all \( n, r, f \in \mathbb{Z} \), the trace of the pullback \( (\iota^n \circ \sigma_1^r \circ F^f)^* \) on \( H_{\acute{e}t}^1((C_{1,0})_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell) \) is given by

\[
\text{Tr}(\iota^n \circ \sigma_1^r \circ F^f)^* = \begin{cases} 
(-1)^{n+1}p^{f/2} & \text{if } f \text{ is even and } p \nmid r, \\
(-1)^n p^{f/2}(p-1) & \text{if } f \text{ is even and } p \mid r, \\
(-1)^n(\frac{p}{2})p^{f+1} & \text{if } f \text{ is odd.}
\end{cases}
\]

**Proof.** It is straightforward to verify that \( \sigma_1 \), \( F \), and \( \iota \) commute. The hyperelliptic involution \( \iota \) acts as multiplication by \(-1\) on the Jacobian variety, so \((\iota^n)^* = (-\text{Id})^n\).

The curve \( C_{1,0} \) has genus \( \frac{p-1}{2} \), and \( \dim H_{\acute{e}t}^1((C_{1,0})_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell) = p - 1 \). We recall from the classical theory that the action of \( F^* \) is semisimple and its eigenvalues have absolute value \( \sqrt{p} \). We claim that \((F^2)^* \) acts as multiplication by \( p \). For this we only need to show \( \text{Tr}(F^2)^* = p(p - 1) \). The Lefschetz trace formula

\[
\text{Tr}(F^2)^* = 1 + p^2 - |C_{1,0}(\mathbb{F}_{p^2})| \leq p + 1.
\]

For every \( x \in \mathbb{F}_{p^2} \) we have \( \text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x^p) = \text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x) \) and \( \text{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(y^2) = 0 \), which is equivalent to \( y^2 + y^{2p} = 0 \). The non-zero solutions of the latter satisfy \( y^{2(p-1)} = -1 \), raising this to the odd power \( \frac{p+1}{2} \) leads to a contradiction. Thus, the affine points of \( C_{1,0}(\mathbb{F}_{p^2}) \) are \((x, 0)\) with \( x \in \mathbb{F}_p \), and thus the claim holds.

The polynomial \( X^2 - p \) is irreducible over \( \mathbb{Z} \). Since the characteristic polynomial of \( F^* \) is in \( \mathbb{Z}[X] \), it must be \((X^2 - p)^{\frac{p+1}{2}}\).

We have \( 0 = (\sigma_1^p)^* - \text{Id} = (\sigma_1^p - \text{Id})\Phi_p(\sigma_1^p) \) where \( \Phi_p \in \mathbb{Z}[X] \) is the \( p \)-th cyclotomic polynomial. The characteristic polynomial \( P_{\sigma_1} \) of \( \sigma_1^p \) is in \( \mathbb{Z}[X] \), so its
unitary irreducible divisors can only be \( X - 1 \) or \( \Phi_p \). Since \( \deg P_{\sigma_i} = p - 1 \), we must have \( P_{\sigma_i}(X) = (X - 1)^{p-1} \) or \( \sigma_i = \Phi_p \). The first case is impossible since \( \sigma_i \) is nontrivial. Thus, \( \text{Tr}(\sigma_1^* F) = -1 \) if \( r \) is prime to \( p \), and \( \text{Tr}(\sigma_1^* F) = p - 1 \) otherwise. The formulas for the case when \( f \) is even hence follow.

If \( f \) is odd, then

\[
\text{Tr}(\ell^n \circ \sigma_1^* F^f) = (-1)^n p^{f-1} \text{Tr}(\sigma_1^* F)^*.
\] (3.1.1)

We use the Lefchetz formula

\[
\text{Tr}(\sigma_1^* F)^* = 1 + p - |\text{Fix}(\sigma_1^* F)|.
\]

The affine points \((x, y) \in C_{1,0}(\mathbb{F}_p)\) fixed by \( \sigma_1^* F \) satisfy \( x = x^p + r \) and \( y = y^p \), so \( y \in \mathbb{F}_p \) and \( -r = x^p - x = y^2 \). The latter equation has exactly \((\frac{p}{2} + 1 = \frac{p^2}{2} + 1 = \frac{p^2}{2} + 1 \) solutions in \( y \) for each \( r \in \mathbb{F}_p \). Each solution \( y \) gives exactly \( p \) solutions for \( x^p - x = y^2 \). We have proved that \( \sigma_1^* F \) has exactly \( p\left(\frac{p}{2} + 1\right) + 1 \) fixed points, so

\[
\text{Tr}(\sigma_1^* F)^* = -\left(\frac{r \mathbb{F}_p}{p}\right) p.
\] (3.1.2)

Substituting (3.1.2) into (3.1.1) finishes the proof.

\[ \square \]

Remark 3.1.1. If \( p \equiv 3 \mod 4 \), then using similar methods one can compute the order \( |C_{1,0}(\mathbb{F}_p^2)| = p(2p - 1) + 1 \) and prove that \((F^*)^2 + p = 0 \). Consequently, analogous formulas for the traces can be given.

### 3.2. The 5-adic Setting

We now continue in the situation where \( K \) is 5-adic and \( C/K \) is a curve of genus 2 whose \( \ell \)-adic representation has cyclic wild inertia image \( p_\ell(I_K^\sigma) \) of order 5. Recall the notation of 2.9.

### 3.3. Galois Action on the Smooth Model

By Proposition 2.9.1 and 2.8.1, the curve \( C_L/L \) has good reduction, so its minimal regular model \( C'/\mathcal{O}_L \) is smooth. For every finite Galois extension \( K'/K \) containing \( L \), the minimal regular model of \( C_{K'}/K' \) is given by the base change \( C'_{\mathcal{O}_{K'}} \coloneqq C' \times_{\mathcal{O}_L} \mathcal{O}_{K'} \). Every element of \( \text{Gal}(K'/K) \) gives an \( K' \)-semilinear automorphism \( C_{K'} \xrightarrow{\gamma} C_{K'} \), which extends uniquely to an \( \mathcal{O}_{K'} \)-semilinear automorphism \( C'_{\mathcal{O}_{K'}} \xrightarrow{\gamma_{C'}} C'_{\mathcal{O}_{K'}} \) (see, e.g., [22, Corollary 1.2]). Passing to the projective limit shows that each \( \gamma \in \Gamma_K \) induces an \( \mathcal{O}_K \)-semilinear automorphism \( \gamma_{C'} : C'_{\mathcal{O}_K} \xrightarrow{\sim} C'_{\mathcal{O}_K} \). The morphism preserves the special fiber, so we obtain a \( \overline{k}_K \)-semilinear \( \Gamma_K \)-action on \( C'_{\mathcal{O}_{K'}} \).

