# Wild Galois representations of elliptic and hyperelliptic curves

By

NIRVANA COPPOLA


School of Mathematics
UNIVERSITY OF BRISTOL

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of DOCTOR OF PHILOSOPHY in the Faculty of Science.

MARCH 7, 2021

# Abstract

In this thesis we investigate the Galois representation attached to an algebraic curve over a local field. In particular, we consider elliptic and hyperelliptic curves with very bad reduction, i.e. which acquire good reduction over a wildly ramified extension.

It is a well-known fact that the primes at which an elliptic curve may acquire good reduction over a wildly ramified extension are 2 and 3. For such primes, a classification of the restriction to inertia of the Galois representation is well understood in the literature; in particular the image of inertia is a finite group, which can be either cyclic or non-abelian. However, less is known about the full Galois action. In this work we give an explicit and algorithmic description of the Galois representations which occur in these cases, with a particular focus on the curves with non-abelian inertia image.

For a hyperelliptic curve of genus $g$, the primes of wild reduction are at most $2g+1$. In this work we consider the family of hyperelliptic curves which have potentially good reduction at $2g+1$, assuming this is a prime, and the largest possible image of inertia. We will see how the result on the Galois representation attached to one such curve is a direct generalisation of the corresponding result for elliptic curves.

## Dedication and acknowledgements

I wish to thank all the people that helped me throughout my PhD, in particular during the writing of the three papers on which this thesis is based. Namely, all my gratefulness goes to Prof. Tim Dokchitser, who suggested a topic that I found interesting and entertaining at the same time, and guided me towards finding all the results; to Dr Davide Lombardo, who always took the time to read and comment my preprints and gave me important and useful suggestions; to Pip Goodman and Simone Museli, who have always been available for exchanging ideas; and finally to all those who suggested applications in related areas of mathematics, among them Dr Matt Bisatt and Prof. Vladimir Dokchitser.

This work was supported by EPSRC studentship No 1961436.

## Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

Nirvana Coppola, 11/01/2021

# TABLE OF CONTENTS

CHAPTER 1

# INTRODUCTION

One of the invariants associated to an algebraic curve $X$ defined over a number field $K$ is the canonical Galois representation. This is a $2g$-dimensional representation of the absolute Galois group of $K$, where $g$ is the genus of the curve, which encodes information on the Galois action on the Tate modules of the Jacobian of $X$.

Understanding this invariant has several consequences, since it can be used to compute, for example, the conductor and the root number of the curve, and it is a tool for the study of other problems such as the inverse Galois problem.

The most natural family of algebraic curves one can consider is that of elliptic curves, in fact these curves are also abelian varieties, and the Galois representation is defined by looking at the Galois action on torsion points of the curve itself. However, a complete and effective description of this representation is non-trivial even in this case, and it cannot be found in literature.

A natural approach to the study of Galois representations is by considering separately the local behaviour at each completion of $K$. Indeed, the Galois representation attached to an elliptic (or higher genus) curve defined over a local field is primarily determined by its reduction type; moreover the absolute Galois group of the completion of a number field $K$ at some prime $\mathfrak{p}$ of $K$ fits into the absolute Galois group of $K$, as it is isomorphic to a decomposition group of $\mathfrak{p}$. Therefore we will consider a curve defined over a $p$-adic field, that is a finite extension of $\mathbb{Q}_p$, for a fixed prime $p$, and for $\ell$ different from $p$, we will study the $\ell$-adic Galois representation attached to this curve, i.e. on the $\ell$-adic Tate module.

For elliptic curves, this problem is well understood if the reduction at $p$ is good, multiplicative, or potentially multiplicative (that is additive and acquiring multiplicative reduction over a finite extension of the base field). In the case of additive potentially good reduction, the Galois representation varies, depending on the curve acquiring good reduction over a tamely or wildly

ramified extension of the base field. The tame case can be easily dealt with, using an algorithmic approach that essentially consists in point-counting over several finite extensions of the base field. However, this approach is not useful in the wild case, and a more systematic study is needed.

The first step is to consider the restriction to the inertia subgroup of the $\ell$-adic Galois representation, which has finite image, isomorphic to either a cyclic group of order $2,3,4$ or $6$, the dicyclic group of 12 elements, the quaternion group, or $\mathrm{SL}_2(\mathbb{F}_3)$; in particular, wild reduction only occurs when $p = 2$ or $3$, and the inertia image is either cyclic or non-abelian. Then we consider the family of curves with given inertia image and we study and classify all the possible Galois representations which can occur.

The non-abelian case is the first one tackled in this thesis. Imposing such a condition on inertia gives more constraints to the full Galois action, and it can be easily shown that in all three non-abelian cases there are at most two possibilities for the Galois representation. In order to distinguish between these two, it is necessary to compute the trace of a certain explicit element, and this can be done after exhibiting a model with good reduction for the curve over an explicit finite extension of the base field.