By functoriality, \( \Gamma_K \) acts on \( H^1_{\text{ét}}(C'_{\mathcal{O}_K}, \mathbb{Q}_\ell) \), and, for every \( n \in \mathbb{Z} \) prime to \( p \), the smooth base change theorem provides an isomorphism of \( \Gamma_K \)-modules

\[
H^1_{\text{ét}}(C_{\mathcal{O}_K}, \mathbb{Z}/n\mathbb{Z}) \cong H^1_{\text{ét}}(C'_{\mathcal{O}_{K'}}, \mathbb{Z}/n\mathbb{Z}).
\] (3.3.1)

We note that every element \( \gamma \in \Gamma_L \) acts on \( C'_{\mathcal{O}_{K'}} = C' \times_{\mathcal{O}_L} \mathcal{O}_{K'} \) as \( \text{id} \times \gamma \). Since \( I_K \) acts trivially on \( \overline{k}_K \), the group \( I_L \) acts trivially on \( C'_{\mathcal{O}_{K'}} \), thus inducing an action of \( I_K/I_L \) on \( C'_{\mathcal{O}_{K'}} \). We obtain a chain of group homomorphisms

\[
I_K/I_L \hookrightarrow \text{Aut}(C'_{\mathcal{O}_{K'}}) \to \text{Aut}(H^1_{\text{ét}}(C'_{\mathcal{O}_{K'}}, \mathbb{Q}_\ell)) \to \text{Aut}(H^1_{\text{ét}}(C_{\mathcal{O}_K}, \mathbb{Q}_\ell)) .
\] (3.3.2)
Proposition 3.3.1. Let $\sigma \in I_{K}^{*}$. The induced automorphism $\sigma_{c'}$ on $C'_{kL}$ descends to $kL$, and $C'_{kL}$ is $kL$-isomorphic to $C_{a,0}$ for some $a \in kL^{\times}$. The automorphism of $C_{a,0}$ induced by $\sigma_{c'}$ is given by $\sigma_{a}^{n} : (x, y) \mapsto (x + r, y)$ with some $r \in \mathbb{F}_{p}$. The image $\rho_{l}(\sigma)$ is nontrivial if and only if $r \neq 0$.

Proof. If $\rho_{l}(\sigma) = \text{Id}$, then $\sigma \in I_{L}$, so $\sigma_{c'}$ is the identity on $C'_{K/k}$ by (3.3.2). In the same way, if $\rho_{l}(\sigma) \neq \text{Id}$, then the class of $\sigma$ in $I_{K}/I_{L}$ has order 5, so it induces an automorphism on $C'_{kK}$ of order 5.

We have seen in Proposition 2.9.4 that the classes of $\sigma$ and $\varphi_{L}$ commute in $\Gamma_{K}/I_{L}$. It follows that they commute as scheme-automorphisms of $C'_{kK}$, which means that $\sigma_{c'}$ descends to a $kL$-automorphism of $C'_{kL}$.

The main arguments for the second part are given in [28] and [13], which we specialize to our situation. Let $\Gamma \simeq C_{5}$ be the image of $I_{K}^{*}$ in $\text{Aut}(C'_{kL})$, and let $\pi : C'_{kL} \to C'_{kL}/\Gamma$ be the quotient map, which is defined over $kL$. As a consequence of the Hurwitz formula, [13, Remark 1.2.(A),(b)] shows that $\Gamma$ fixes a unique closed point $P$ in $C'_{kL}$, and that $C'_{kL}/\Gamma$ has genus zero. Since $\Gamma$ commutes with $(\varphi_{L})_{c'}$, the point $(\varphi_{L})_{c'}(P)$ is also fixed by $\Gamma$, so $(\varphi_{L})_{c'}(P) = P$, meaning that $P$ is a $kL$-rational point. Then $\pi(P)$ is $kL$-rational, so $\pi$ is in indeed a finite $kL$-morphism $C'_{kL} \to \mathbb{P}^{1}_{kL}$ of degree 5 ramified only at $P$. Let $kL(C'_{kL})$ denote the function field of $C'_{kL}$, then $kL(C'_{kL})$ is a rational function field over $kL$, and we let $y$ be a generator having a (unique) pole at $P$.

Since $kL(C'_{kL})$ is cyclic of order 5, applying Artin–Schreier theory we have $kL(C'_{kL}) = kL(x, y)$ satisfying an equation $x^{5} - x = f$ with $f \in kL(y)$. Furthermore, since the pole of $y$ is the unique branch point of $\pi$, we may suppose that $f \in kL[y]$. Since $C'_{kL}$ has genus 2, we must have $\deg f = 2$. We may further suppose that $f(y) = ay^{2} + c$ with $a, c \in kL$, $a \neq 0$, thus we have a $kL$-isomorphism $C'_{kL} \simeq C_{a,c}$.

With our particular choice of $L/K$ in 2.9, the points of $J(C)[2]$ are rational over $L$. The isomorphism (3.3.1) implies that the points of $J(C)[2]$ are $kL$-rational, which means that the polynomial $x^{5} - x - c$ splits completely over $kL$. By translating $x$ with one of the roots we find that $C'_{kL} \simeq C_{a,0}$ as $kL$-schemes.

Lastly, every $\gamma \in \Gamma$ fixes $y$, so $x - \gamma(x)$ is a root of $X^{5} - X = 0$, thus giving $\gamma = \sigma_{a}^{n}$ for some $r \in \mathbb{F}_{5}$, and $r = 0$ if and only if $\gamma$ is trivial. $\square$

Proposition 3.3.2. We fix $\sigma \in I_{K}^{*}$. Let $a \in kL^{\times}$ and $r \in \mathbb{F}_{5}$ be as in Proposition 3.3.1. For every $m, n \in \mathbb{Z}$ we have

$$\text{Tr} \rho_{l}(\sigma_{c'}^{m} \varphi_{L}^{n}) = \begin{cases} \left(\frac{a}{kL}\right)^{n} 5^{\frac{n[kL : \mathbb{F}_{5}]}{2}} & \text{if } n[kL : \mathbb{F}_{5}] \text{ is even and } 5 \nmid m, \\
\left(\frac{a}{kL}\right)^{n} 4 \cdot 5^{\frac{n[kL : \mathbb{F}_{5}]}{2}} & \text{if } n[kL : \mathbb{F}_{5}] \text{ is even and } 5 \mid m, \\
\left(\frac{a}{kL}\right)^{n} 5^{\frac{n[kL : \mathbb{F}_{5}]+1}{2}} & \text{if } n[kL : \mathbb{F}_{5}] \text{ is odd.} \end{cases}$$

Proof. By Proposition 3.3.1, the automorphism induced by $\sigma$ on $C_{a,0}$ is given by $\sigma_{a}^{n} : (x', y') \mapsto (x' + r, y')$. From the classical theory of the Frobenius actions on the étale cohomology group we know that the morphism $F_{q} : (x', y') \mapsto (x'^{qL}, y'^{qL})$ of $C_{a,0}$ induces the action of $\varphi_{L}$ on $H^{1}_{\text{ét}}(C'_{kK}, \mathbb{Q}_{\ell})$. 
We fix a square root $\sqrt{a} \in \overline{k}_K$. Then there is a $\overline{k}_K$-isomorphism $C_{1,0} \to C_{a,0}$ given by $(x, y) \mapsto (x, \frac{y}{\sqrt{a}})$. Using this isomorphism we compute that the $\overline{k}_K$-automorphism on $C_{1,0}$ induced by $\sigma_a$ descends to $\mathbb{F}_5$ and is exactly $\sigma_1$. Similarly, $F_q$ induces $F^{[k_L: \mathbb{F}_5]} \circ \iota$ on $C_{1,0}$ if $(\frac{a}{k_L}) = -1$ or $F^{[k_L: \mathbb{F}_5]}$ if $(\frac{a}{k_L}) = 1$.