The remaining cases, although apparently more similar to the tame cases, are more subtle: since the inertia image is small, there are less constraints to the full Galois action. In particular, if the size of the inertia image is 2, we can only conclude that a quadratic twist of the curve has good reduction. Nonetheless, the techniques employed in the non-abelian cases can be adapted to find an explicit answer also in the wild cyclic cases at $p = 3$ and for the case $p = 2$ and inertia image of size 4.

The classification presented here is completely explicit, hence it provides an algorithm for the computation of the Galois representation in each case. This algorithm has been implemented in a MAGMA function by the author, in the non-abelian cases.

For higher genus curves, there are few available results on Galois representations, which largely rely on recent developments in the study of regular models of curves over local fields. A natural generalisation of elliptic curves is given by hyperelliptic curves and, in the case of potentially good reduction, only the restriction to inertia is completely understood. However, if we restrict to the family of hyperelliptic curves of genus $g$ which have potentially good reduction at $p = 2g + 1$ (assuming this is a prime), which have the largest possible inertia image, we find that the Galois representation behaves in exactly the same way as in the non-abelian 3-adic case; in fact, the result for elliptic curves is just a corollary of the result that we will prove for this family of hyperelliptic curves.

The structure of this thesis is as follows. In Chapter 2 we introduce the notation and review all the results known in literature, concerning elliptic curves with good, multiplicative, potentially multiplicative, and tame potentially good reduction. In Chapters 3 and 4, we focus on the non-abelian cases for $p = 3$ and 2 respectively. In Chapter 5, we consider all the remaining wild cases. Finally, in Chapter 6 we generalise the main theorem of Chapter 3 to the family of hyperelliptic

curves described above.

CHAPTER 2

# PRELIMINARIES

In this chapter, we introduce the terminology and classic results concerning elliptic curves over a local field. We show how the different reduction types of an elliptic curve lead to substantially different behaviour in the Galois representation and give known results that are already present in literature. The main (but not only) references are [10, 15, 23, 24].

## 2.1 Elliptic curves: definitions

Let $K$ be any field and let $E$ be an elliptic curve defined over $K$, i.e. a smooth projective curve of genus 1, with a specified $K$-rational point $O$. As explained in [23, III,§1-3], such a curve can be expressed via a Weierstrass equation, that is an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{2.1}$$

We have that $O = [0:1:0]$ and the coefficients $a_i$ are in $K$. Using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ we will simply identify $E$ with its affine Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.2}$$

where $O$ is still the (unique) point at infinity.

To a Weierstrass equation we can associate the $c$-invariants $c_4$, $c_6$, the discriminant $\Delta$ and the $j$-invariant, as defined in op. cit. We recall that a Weierstrass equation is the equation of an elliptic curve (in particular, of a smooth curve) if and only if its discriminant is non-zero.

Let $\overline{K}$ be an algebraic closure of $K$. Two Weierstrass equations define the same elliptic curve up to $\overline{K}$-isomorphism, if they are obtained one from the other via a change of coordinates of the

form

$$\begin{cases} x &= u^2x' + r, \\ y &= u^3y' + u^2sx' + t, \end{cases} \tag{2.3}$$

where $u,r,s,t \in \overline{K}$ of $K$ and $u \neq 0$. If $u,r,s,t \in K$, then we obtain two elliptic curves which are isomorphic over $K$; in this case, we identify the two curves and we call the two corresponding equations two different Weierstrass models for the same curve.

Observe that, under a change of coordinates as in Equation (2.3), the invariants are scaled as follows:

$$\begin{cases} c_4 &= u^4c_4', \\ c_6 &= u^6c_6', \\ \Delta &= u^{12}\Delta', \\ j &= j'; \end{cases} \tag{2.4}$$

in particular, the $j$-invariant is an invariant of the elliptic curve up to $\overline{K}$-isomorphism.

The set of $\overline{K}$-rational points on an elliptic curve (including the point at infinity $O$), form an abelian group which we denote by $E(\overline{K})$, with identity element given by $O$. For details on the definition of the group law on $E(\overline{K})$ see [23, III, §2]; observe in particular that the group law is defined over $K$, i.e. it is given by rational functions with coefficients in $K$. For each intermediate field $K \subseteq L \subseteq \overline{K}$, we have that the subset of $L$-rational points is also a subgroup of $E(\overline{K})$, which we denote by $E(L)$.

If $K$ has characteristic different from 2 or 3, any elliptic curve over $K$ can be expressed via a short Weierstrass equation, i.e. an equation of the form

$$y^2 = x^3 + a_4x + a_6. \tag{2.5}$$

In the rest of this thesis, unless the characteristic of $K$ is 2 or 3, we will always implicitly fix a short Weierstrass equation for an elliptic curve over $K$.

## 2.2 Torsion, Tate modules and Galois representations

Let $P \in E(\overline{K})$. If there exists a positive integer $m$ such that $[m]P = O$, by which we mean $P$ added to itself $m$ times is equal to the point at infinity, we say that $P$ is an $m$-torsion point of $E$. If $m$ is minimal with this property, we say that $P$ has order $m$. In particular, $O$ has order 1 and is an $m$-torsion point for any $m$. We denote by $E[m]$ the subset of $E(\overline{K})$ given by all $m$-torsion points. It is easy to check that $E[m]$ is a subgroup of $E(\overline{K})$. Moreover, if the characteristic of $K$ is zero or coprime to $m$, we have an isomorphism (see [23, III, §6, Corollary 6.4]):

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2. \tag{2.6}$$

It is possible to compute explicitly the coordinates of $m$-torsion points, for a given integer $m$. This is done via the $m$-division polynomials, which are polynomials defined over $K$ whose roots are the abscissas of the $m$-torsion points. We denote by $K(E[m])$ the minimal field extension of $K$ which contains the $x$- and $y$-coordinates of a Weierstrass model of all $m$-torsion points of $E$, or equivalently, where all $m$-torsion points are defined. Then the extension $K(E[m])/K$ is Galois. Moreover, by the isomorphism in Equation (2.6), we have that if we fix a basis for $E[m]$ as a $\mathbb{Z}/m\mathbb{Z}$-module, we obtain the field $K(E[m])$ by simply adjoining the coordinates of the two elements in the basis.

The $m$-division polynomials for $m \in \{2,3\}$ are simple to compute from the coefficients of a short Weierstrass equation and will be used in Chapters 3 and 4. Let $E/K : y^2 = x^3 + a_4x + a_6$. Then the 2 and 3-division polynomials are, respectively:

$$\phi_2(x) = x^3 + a_4x + a_6, \tag{2.7}$$

$$\phi_3(x) = 3x^4 + 6a_4x^2 + 12a_6x - a_4^2. \tag{2.8}$$

Now let $\ell$ be a prime, different from the characteristic of $K$ if this is non-zero. For all $n$, there is a well-defined and surjective map: $E[\ell^{n+1}] \to E[\ell^n]$ given by multiplication by $\ell$. This construction makes $\{E[\ell^n], n \in \mathbb{N}\}$ into a projective system. We define the $\ell$-adic Tate module of $E$ as the following inverse limit:

$$T_\ell(E) = \varprojlim_n E[\ell^n]. \tag{2.9}$$

Notice that we have $T_\ell(E) \cong \mathbb{Z}_\ell^2$. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the absolute Galois group of $K$, and let $P = (x_P, y_P) \in E(\overline{K})$. We define

$$P^\sigma = \sigma(P) = (\sigma(x_P), \sigma(y_P)). \tag{2.10}$$

Then $P^\sigma \in E(\overline{K})$, since $E$ is defined over $K$. Moreover, the action of $\mathrm{Gal}(\overline{K}/K)$ on $E(\overline{K})$ is linear, since the group law is defined over $K$; in particular for any integer $m$ we have

$$([m]P)^\sigma = [m]P^\sigma, \tag{2.11}$$

therefore the Galois action restricts to the torsion subgroups, and we have a representation

$$\overline{\rho_{E,m}} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]) \tag{2.12}$$

which we call the mod $m$ Galois representation attached to $E$. If $m$ is coprime to $\mathrm{char}(K)$, or $\mathrm{char}(K) = 0$, after we fix a basis for $E[m]$ over $\mathbb{Z}/m\mathbb{Z}$, we can view this representation as a homomorphism: $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Furthermore, taking the inverse limits produces an action on the $\ell$-adic Tate module for each prime $\ell$, which we call the $\ell$-adic Galois representation attached to $E$, denoted as follows:

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell). \tag{2.13}$$

We can and will view $\rho_{E,\ell}$ as a representation with image in a vector space over an algebraically closed field, by taking the tensor product $\mathrm{Aut}(T_\ell(E)) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$, where $\overline{\mathbb{Q}}_\ell$ is a fixed algebraic closure of $\mathbb{Q}_\ell$. We fix for each $\ell$ an embedding $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$, in order to identify the elements of $\overline{\mathbb{Q}}_\ell$ with complex numbers. We will specify the image of finitely many elements of $\overline{\mathbb{Q}}_\ell$ under such embedding, when needed, in the following chapters.

## 2.3 Elliptic curves over local fields

From this moment on, we assume that $K$ is a non-archimedean local field of characteristic 0. Equivalently, $K$ is isomorphic to a $p$-adic field, for a prime number $p$, that is a finite extension of $\mathbb{Q}_p$. Such a field has a maximal unramified extension, which we denote by $K^{nr}$ (see [21, III, §5] for details). We denote by $\pi_K$ a uniformiser of $K$, by $\mathcal{O}_K$ its ring of integers and by $k$ the residue field $\mathcal{O}_K/(\pi_K)$, which is a finite field of characteristic $p$. Moreover, let us fix a valuation $v$ on $K$, normalised so that $v(\pi_K) = 1$. Let $n = [k : \mathbb{F}_p]$, then $n$ is equal to the absolute inertia degree of $K$, i.e. the inertia degree $f_{K/\mathbb{Q}_p}$ of the extension $K/\mathbb{Q}_p$. Finally let $\overline{k}$ be an algebraic closure of $k$, then $\overline{k}$ is isomorphic to the residue field of $K^{nr}$.