Therefore, 

$$\text{Tr} \rho_i(\sigma^m \varphi^m_L) = \left(\frac{a}{k_L}\right)^n \cdot \text{Tr} \left(\sigma_1^m \circ F^{n[k_L: \mathbb{F}_5]}\right)^*.$$ 

The desired formulas follow from Lemma 3.1.1. 

3.4. Square Classes of Differences of Weierstrass Roots

Let $Y^2 = P(X)$ be a Weierstrass equation defining $C/K$ with $P \in K[X]$ unitary of degree 5 as in Proposition 2.10.1. In particular, $A_5 = 1$. Any element $\sigma \in I_K^w$ for which $\rho_1(\sigma)$ is nontrivial acts transitively on the roots of $P$. We fix a root $\alpha_1 \in M$ of $P$, then the other roots are $\alpha_i := \sigma^{i-1}(\alpha_1)$. Following Proposition 3.3.1, the exists $a \in k_L^\times$ such that $C_{k_L} \simeq C_{a,0}$ over $k_L$, and $\sigma$ induces $\sigma_a^r \in \text{Aut}(C_{a,0})$ for some $r \in \mathbb{F}_5^\times$. We note that the curve $C_{a,0}$ is $k_L$-isomorphic to the curve defined by the equation $y^2 = x^5 - a^4x'$, where $y' = a^3y$ and $x' = ax$. We have $\sigma_a^r \cdot (x', y') \mapsto (x' + ar, y')$.

Proposition 3.4.1. The following properties hold:

1. The valuation of $\alpha_i - \alpha_j$ is the same for every $i \neq j$;
2. Assume that $[k_L : \mathbb{F}_5]$ is odd. There exists $\sigma \in I_K^w$ such that $(\frac{a}{k_L}) = 1$. In this case, $\alpha_1 - \sigma(\alpha_1) \in (L^\times)^2$.

Proof. (1) Since $C_L/L$ has good reduction by Proposition 2.8.1, there exists an affine variable change over $L$ which transforms $Y^2 = P(X)$ into a Weierstrass equation with coefficients in $O_L$ and an invertible discriminant (see [19, Lemme 3]). An affine transformation modifies all $v_L(\alpha_i - \alpha_j)$ by adding the same constant $v$. The new discriminant has zero valuation so we must have $v_L(\alpha_i - \alpha_j) + v = 0$ for all $i \neq j$.

(2) The existence of $\sigma$ such that $(\frac{a}{k_L}) = 1$ follows from $(\frac{r}{k_L}) = (\frac{2}{5})$.

The extension $H/K$ from 2.9 is at most tamely ramified, so $\sigma$ acts trivially on it. By Proposition 2.9.1, the extension $L/H$ is Galois, so $\sigma$ acts on $L$. Then, $\sigma$ induces an $L$-semilinear automorphism of $C_L/L$.

The action of $\sigma$ on the function field $K(X, Y)$ with $Y^2 = P(X) \in K[X]$ is trivial. Applying the change of variables $X = X' + \alpha_1$ gives the equation

$$Y^2 = P'(X') := X'(X' - \alpha_2 + \alpha_1) \cdots (X' - \alpha_5 + \alpha_1) \in M[X'].$$

The $\sigma$-action extends $M$-semilinearly to $M(X, Y) = M(X', Y)$ and

$$\sigma(X') = X' - \alpha_2 + \alpha_1.$$

With $P$ as in Proposition 2.10.1, we have $40 \mid e(L/K)v_K(\Delta(P))$ by Proposition 2.9.3. Let $\varpi_L$ be any uniformizer of $L$ and $\delta := \varpi_L^{e(L/K)v_K(\Delta(P))}$. After applying another change of variables $Y = \delta^3Y''$, $X' = \delta^2X''$ we obtain

$$Y''^2 = P''(X'') := X'' \left(X'' - \frac{\alpha_2 - \alpha_1}{\delta^2}\right) \cdots \left(X'' - \frac{\alpha_5 - \alpha_1}{\delta^2}\right),$$

where $\delta^2 \equiv 1 \pmod{40}$. 

 Argentine Mathematical Society
and $\sigma(X'') = X'' - \frac{\alpha_2 - \alpha_1}{\delta^2}$. The formula (2.3.2) gives

$$v_L(\Delta(P'')) = v_L(\delta^{-100} \cdot \delta^{60} \Delta(P)) = e(L/K)v_K(\Delta(P)) - 40v_L(\delta) = 0.$$ 

For all $i \neq j$, applying part (1) gives

$$v_L\left(\frac{\alpha_i - \alpha_j}{\delta^2}\right) = \frac{1}{20}v_L(\Delta(P)) - 2v_L(\delta) = 0.$$

It follows that $Y''^2 = P''(X')$ defines a smooth model $\mathcal{W}/\mathcal{O}_L$ of $C_L/\mathcal{L}$, which is unique up to isomorphism. Its reduction $\mathcal{W}_{k_L}/k_L$ must be $k_L$ isomorphic to the curve $C_{a,0}/k_L$, defined by $y^2 = x^5 - a^4x'$. Let $x''$ denote the class of $X''$ in the function field of $\mathcal{W}_{k_L}$. By construction, the points at infinity of both of these models are fixed by the $k_L$-linear automorphisms induced by $\sigma$. Since on each curve there is a unique such fixed point (proven in [13]), there must be an affine variable change $y'' = ay' x'' = bx' + c$ for some $a, b, c \in k_L$. Then $b^5 = a^2$, so $b$ is a square in $k_L$.