We have that $\mathrm{Gal}(\overline{K}/K)$ has a normal subgroup given by the inertia subgroup $I_K$, which we identify with $\mathrm{Gal}(\overline{K}/K^{nr})$. The quotient $\mathrm{Gal}(\overline{K}/K)/I_K$ is isomorphic to $\mathrm{Gal}(K^{nr}/K)$, which is in turn isomorphic to $\mathrm{Gal}(\overline{k}/k)$. This is a procyclic group generated by the Frobenius automorphism, which acts as

$$x \mapsto x^{|k|}. \tag{2.14}$$

We call arithmetic Frobenius of $K$, and denote by $\mathrm{Frob}_K$, any element of $\mathrm{Gal}(\overline{K}/K)$ which maps to the Frobenius automorphism under the quotient map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{nr}/K) \cong \mathrm{Gal}(\overline{k}/k)$. There is more than one choice for $\mathrm{Frob}_K$, as it is only well-defined up to inertia, so it will be necessary to fix a specific choice for $\mathrm{Frob}_K$ in each case we consider. This will be done explicitly in each case.

Let $E$ be an elliptic curve over $K$ and let us fix a Weierstrass equation for $E$ with coefficients in $\mathcal{O}_K$. This can always be done by an appropriate change of variables as in Equation (2.3). Among all the equations with integer coefficients, we call one such that the valuation $v(\Delta)$ of the discriminant is minimal a minimal model for the curve, and the corresponding discriminant $\Delta_{\min}$ is called a minimal discriminant. In particular, $\Delta_{\min}$ is well-defined up to units of $K$, so it is not unique, but its valuation is. Let us fix a minimal model for $E/K$ and consider the equation defined over $k$ which we obtain by reducing all the coefficients modulo $(\pi_K)$. This curve reduces to a smooth (hence elliptic) curve if and only if the reduction of the discriminant of a minimal model is non-zero, or equivalently if and only if $v(\Delta_{\min}) = 0$, for any choice of the minimal model. In this case, we say that $E/K$ has good reduction. Otherwise, the reduced curve is singular, with exactly one singular point, which can be a node or a cusp. We say that $E/K$ has multiplicative reduction in the first case, and additive reduction otherwise. Furthermore, we say that a curve

with multiplicative reduction has split reduction if the tangent lines at the nodes are defined over the residue field, and non-split otherwise. These conditions can be checked by looking at the valuation of the $c$-invariants of a minimal model, namely we have that:

- $E/K$ has multiplicative reduction if $v(\Delta_{\min}) > 0$ and $v(c_{4,\min}) = 0$;
- $E/K$ has additive reduction if $v(\Delta_{\min}) > 0$ and $v(c_{4,\min}) > 0$.

For a proof, see [23, VII, §5, Proposition 5.1]. We will make great use of the following results, which can be found in [23, VII, §5, Propositions 5.4 and 5.5].

**Proposition 2.1.** *Let $E/K$ be an elliptic curve.*

- *Let $K'/K$ be an unramified extension. Then the reduction type of $E$ over $K$ is the same as the reduction type over $K'$.*
- *Let $K'/K$ be a finite extension. If $E$ has either good or multiplicative reduction over $K$, then it has the same reduction type over $K'$.*
- *There exists a finite extension $K'/K$ such that $E$ has either good or multiplicative reduction over $K'$.*

For a curve $E/K$ with additive reduction, we say that $E$ has potentially good reduction if it acquires good reduction over a finite extension, and potentially multiplicative reduction otherwise.

**Proposition 2.2.** *Let $E/K$ be an elliptic curve, then $E$ has potentially good reduction if and only if its $j$-invariant has non-negative valuation.*

## 2.4 Known results

### 2.4.1 Elliptic curves with good reduction

Let $K$ be as in the previous section and let $E$ be an elliptic curve defined over $K$. In this work we address the $\ell$-adic Galois representation attached to $E$, where $\ell$ is a prime different from $p$. We will see how the $\ell$-adic Galois representation changes substantially depending on the reduction type of $E/K$.

**Theorem 2.3** (Criterion of Néron-Ogg-Shafarevich)**.** *Let $E/K$ be an elliptic curve. Then the following are equivalent:*

- *$E/K$ has good reduction.*
- *The restriction of $\overline{\rho_{E,m}}$ to $I_K$ is trivial for all integers $m > 1$ that are relatively prime to $p$.*
- *The restriction of $\rho_{E,\ell}$ to $I_K$ is trivial for all primes $\ell \neq p$.*

- *The restriction of $\overline{\rho_{E,m}}$ to $I_K$ is trivial for infinitely many integers $m \geq 1$ that are relatively prime to $p$.*

**Proof.** See [23, VII, §7, Theorem 7.1]. ■

An immediate consequence of this Criterion is the following result.