On one hand, as pointed out in 3.4, we have

$$\sigma(x'') = b\sigma(x') + c = bx' + bar + c,$$

and on the other hand, from the construction of $P''$, we have

$$\sigma(x'') = bx' + c + \left(\frac{\alpha_1 - \alpha_2}{\delta^2} \mod m_L\right).$$

Thus, the class of $\frac{\alpha_1 - \alpha_2}{\delta^2}$ in $k_L$ is $bar$, which is a square, so $\alpha_1 - \alpha_2 \in (L^\times)^2$. \hfill $\square$

**Proposition 3.4.2.**

1. We have $H \subset M$.
2. For all $k \neq l$, the element $\alpha_k - \alpha_l$ is a square in $L(\zeta_8)$.

**Proof.** For (2), by replacing $\sigma$ with some power, without loss of generality we may assume that $k = 1, l = 2$. Applying (2.2.2) gives

$$-\beta = \Delta(P) = 2^8 \prod_{i < j} (\alpha_i - \alpha_j)^2 = 2^8(\alpha_1 - \alpha_2)^{20} \prod_{i < j} \left(\frac{\alpha_i - \alpha_j}{\alpha_1 - \alpha_2}\right)^2. \quad (3.4.1)$$

The wild ramification group $I^w(M/K)$ acts trivially on $M^\times/U^1_M$, so

$$\frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1} = \sum_{k=0}^{i-2} \sigma^k(\alpha_2 - \alpha_1) \equiv i - 1 \mod m_M.$$ 

Then

$$\prod_{i < j} \left(\frac{\alpha_i - \alpha_j}{\alpha_1 - \alpha_2}\right)^2 \equiv \prod_{i < j} (j - i)^2 \equiv (288)^2 \equiv -1 \mod m_M.$$ 

Since $U^1_M$ is 8-divisible, it follows that $\beta \in (M^\times)^4$. In particular, $M$ contains all the 4th roots of $\beta$, thus (1) holds. Recall that $\beta \in (L^\times)^8$, thus $(\alpha_1 - \alpha_2)^4 \in (L^\times)^8$. It follows that $\alpha_1 - \alpha_2$ is a square in $L(\zeta_8)^\times$, thus proving (2). \hfill $\square$

**Remark 3.4.1.** Proposition 3.4.2 must be contrasted with Proposition 3.4.1. Unless $L = L(\zeta_8)$, only half of the differences $\alpha_i - \alpha_j$ are squares in $L$. 


Proposition 3.4.3. For any discriminant $\Delta$ of $C/K$ we have
$$v_K(\Delta) \equiv a(\rho_\ell) \mod 2.$$  

Proof. This is derived from [17]. First, $v_K(\Delta) \equiv v_K(\Delta_{\text{min}}) \mod 2$ for $\Delta_{\text{min}}$ associated to a so-called minimal equation. Then, using [17, Prop. 1, Thm. 1] we have $v_K(\Delta_{\text{min}}) - a(\rho_\ell) = m - 1 + \frac{d-1}{2}$ where $m$ is the number of irreducible components of the special geometric fiber of the minimal regular model of $C/K$ and $d$ is a geometric invariant of $C/K$ defined in [17, §5.2]. Finally, for each possible geometric type of the minimal regular model Liu computes $d$. In our case, $m$ is 1, 3, 4, 5, 9, 11, or 13 and $d = 1$ for each value of $m$, except $d = 3$ when $m = 4$. □

4. Maximal Inertia Action Over 5-adic Fields  

We continue in the setting of 3.2.

Proposition 4.0.4. The following are equivalent:
1. $v_K(\Delta)$ is odd for any discriminant $\Delta$ of $C/K$;
2. The extension $M/K$ is totally ramified and $\text{Gal}(M/K) \simeq F_5$;
3. $\rho_\ell(I_K) \simeq C_5 \rtimes C_8$;
4. $a(C/K)$ is odd.

Proof. Proposition 2.9.3 gives (1) $\Leftrightarrow$ (3), and Proposition 3.4.3 gives (1) $\Leftrightarrow$ (4). Proposition 2.9.1 shows that $\rho_\ell(I_K)$ has a quotient isomorphic to the inertia subgroup of $\text{Gal}(M/K)$. Then 2.8 shows that (2) implies (3). Suppose (3), then $L/K$ has ramification index 40. By 2.7, the ramification index of $M/K$ is at least 20. Statement (2) now follows from Proposition 2.9.2. □

4.1. Maximal Ramification Hypothesis  

From now on we suppose that $\rho_\ell(I_K) \simeq C_5 \rtimes C_8$. The complex Weil–Deligne representation associated to $\rho_\ell$ is given by the complex Weil representation $\rho := \rho_\ell|_{W_K \otimes \mathbb{Q}_\ell}$ and the trivial monodromy operator.

Proposition 4.1.1. The extension $L/K$ is totally ramified, and $[L : M] = 2$, $[M : H] = 5$, and $[H : K] = 4$.

Proof. It follows from Proposition 3.4.2.(1) that $H \subset N \cap M$. Proposition 4.0.4 shows that $M/K$ is totally ramified of degree 20 and that $[H : K] = 4$. Therefore, $M/H$ is totally ramified of degree 5, and $N \cap M = H$. From Proposition 4.0.4 we also see that $[N : H] = 2$ and that $L/K$ has ramification index 40, so $[L : K] = [H : K][N : H][M : H] = 40$. It follows that $L/K$ is totally ramified. □

Proposition 4.1.2. In the notation of [11], we have
$$\text{Gal}(L(\zeta_8)/K) \simeq \begin{cases} 
C_5 \rtimes C_8 & \text{if } [k_K : \mathbb{F}_5] \text{ is even}, \\
C_5^2 \cdot F_5 & \text{if } [k_K : \mathbb{F}_5] \text{ is odd}.
\end{cases}$$

Proof. The inertia subgroup $I(L(\zeta_8)/K) \subset \text{Gal}(L(\zeta_8)/K)$ is isomorphic to $C_5 \rtimes C_8$ and has index at most 2 (from Propositions 2.9.1 and 4.1.1).
It remains to show that if $L(\zeta_8)/L$ is nontrivial, then $\text{Gal}(L(\zeta_8)/K) \simeq C_2^2 \cdot F_5$. In this case we have $\text{Gal}(L(\zeta_8)/M) \simeq C_2^2$ since $L/M$ is totally ramified of degree 2. It follows from Proposition 4.0.4 that $\text{Gal}(L(\zeta_8)/K)$ is an extension of $F_5$ by $C_2^2$. The extension cannot be split, because otherwise $\text{Gal}(L(\zeta_8)/K)$ would have $C_2^2 \times C_4$ as a 2-Sylow subgroup, which has exponent 4 and therefore has no element of order 8. In order to identify $\text{Gal}(L(\zeta_8)/K)$ as $C_2^2 \cdot F_5$ by using [11] we are left to show that the extension $G$ is non-central, i.e. that the subgroup $C_2^2 \subset G$ which identifies with $\text{Gal}(L(\zeta_8)/M) \subset \text{Gal}(L(\zeta_8)/K)$ is non-central. Indeed, $\text{Gal}(L(\zeta_8)/M)$ cannot be central because $\text{Gal}(L/K)$ is non-Galois.

**Proposition 4.1.3.** Under the hypothesis of 4.1 the following statements hold:

1. The representation $\rho$ is irreducible;
2. There exists characters $\chi$ and $\chi'$ of $W_H$ such that
   
   $$\rho|_{W_H} \simeq \chi \oplus \chi^{-1}(-1) \oplus \chi' \oplus \chi'^{-1}(-1);$$

3. If $\chi$ is any of the four direct summands in (4.1.1), then
   
   $$\rho \simeq \text{Ind}_{W_H}^{W_K} \chi,$$

and the Artin conductor $a(\chi)$ is even.

**Proof.** We observe that every irreducible representation of $C_5 \rtimes C_8$ necessarily has dimension 1 or 4 (see, e.g., [11]). It follows that $\rho|_{I_K}$ is irreducible since it cannot be a direct sum of 1 dimensional representations. Thus, (1) holds.

The extension $L/H$ is the compositum of the $C_5$-extension $M/H$ and the quadratic extension $N/H$, so $\text{Gal}(L/H) \simeq C_{10}$. It follows that $LK^{ur}/H$ is abelian. Therefore, $\rho|_{W_H}$ has abelian image and splits into 1-dimensional factors

$$\rho|_{W_H} \simeq \chi_1 \oplus \chi_2 \oplus \chi_3 \oplus \chi_4.$$  

Frobenius reciprocity gives a nontrivial morphism of representations

$$\text{Ind}_{W_H}^{W_K} \chi_1 \rightarrow \rho.$$  

Since $\rho$ is irreducible, the morphism is surjective and, in fact, is an isomorphism because $\dim \text{Ind}_{W_H}^{W_K} \chi_1 = 4 = \dim \rho$. Thus, (3) holds.

Since $\rho$ is wildly ramified, by using an explicit construction of the induced representation we observe that $\chi_1$ must be wildly ramified.

The twisted representation $\rho(\frac{1}{2})$ is symplectic with respect to the Weil pairing, so, in particular, the dual of $\rho$ is $\rho^* \simeq \rho(1)$ and $\det \rho = \chi_{ur}^{-2}$. Then (4.1.2) gives

$$\rho|_{W_H} \simeq (\rho|_{W_H})^*(-1) \simeq \chi_1^{-1}(-1) \oplus \chi_2^{-1}(-1) \oplus \chi_3^{-1}(-1) \oplus \chi_4^{-1}(-1).$$

The wild ramification of $\chi_1$ implies that $\chi_1 \not\simeq \chi_1^{-1}(-1)$, so we may suppose that $\chi_2 \simeq \chi_1^{-1}(-1)$. We then have $\chi_4 \simeq \chi_3(-1)$. Posing $\chi = \chi_1$ and $\chi' = \chi_3$ gives (2).

By Proposition 4.0.4, $a(C/K)$ is odd. Since $H/K$ is totally tamelyramified of degree 4, from [26, §10.(a2)] we have $a(C/K) = a(\rho) = a(\chi) + 3$. 

**Proposition 4.1.4.** Each point of $J(C)[4]$ is rational over $L(\zeta_8)$.
Proof. Let $Y^2 = P(X)$ be as in Proposition 2.10.1, and let $\alpha_1, \ldots, \alpha_5 \in \overline{K}$ be the roots of $P$, so that $M = K(\alpha_1, \ldots, \alpha_5)$. Let $\tilde{M} := \mathbb{Q}(\sqrt{-1}, \alpha_1, \ldots, \alpha_5) \subset M$. Then, $C$ and $J(C)$ are defined over $\tilde{M}$, and it follows from [35, Remark 4.2] that
\[
\tilde{M}(J(C)[4]) = \tilde{M}\left(\left(\sqrt{\alpha_i - \alpha_j}\right)_{i < j}\right).
\]
The proposition now follows from Proposition 3.4.2.(2).

Corollary 4.1.1. The map $\rho(\varphi_{L(\zeta_5)})$ is given as multiplication by the scalar $\sqrt{q_L(\zeta_5)}$. As an immediate consequence, the twisted representation $\rho(\frac{1}{2})$ is trivial on $W_L(\zeta_5)$.

Proof. Since $\rho(\varphi_{L(\zeta_5)})$ is central in $\text{Im}(\rho)$ by Proposition 2.9.4, it acts as multiplication by a scalar $z \in \mathbb{C}^\times$. From (4.1.1) we see that $z = z^{-1}q_L(\zeta_5)$, so $z = \pm \sqrt{q_L(\zeta_5)}$. We note that $\sqrt{q_L(\zeta_5)}$ is always an integral power of 5, thus, in particular, $z \equiv \pm 1 \mod 4$. On the other hand, Proposition 4.1.4 implies that $\rho_2(\varphi_{L(\zeta_5)}) \in \text{Aut}_{\mathbb{Z}_2}(H^1_{et}(C_{\overline{K}}, \mathbb{Z}_2))$ satisfies $\rho_2(\varphi_{L(\zeta_5)}) \equiv \text{Id} \mod 4$. We therefore conclude that $z = \sqrt{q_L(\zeta_5)}$. □

5. Computation of Root Numbers

We assume the hypotheses of 3.2 and 4.1 and prove our main result.

Theorem 5.0.1. Let $a_6$ be as in Proposition 2.10.1, and let $\Delta$ be the discriminant associated to any Weierstrass equation defining $C/K$. The root number of $C/K$ is given by
\[
w(C/K) = (-1)^{[k_K: \mathbb{F}_5]} \cdot \left(\frac{\nu_K(a_6)}{k_K}\right) \cdot (\Delta, a_6)_K.
\]

Let $\psi_k : K \to \mathbb{C}^\times$ be the additive character from 1.1. For the general theory and the formulas of root numbers the reader may refer to [26].

5.1. Root Number of an Induced Representation

We have $\rho = \text{Ind}_{W_H}^{W_{K}} \chi$ from Proposition 4.1.3, so the formula [26, §11.(e2)] gives
\[
w(C/K) = w(\chi_k \circ \text{Tr}_{K/H}) \cdot w(\text{Ind}_{W_H}^{W_K} 1, \psi_k). \quad (5.1.1)
\]

Lemma 5.1.1. We have $w(\text{Ind}_{W_H}^{W_K} 1, \psi_k) = -1$.