**Corollary 2.4.** *Let $E/K$ be an elliptic curve. Then $E$ has potentially good reduction if and only if $I_K$ acts on $T_\ell(E)$ through a finite quotient for some (or equivalently all) primes $\ell \neq p$.*

**Proof.** See [23, VII, §7, Corollary 7.3]. ■

These two results give a first, rough way to classify Galois representations of elliptic curves with different reduction types. Indeed we have that:

- the image of inertia is trivial if and only if the curve has good reduction;
- the image of inertia is finite if and only if the curve has potentially good reduction;
- the image of inertia is infinite if and only if the curve has (potentially) multiplicative reduction.

In the good reduction case, since the image of inertia is trivial, we have that $\rho_{E,\ell}$ factors through the quotient $\mathrm{Gal}(\overline{K}/K)/I_K$, which is generated by $\mathrm{Frob}_K$. So we only need to compute $\rho_{E,\ell}(\mathrm{Frob}_K)$ to fully understand the Galois action. Moreover, the action of $\mathrm{Frob}_K$ is independent of the particular choice of Frobenius in this case (we will see later that this is no longer true if, for example, $E/K$ only has potentially good reduction). As is shown in [22, IV, §2.3], the image of $\mathrm{Frob}_K$ is always diagonalisable (at least in $\overline{\mathbb{Q}}_\ell$), so it is enough to compute its eigenvalues to uniquely determine its action. This can be done using the following result (see [22, IV, §1.3]).

**Theorem 2.5.** *Let $\ell \neq p$ be a prime. The characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_K)$ is given by*

$$F(T) = T^2 - aT + q, \tag{2.15}$$

*where $q = |k|$ and $a = q + 1 - |\tilde{E}(k)|$, and $\tilde{E}$ denotes the reduction of the curve $E$ to $k$.*

Observe that, although $\rho_{E,\ell}(\mathrm{Frob}_K)$ is a matrix with coefficients in $\mathbb{Q}_\ell$, the theorem above shows that its characteristic polynomial is defined over $\mathbb{Z}$ and independent of $\ell$, as long as $\ell \neq p$.

### 2.4.2 Elliptic curves with potentially good reduction: the image of inertia and the tame case

Let $K$ be as in the previous sections and $E/K$ be an elliptic curve with potentially good reduction. Let $\ell$ be a prime different from $p$ and $\rho_{E,\ell}$ be the $\ell$-adic Galois representation attached to $E$. We fix a Weierstrass equation for $E$, which we assume to be minimal. We denote by $\Delta$ the discriminant of this equation, and by $c_4, c_6$ the $c$-invariants.

First of all, we observe that $\rho_{E,\ell}$ is independent of $\ell$. Indeed we have the following result.

**Lemma 2.6.** *Let $E/K$ be an elliptic curve with potentially good reduction and let $\ell$ be a prime different from $p$. Then the kernel of $\rho_{E,\ell}$ is the same for all $\ell$, and the character of $\rho_{E,\ell}|_{I_K}$ has values in $\mathbb{Z}$ which are independent of $\ell$.*

**Proof.** See [19, Theorem 2 (ii)]. ■

We know from Corollary 2.4 that $I = \rho_{E,\ell}(I_K)$ is finite, but this can be made more precise. So, our first step is to determine the group $I$. Recall by Proposition 2.1 that the reduction types of $E$ over $K$ and $K^{nr}$ are the same. Let $L$ be the minimal finite extension of $K^{nr}$ over which $E$ acquires good reduction. Then it follows from Theorem 2.3 that the representation $\rho_{E,\ell}$ factors through the quotient $I_K/I_L$, which is isomorphic to $\mathrm{Gal}(L/K^{nr})$: notice that the subgroup $I_L$ is normal in $I_K$, so $L/K^{nr}$ is Galois. This group is also finite, and since we chose $L$ to be minimal, it injects into $\mathrm{Aut}(T_\ell(E))$ and it is isomorphic to $I$.

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K^{nr}) & \xrightarrow{\quad\rho_{E,\ell}\quad} & \mathrm{Aut}(T_\ell(E)) \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}(L/K^{nr}) & \end{array}$$

Furthermore, there is an injection of $\mathrm{Gal}(L/K^{nr})$ into $\mathrm{Aut}(\tilde{E}_L)$, where $\tilde{E}_L$ is the reduction of a minimal equation for $E$ over $L$ (for more details see [19, proof of Theorem 2]). In particular, the image of inertia is one of

$$C_2, C_3, C_4, C_6,$$
$$C_3 \rtimes C_4 \text{ only when } p = 3,$$
$$Q_8, \mathrm{SL}_2(\mathbb{F}_3) \text{ only when } p = 2,$$

where $C_n$ is the cyclic group of order $n$, $C_3 \rtimes C_4$ is the only non-abelian semidirect product of $C_3$ and $C_4$, which is also known as the Dicyclic group (see [7]), $Q_8$ is the group of quaternions and $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ given by matrices with determinant 1. This list comes from the following classification of the automorphisms of an elliptic curve defined over a field of characteristic $p$ (see [23, III, §10, proof of Theorem 10.1 and Appendix A, Proposition 1.2(c), Exercise A.1]).

| | $j \neq 0, 1728$ | $j = 1728$ | $j = 0$ |
|---|---|---|---|
| $p \neq 2, 3$ | $C_2$ | $C_4$ | $C_6$ |
| $p = 3$ | $C_2$ | $C_3 \rtimes C_4$ | $C_3 \rtimes C_4$ |
| $p = 2$ | $C_2$ | $SL_2(\mathbb{F}_3)$ | $SL_2(\mathbb{F}_3)$ |

Since these groups all have different orders, if we know the degree of the extension $L/K^{nr}$, we can uniquely determine the Galois group of this extension, hence the structure group of the image of inertia. In order to do so, we follow the work of Kraus, namely [15, Proposition 1, Theorems 1, 2, 3]. These are complete classification theorems that depend on the residue characteristic being 2, 3 or higher.

**Proposition 2.7.** *Let $p \geq 5$. Then $L$ is the only tamely ramified extension of $K^{nr}$ of degree equal to the denominator of $v(\Delta)/12$.*

**Proof.** See [15, Proposition 1]. ■

**Theorem 2.8.** *Let $p = 3$. Then:*

*(a) if $E$ has type $I_0^*$, then $v(\Delta) = 6$ and $I \cong C_2$;*

*(b) if $E$ has type $III$, then $v(\Delta) = 3$ and $I \cong C_4$;*

*(c) if $E$ has type $III^*$, then $v(\Delta) = 9$ and $I \cong C_4$;*

*(d) if $v(\Delta) \equiv 0 \pmod 4$, then $I \cong C_3$;*

*(e) if $v(\Delta) \equiv 2 \pmod 4$ and $E$ has type different from $I_0^*$, then $I \cong C_6$;*

*(f) if $v(\Delta)$ is odd and $E$ has type different from $III$ and $III^*$, then $I \cong C_3 \rtimes C_4$.*

**Proof.** See [15, Theorem 1]. For the definition of the Néron type of an elliptic curve, see [24, IV, §9]. ■

**Theorem 2.9.** *Let $p = 2$. Then:*

*(a) we have $I \cong C_3$ if and only if $E$ has type $IV$ (and then $v(\Delta) = 4$) or $IV^*$ (and then $v(\Delta) = 8$);*

*(b) if $3v(c_4) = v(\Delta)$, then $I \cong C_2$;*

*(c) if $3v(c_4) \geq 12v(2) + v(\Delta)$, then if $3 \mid v(\Delta)$, we have $I \cong C_2$, otherwise if $E$ does not have type $IV$ or $IV^*$ we have $I \cong C_6$.*

*(d) if $v(\Delta) < 3v(c_4) < 12v(2) + v(\Delta)$, let $\Delta^{1/3}$ be a third root of $\Delta$ in $\overline{K}$. Moreover let $A = c_4 - 12\Delta^{1/3}$, $B = c_4^2 + 12c_4\Delta^{1/3} + (12\Delta^{1/3})^2$, $A^{1/2}$ and $B^{1/2}$ respectively a square root of $A, B$ in $\overline{K}$ and $C = 2(c_4 + 6\Delta^{1/3} + B^{1/2})$. Then:*

*(i) if* $3 \mid v(\Delta)$*, and* $A,B,C$ *are squares in* $K^{nr}$*, then* $I \cong C_2$*; if only* $A,B$ *are squares in* $K^{nr}$*, then* $I \cong C_4$*;*

*(ii) if* $3 \mid v(\Delta)$*, and* $A$ *or* $B$ *is not a square in* $K^{nr}$*, then if* $C$ *is a square in* $K^{nr}(A^{1/2},B^{1/2})$ *then* $I \cong C_4$*, otherwise* $I \cong Q_8$*;*

*(iii) if* $3 \nmid v(\Delta)$*, if* $A$ *and* $B$ *are squares in* $K^{nr}(\Delta^{1/3})$ *then* $I \cong C_3$ *if* $E$ *has type* $IV$ *or* $IV^*$*, and* $I \cong C_6$ *otherwise. If* $A$ *or* $B$ *is not a square in* $K^{nr}(\Delta^{1/3})$*, then* $I \cong \mathrm{SL}_2(\mathbb{F}_3)$*.*

**Proof.** See [15, Theorems 2, 3]. ■

This last theorem allows us to recover the image of inertia by just looking at a minimal equation for $E$, however it is not very helpful for computing $L$. A more general result, which is less explicit but will be useful in Chapter 4, is the following, see [19, Corollary 2 to Theorem 2].