Proof. The representation $\text{Ind}_{W_H}^{W_K} 1$ is isomorphic to the regular representation of $\text{Gal}(H/K) \simeq C_4$. Let $\chi_4 : W_K \to \mathbb{C}^\times$ denote a totally ramified character of order 4 such that $\ker \chi_4 = W_H$. We then have a decomposition
\[
\text{Ind}_{W_H}^{W_K} 1 \simeq 1 \oplus \chi_4^2 \oplus \chi_4 \oplus \chi_4^{-1}, \quad (5.1.2)
\]
and thus multiplicativity of root numbers [26, §11.(e1)] gives
\[
w(\text{Ind}_{W_H}^{W_K} 1, \psi_k) = w(\chi_4^2, \psi_k) \cdot w(\chi_4 \oplus \chi_4^{-1}, \psi_k).
\]
The properties from [26, §12 Lemma] give
\[
w(\chi_4 \oplus \chi_4^{-1}, \psi_k) = \chi_4(\theta_K(-1)),
\]
where $\theta_K$ is Artin’s reciprocity map. We have $\chi_4(\theta_K(-1)) = 1$ exactly when $-1$ is a 4th power in $K^\times$, so
\[
 w(\chi_4 \oplus \chi_4^{-1}, \psi_k) = (-1)^{|k_K:F_k|}. \]
In order to compute $w(\chi_4^2, \psi_k)$ we apply the formula \[1, (8.7.1)\] with $\beta = 1$ there and $\tau(\chi_4^2, \psi_k) = -G_{[k_K:F_k]}(\chi_4^2) = (-\sqrt{5})^{[k_K:F_k]}$ (we use \[2, \text{Thm. 11.5.2}\]), which gives
\[
 w(\chi_4^2, \psi_k) = (-1)^{|k_K:F_k|+1}, \]
thus completing the proof of the lemma. \hfill \Box

5.2. Connection with a Weierstrass Equation

Let $Y^2 = P(X)$ be the Weierstrass equation for $C/K$ from Proposition 2.10.1. We fix a root $\alpha_1 \in M$ of $P$, then $M = H(\alpha_1)$. Let $\chi$ be as in Proposition 4.1.3, and let $\sigma \in I_H$ be an element such that
\[
 \chi(\sigma) = e^{\frac{2\pi i}{4}}. \tag{5.2.1} \]
It follows that $\sigma$ restricts to a generator of $\text{Gal}(M/H) \simeq C_5$. Let $\alpha := \sigma^{-1}(\alpha_1)$ be the roots of $P$, and let $d_{\alpha_1, \chi} := N_{M/H}(\alpha_1 - \alpha_2)$. We have $N_{M/H}(\alpha_1) = -a_6$ and
\[
 v_M(\alpha_1) = v_H(N_{M/H}(\alpha_1)) = v_H(a_6) = 4v_K(a_6). \tag{5.2.2} \]
Since $a(\chi)$ is even by Proposition 4.1.3.(3), applying Corollary 1.4.1 (with $K = H$ there) gives (recall the notation $\approx$ from 1.3)
\[
 w(\chi, \psi_k \circ \text{Tr}_{H/K}) \approx \chi \circ \theta_H \left( v_M(\alpha_1) \cdot N_{M/H}(\alpha_1) \right)^{-1} \cdot \chi \circ \theta_H(d_{\alpha_1, \chi}) \approx \chi \circ \theta_H(-4v_K(a_6)a_6)^{-1} \cdot \chi \circ \theta_H(d_{\alpha_1, \chi}). \tag{5.2.3} \]
Recall that $\det \rho = \chi_{ur}^{-2}$. Let $t : W_K^{ab} \to W_H^{ab}$ be the transfer map. Deligne’s determinant formula \[10, 508\] gives
\[
 \chi_{ur}^{-2} = \det \text{Ind}_{W_K}^{W_H} \chi = \det \text{Ind}_{W_K}^{W_H} 1 \cdot \chi \circ t. \]
Composing with $\theta_K$ and taking into account the decomposition (5.1.2) gives
\[
 || \cdot ||_{K^\times}^2 = \chi_4^2 \circ \theta_K \cdot (\chi \circ \theta_H)|_{K^\times}. \]
Since $-4v_K(a_6)a_6 \in K^\times$ and $|| \cdot ||_{K^\times} \approx 1$, the above gives
\[
 \chi \circ \theta_H(-4v_K(a_6)a_6) \approx \chi_4^2 \circ \theta_K(-4v_K(a_6)a_6). \tag{5.2.4} \]
Since $-\beta$ is a norm from $K(\sqrt{3})$, we have $\chi_4^2 \circ \theta_K(-\beta) = 1$. Therefore, $\chi_4^2 \circ \theta_K$ is equal to the Hilbert symbol $(\beta, \cdot)_K$, since both are quadratic ramified characters trivial on $-\beta$. Since $\beta$ differs from any discriminant $\Delta$ of $C/K$ by a square in $K^\times$, we have $(\beta, \cdot)_K = (\Delta, \cdot)_K$. Applying this to (5.2.4) together with the formula \[24, V.(3.4)\] gives
\[
 \chi \circ \theta_H(-4v_K(a_6)a_6) \approx \left(\frac{v_K(a_6)}{k_K}\right) \cdot (\Delta, a_6)_K. \tag{5.2.5} \]
Plugging (5.2.5) into (5.2.3) we obtain
\[
 w(\chi, \psi_k \circ \text{Tr}_{H/K}) \approx \left(\frac{v_K(a_6)}{k_K}\right) \cdot (\Delta, a_6)_K \cdot \chi \circ \theta_H(d_{\alpha_1, \chi}). \tag{5.2.6} \]
Lemma 5.2.1. If $[k_K : \mathbb{F}_5]$ is even, then $\chi \circ \theta_H(d_{\alpha_1, \chi}) \approx 1$.

Proof. Here we have $L(\zeta_8) = L$. Then Proposition 3.4.2.(2) implies that

$$\alpha_1 - \alpha_2 \in \mathcal{N}_{L(\zeta_8)/M}(L(\zeta_8)^\times),$$

thus $d_{\alpha_1, \chi}$ is a norm from $L(\zeta_8)^\times$. Since $\rho(\frac{1}{2}) = \text{Ind}_{W_H}^W(\chi(\frac{1}{2}))$, Corollary 4.1.1 implies that $\chi(\frac{1}{2}) \circ \theta_H$ is trivial on $\mathcal{N}_{L(\zeta_8)/H}(L(\zeta_8)^\times)$. Then,

$$\chi \circ \theta_H(d_{\alpha_1, \chi}) = ||d_{\alpha_1, \chi}||_{H}^{-\frac{1}{2}} \cdot (\chi(\frac{1}{2}) \circ \theta_H)(d_{\alpha_1, \chi}) = ||d_{\alpha_1, \chi}||_{H}^{-\frac{1}{2}} \approx 1. \quad (5.2.7)$$

Lemma 5.2.2. Suppose that $[k_K : \mathbb{F}_5]$ is odd. Let $a \in k_L$ and $r \in \mathbb{F}_5$ be associated to $\sigma$ as in Proposition 3.3.1. For every geometric Frobenius lift $\varphi_L \in W_L$, we have

$$\chi(\varphi_L) = -\left(\frac{ar}{k_L}\right)\sqrt{q_K}.$$  

Proof. Recall from Proposition 4.1.1 that $L/K$ is totally ramified, so $k_L = k_K$. Since $[k_K : \mathbb{F}_5]$ is odd, $q_K = q_L = \sqrt{q_{L(\zeta_8)}}$, and $(\frac{q_L}{k_L})$ is the restriction of $(\frac{q_{L(\zeta_8)}}{k_L})$ to $\mathbb{F}_5$.

Let $\chi'$ be the other character appearing in Proposition 4.1.3. From Proposition 3.3.2 we have $\text{Tr} \rho(\sigma) = -1$, which, together with (5.2.1), forces

$$\chi'(\sigma) \in \left\{ (e^{\frac{2\pi i}{5}})^2, (e^{\frac{2\pi i}{5}})^3 \right\}. \quad (5.2.8)$$

Corollary 4.1.1 implies that the eigenvalues of $\rho(\varphi_L)$ are $\pm \sqrt{q_L}$. From Proposition 3.3.2 we have $\text{Tr} \rho(\varphi_L) = 0$, so there exists some $w = \pm 1$ such that

$$\chi(\varphi_L) = w\sqrt{q_L} \quad \text{and} \quad \chi'(\varphi_L) = -w\sqrt{q_L}. \quad (5.2.9)$$

Using (5.2.1), (5.2.8), and (5.2.9) together with a classical formula for Gauss sums [2, §1.1] gives

$$\text{Tr} \rho(\sigma \varphi_L) = w\sqrt{q_L} \left( e^{\frac{2\pi i}{5}} + (e^{\frac{2\pi i}{5}})^4 - (e^{\frac{2\pi i}{5}})^2 - (e^{\frac{2\pi i}{5}})^3 \right) = w\sqrt{5q_L}.$$

It now follows from Proposition 3.3.2 that $w = -\left(\frac{ar}{k_L}\right)$.

5.3. Choosing $\chi$

We assume that $[k_K : \mathbb{F}_5]$ is odd, then $[k_L : \mathbb{F}_5]$ is also odd. Although the root number $w(\chi, \psi_k \circ \Theta_{H/K})$ does not depend on the choice of the character $\chi$ in Proposition 4.1.3. (3), in order to carry out a detailed computation we will need to fix a particular $\chi$. Depending on whether $a$ is a square in $k_L^\times$, we may choose $\sigma$ and, consequently, $\chi$ so that $\left(\frac{ar}{k_L}\right) = 1$ and that we still have (5.2.1).

Lemma 5.3.1. If $[k_K : \mathbb{F}_5]$ is odd and $\chi$ is as in 5.3, then $\chi \circ \theta_H(d_{\alpha_1, \chi}) \approx -1$.

Proof. Applying Lemma 5.2.2 for the chosen $\chi$ gives

$$\chi(\varphi_L) = -\sqrt{q_K}.$$  

On the other hand, Proposition 3.4.1.(2) tells us that $\alpha_1 - \alpha_2$ is a square in $L$, so there exists some $b \in L$ such that $\alpha_1 - \alpha_2 = \mathcal{N}_{L/M}(b)$. Proposition 3.4.1. (1) and Proposition 4.1.1 give

$$v_L(b) = v_M(\alpha_1 - \alpha_2) = \frac{1}{20}v_M(\Delta(P)) = v_K(\Delta(P)).$$
It now follows from Proposition 4.0.4 that \( v_L(b) \) is odd. The restriction \( \chi|_{W_L} \) is unramified, so the above discussion shows that

\[
\chi \circ \theta_H(d_{a_1, \chi}) = \chi \circ \theta_L(b) = \chi(\varphi_L)^{v_L(b)} = (-\sqrt{q_K})^{v_L(b)} \approx -1.
\]

**Proof of Theorem 5.0.1.** When \([k_K : \mathbb{F}_5]\) is even we use Lemma 5.2.1, and when \([k_K : \mathbb{F}_5]\) is odd we choose \( \chi \) as in 5.3 and use Lemma 5.3.1 in order to obtain \( \chi \circ \theta_H(d_{a_1, \chi}) \approx (-1)^{[k_K: \mathbb{F}_5]} \). Plugging the latter into (5.2.6) gives

\[
w(\chi, \psi_k \circ \text{Tr}_{H/K}) \approx (-1)^{[k_K: \mathbb{F}_5]} \cdot \left( \frac{v_K(a_6)}{k_K} \right) \cdot (\Delta, a_6)_K. \tag{5.3.1}
\]

Combining (5.3.1) and Lemma 5.1.1 into (5.1.1) proves the relation \( \approx \) between the two sides of the formula of Theorem 5.0.1. Since both sides take values in \( \{1, -1\} \), the theorem holds (see 1.3).

\[\□\]

### 5.4. An Example

This is [21, genus 2 curve 896875.a.896875.1]. Let \( C/\mathbb{Q} \) be the hyperelliptic curve defined by

\[
Y^2 = P(X) := X^5 + \frac{5}{4}X^4 - \frac{5}{2}X^3 - \frac{5}{4}X^2 + \frac{5}{2}X + \frac{1}{4}.
\]

Its discriminant is \( \Delta = -5^5 \cdot 7 \cdot 41 \), and a smooth model over \( \mathbb{Z}_2 \) can be given.

Good reduction over 2 gives \( w(C/\mathbb{Q}_2) = 1 \). At the infinite place we have \( w(C/\mathbb{R}) = (-1)^g = 1 \).

Over 7 the reduction is semi-stable, the singular point of the special fiber is given by \( X = 5, Y = 0 \), and we have \( P(X) \equiv (X - 5)^2H_7(X) \) mod 7 with \( H_7(X) = X^3 + 6X^2 + X + 4 \) separable over \( \mathbb{F}_7 \). We apply the Brumer–Kramer–Sabitova formula [5, Lemma 6.7] to compute \( w(C/\mathbb{Q}_7) = -(\frac{H_7(5)}{47}) = -(\frac{4}{7}) = -1 \).

Over 41 the reduction is again semi-simple, the singular point is at \( X = 12, Y = 0 \), and we have \( P(X) \equiv (X - 12)^2H_{41}(X) \) mod 41 with \( H_{41}(X) = X^3 + 15X^2 + 29X + 21 \) separable over \( \mathbb{F}_{41} \). Similarly as above, we compute \( w(C/\mathbb{Q}_{41}) = -(\frac{H_{41}(12)}{41}) = -(\frac{34}{41}) = 1 \).