**Theorem 2.10.** *We have* $L = K^{nr}(E[m])$*, where* $m$ *is any integer with* $m \geq 3$ *and* $(p,m) = 1$*. The Galois group* $\mathrm{Gal}(\overline{K}/L)$ *is equal to* $\ker(\rho_{E,\ell}\big|_{I_K})$ *for any* $\ell \neq p$*.*

In particular, we will use this theorem with $p = 2$ and $m = 3$, and we will study the extension given by adjoining 3-torsion to $K$ in order to describe $\rho_{E,\ell}$.

In the rest of this section, we focus on the case where $E$ acquires good reduction over a tamely ramified extension. By the results above, this happens if $p \geq 5$, or $p = 3$ and $E$ has Néron type $I_0^*$, $III$ or $III^*$, or $p = 2$ and $E$ has Néron type $IV$ or $IV^*$.

The case of tame potentially good reduction has been studied extensively in literature. The following results allow us to compute $\rho_{E,\ell}$ for any $E$ that satisfies one of the conditions we just listed.

**Remark 2.11.** *Let* $p \geq 3$ *and let* $E$ *have Néron type* $I_0^*$*. Then* $E$ *is a quadratic twist of an elliptic curve with good reduction. Equivalently, we have that* $I = \rho_{E,\ell}(I_K) \cong C_2$*.*

This property comes from Tate's algorithm (see [24, IV, §9]), and we have that such a curve acquires good reduction over $K(\sqrt{\pi_K})$. Let $\chi_\pi$ be the quadratic character of $K(\sqrt{\pi_K})/K$, and let $E_\pi$ be the quadratic twist of $E$ by $K(\sqrt{\pi_K})$, then it is straightforward to check the following identity:

$$\rho_{E_\pi,\ell} \cong \chi_\pi \otimes \rho_{E,\ell}. \tag{2.16}$$

We can compute $\rho_{E_\pi,\ell}$ as in Section 2.4.1, and thus $\rho_{E,\ell}$.

Now let $p$ be any prime and suppose that $E/K$ has tame potentially good reduction, but not Néron type $I_0^*$. Let $e$ be the denominator of $v(\Delta)/12$ and $\pi_K^{1/e}$ be any $e$-th root of the uniformiser $\pi_K$. Then, combining Proposition 2.7 and Theorems 2.8, 2.9, together with Proposition 2.1, we have that $E$ acquires good reduction over:

- $F = K(\pi_K^{1/e})$, if $p \geq 5$, indeed this is a tamely totally ramified extension of $K$ of degree equal to the denominator of $v(\Delta)/12$;

- $F = K(\Delta^{1/4})$ for any 4-th root of $\Delta$ in $\overline{K}$, if $p = 3$, since in this case $E$ has type $III$ or $III^*$ (see Theorem 2.8, cases (b,c));
- $F = K(\Delta^{1/3})$ for any 3-th root of $\Delta$ in $\overline{K}$, if $p = 2$, since in this case $E$ has type $IV$ or $IV^*$ (see Theorem 2.9, cases (a) and (d.iii)).

In all three cases, the degree $[F : K]$ is equal to $e$. Moreover, $e$ is a proper divisor of 12: since the group of automorphisms of an elliptic curve over a field of characteristic $p \geq 5$ is either $C_2$, $C_4$ or $C_6$, the possible values for $e$ are $2, 3, 4, 6$, as we observed at the beginning of this section. The extension $F/K$ is Galois and cyclic if and only if $K$ contains a primitive $e$-th root of unity, $\zeta_e$. Otherwise, the Galois closure of $F/K$ is given by $F(\zeta_e)$ and $\mathrm{Gal}(F(\zeta_e)/K)$ is isomorphic to the dihedral group with $2e$ elements, $D_e$. Observe that we can choose, alternatively, $F = K(\pi_K^{1/e})$ in all cases: all are totally ramified of degree $e$ over $K$ and are Galois if and only if $\zeta_e \in K$.

We first assume that $\zeta_e \in K$, so the field extension $F/K$ is cyclic of order $e \in \{3, 4, 6\}$. Let $u \in \mathcal{O}_K^\times$ be a unit which is not a $e$-th power, and let $F' = K(u^{1/e}\Delta^{1/12})$ if $p \geq 5$, $K((u\Delta)^{1/4})$ if $p = 3$, $K((u\Delta)^{1/3})$ if $p = 2$. Furthermore let $\mathrm{Frob}_F$ and $\mathrm{Frob}_{F'}$ be arithmetic Frobenius elements of $F$ and $F'$ respectively. Then, by [10, Theorem 1], the representation $\rho_{E,\ell}$ is uniquely determined by the characteristic polynomials of $\rho_{E,\ell}(\mathrm{Frob}_F)$ and $\rho_{E,\ell}(\mathrm{Frob}_{F'})$. See also [10, §3] for an explicit application of this theorem.