We observe that \( P(X + 1) \) is Eisenstein over \( \mathbb{Z}_5 \), so the \( \Gamma_{Q_5} \)-action on \( J(C)[2] \) is wildly ramified. Thus, \( \rho_\ell \) is wildly ramified for every \( \ell \neq 5 \), and \( C/\mathbb{Q}_5 \) has potentially good reduction by Proposition 2.8.1. The equation \( Y^2 = P(X + 1) \) satisfies the conditions of Proposition 2.10.1 with \( a_6 = \frac{5}{4} \), so Theorem 5.0.1 applies to give

\[
w(C/\mathbb{Q}_5) = \left( -5^5 \cdot 7 \cdot 41, \frac{5}{4} \right)_{Q_5} = -1.
\]

The global root number is then \( w(C/\mathbb{Q}) = 1 \), which is compatible with the Hasse–Weil and the BSD conjectures since both analytic and Mordeil-Weil ranks of \( J(C)/K \) are 2 (see [21]).
Acknowledgements

I thank my doctoral thesis advisors Adriano Marmora and Rutger Noot as well as Kęstutis Česnavičius and Takeshi Saito for their remarks and suggestions concerning the manuscript. I also thank Jeff Yelton for answering my questions about his results on the splitting fields of the 4-torsion of Jacobians. The study presented in this paper constitutes a part of my thesis.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

References

[1] Abbes, A., Saito, T.: Local Fourier transform and epsilon factors. Compos. Math. 146(6), 1507–1551 (2010). https://doi.org/10.1112/S0010437X09004631

[2] Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi Sums (Canadian Mathematical Society Series of Monographs and Advanced Texts), pp. xii+583. Wiley, New York (1998)

[3] Bisatt, M.: Explicit root numbers of abelian varieties. Trans. Am. Math. Soc. 372(11), 7889–7920 (2019). https://doi.org/10.1090/tran/7926

[4] Bisatt, M.: Root number of the jacobian of $y^2 = x^p + a$, (2021). arXiv: 2102.05720 [math.NT]

[5] Brumer, A., Kramer, K., Sabitova, M.: Explicit determination of root numbers of abelian varieties. Trans. Am. Math. Soc. 370(4), 2589–2604 (2018). https://doi.org/10.1090/tran/7116

[6] Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron Models (Ergeb. Math. Grenzgeb. (3)), vol. 21, pp. x+325. Springer, Berlin (1990) https://doi.org/10.1007/978-3-642-51438-8

[7] Chai, C.-L.: Néron models for semiabelian varieties: Congruence and change of base field. Asian J. Math. 4(4), 715–736 (2000). https://doi.org/10.4310/AJM.2000.v4.n4.a1

[8] Coppola, N.: Wild galois representations: A family of hyperelliptic curves with large inertia image (2020). arXiv:2001.08287 [math.NT]

[9] Dokchitser, T., Dokchitser, V.: Root numbers of elliptic curves in residue characteristic 2. Bull. Lond. Math. Soc. 40(3), 516–524 (2008). https://doi.org/10.1112/blms.bdn034

[10] Deligne, P. Les constantes des équations fonctionnelles des fonctions L. In: Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp; ser. Lecture Notes in Math., vol. 349, pp. 501–597. Springer, Berlin (1972)

[11] Dokchitser, T.: GroupNames. (Feb. 2020), [Online]. http://groupnames.org
[12] Hasse, H.: Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. J. Reine Angew. Math. 172, 37–54 (1935). https://doi.org/10.1515/crll.1935.172.37

[13] Homma, M.: Automorphisms of prime order of curves. Manuscripta Math. 33(1), 99–109 (1980/81). https://doi.org/10.1007/BF01298341

[14] Kobayashi, S.: The local root number of elliptic curves with wild ramification. Math. Ann. 233(3), 609–623 (2002). https://doi.org/10.1007/s002080200318

[15] Kraus, A.: Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. Manuscripta Math. 69(4), 353–385 (1990). https://doi.org/10.1007/BF02567933

[16] Liu, Q.: Courbes stables de genre 2 et leur schéma de modules. Math. Ann. 295(2), 201–222 (1993). https://doi.org/10.1007/BF01444884

[17] Liu, Q.: Conducteur et discriminant minimal de courbes de genre 2. Compos. Math. 94(1), 51–79 (1994)

[18] Liu, Q.: Modèles minimaux des courbes de genre deux. J. Reine Angew. Math. 453, 137–164 (1994). https://doi.org/10.1515/crll.1994.453.137

[19] Liu, Q.: Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. Trans. Am. Math. Soc. 348(11), 4577–4610 (1996). https://doi.org/10.1090/S0002-9947-96-01684-4

[20] Liu, Q.: Algebraic Geometry and Arithmetic Curves (Oxford Graduate Texts in Mathematics), vol. 6, pp. xvi+576. Oxford University Press, Oxford (2002)

[21] The LMFDB Collaboration: The L-functions and modular forms database. http://www.lmfdb.org (2021)

[22] Liu, Q., Tong, J.: Néron models of algebraic curves. Trans. Am. Math. Soc. 368(10), 7019–7043 (2016). https://doi.org/10.1090/tran/6642

[23] Mumford, D.: Tata Lectures on Theta. II (Progress in Mathematics), vol. 43, pp. xiv+272. Birkhäuser Boston, Inc., Boston (1994)

[24] Neukirch, J. Algebraic Number Theory (Grundlehren Math. Wiss.), vol. 322, pp. xviii+571. Springer, Berlin (1999). https://doi.org/10.1007/978-3-662-03983-0

[25] Namikawa, Y., Ueno, K.: The complete classification of fibres in pencils of curves of genus two. Manuscripta Math. 9, 143–186 (1973). https://doi.org/10.1007/BF01297652

[26] Rohrlich, D. E.: Elliptic Curves and the Weil–Deligne Group, in Elliptic Curves and Related Topics, ser. CRM Proc. Lecture Notes, vol. 4, pp. 125–157. Amer. Math. Soc., Providence (1994)

[27] Rohrlich, D.E.: Galois theory, elliptic curves, and root numbers. Compositio Math. 100(3), 311–349 (1996)

[28] Roquette, P.: Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik. Math. Z. 117, 157–163 (1970). https://doi.org/10.1007/BF01109838

[29] Sabitova, M.: Root numbers of abelian varieties. Trans. Am. Math. Soc. 359(9), 4259–4284 (2007). https://doi.org/10.1090/S0002-9947-07-04148-7

[30] Serre, J.-P.: Rigidité du foncteur de jacobi d’échelon $n \geq 3$, Appendix to A. Grothendieck, Techniques de construction en géométrie analytique, X. Construction de l’espace de Teichmüller, Séminaire Henri Cartan, 1960/61, no. 17

[31] Serre, J.-P.: Local Fields (Graduate Texts in Mathematics). Springer, New York (1977)
[32] Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. 2(88), 492–517 (1968)

[33] Stichtenoth, H.: Algebraic Function Fields and Codes (Graduate Texts in Mathematics), Second, vol. 254, pp. xiv+355. Springer, Berlin (2009)

[34] Silverberg, A., Zarhin, Y.G.: Inertia groups and abelian surfaces. J. Number Theory 110(1), 178–198 (2005). https://doi.org/10.1016/j.jnt.2004.05.015

[35] Yelton, J.: Images of 2-adic representations associated to hyperelliptic Jacobians. J. Number Theory 151, 7–17 (2015). https://doi.org/10.1016/j.jnt.2014.10.020

Lukas Melninkas
IRMA, UMR 7501
Université de Strasbourg et CNRS
7 rue René Descartes
67000 Strasbourg
France
e-mail: lmelninkas@gmail.com

Received: May 28, 2022.
Accepted: March 14, 2023.