Now we assume that $\zeta_e \notin K$, so the field extension $F/K$ has dihedral Galois closure given by $F(\zeta_e)$. Moreover let $L$ be the maximal unramified extension of $F(\zeta_e)$, or, equivalently, of $F$. Let $\mathrm{Frob}_F$ and $\mathrm{Frob}_{F(\zeta_e)}$ be arithmetic Frobenius elements of $F$ and $F(\zeta_e)$ respectively, then $\mathrm{Frob}_{F(\zeta_e)}$ is central in $\mathrm{Gal}(L/K)$ and therefore $\rho_{E,\ell}(\mathrm{Frob}_{F(\zeta_e)}) = \lambda\,\mathrm{Id}_2$ is a scalar matrix. On the other hand, $\rho_{E,\ell}(\mathrm{Frob}_{F(\zeta_e)}) = \rho_{E,\ell}(\mathrm{Frob}_F)^2$, since $F(\zeta_e)/F$ is unramified and quadratic. Moreover $\mathrm{Frob}_F$ is not central, so we have, in some basis of $T_\ell(E) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$, that $\rho_{E,\ell}(\mathrm{Frob}_F) = \begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & -\sqrt{\lambda} \end{pmatrix}$. In order to determine $\lambda$, we notice that the determinant of $\rho_{E,\ell}(\mathrm{Frob}_F)$ is equal to $|k|$, so we have $\lambda = -|k|$. So we have

$$\rho_{E,\ell}(\mathrm{Frob}_F) = \begin{pmatrix} \sqrt{-|k|} & 0 \\ 0 & -\sqrt{-|k|} \end{pmatrix}, \tag{2.17}$$

where we identify $\sqrt{-|k|} \in \overline{\mathbb{Q}}_\ell$ with the complex number $i\sqrt{|k|}$.

Now let $\mathrm{Frob}_K$ be the arithmetic Frobenius of $K$ that fixes $F$ point-wise, in other words we choose $\mathrm{Frob}_K = \mathrm{Frob}_F$. We define the following unramified character (i.e. with trivial restriction to inertia):

$$\begin{aligned} \chi : \quad & \mathrm{Gal}(\overline{K}/K) \to \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C} \\ & \mathrm{Frob}_K \mapsto \sqrt{-|k|}. \end{aligned} \tag{2.18}$$

We observe that $\rho_{E,\ell} \otimes \chi^{-1}$ factors through $\mathrm{Gal}(F(\zeta_e)/K)$, with image isomorphic to it. Therefore, as a representation of $\mathrm{Gal}(F(\zeta_e)/K)$, it is faithful, and also irreducible, since $\mathrm{Gal}(F(\zeta_e)/K)$,

hence the image of $\rho_{E,\ell}$, is non-abelian, otherwise it would be the direct sum of two representations of dimension 1, hence it would be abelian.

Now, for $e \in \{3,4,6\}$, the group $D_e$ has only one 2-dimensional irreducible and faithful representation, as can be seen by direct computation or in [7]. To conclude, we have $\rho_{E,\ell} \cong \chi \otimes \psi$, where $\psi$ is the unique irreducible and faithful 2-dimensional representation of $D_e$.

This argument proves the following theorem.

**Theorem 2.12** (Elliptic curves with tame potentially good reduction)**.** *Let $E/K$ be an elliptic curve with tame potentially good reduction, and discriminant of a minimal model $\Delta$.*

*(a) If $p \geq 3$ and $E$ has type $I_0^*$, then $\rho_{E,\ell} = \rho_{E_\pi,\ell} \otimes \chi_\pi$ where $\chi_\pi$ is the quadratic character of $K(\sqrt{\pi_K})/K$, and $E_\pi$ is the quadratic twist of $E$ by $K(\sqrt{\pi_K})$, which has good reduction.*

*(b) If $p \geq 5$ or $p = 3$ and $E$ has type $III$ or $III^*$ or $p = 2$ and $E$ has type $IV$ or $IV^*$, let $e$ be the denominator of $v(\Delta)/12$.*

*(i) If $\zeta_e \in K$, then $\rho_{E,\ell}$ is determined by the characteristic polynomial of the Frobenius elements of $K(\Delta^{1/12})$ and $K(u^{1/e}\Delta^{1/12})$ if $p \geq 5$, $K(\Delta^{1/e})$ and $K((u\Delta)^{1/e})$ if $p = 3$ or 2 for $u \in \mathcal{O}_K^\times$ not a $e$-th power.*

*(ii) If $\zeta_e \notin K$, then $\rho_{E,\ell} = \chi \otimes \psi$, where $\chi$ is the unramified character sending $\mathrm{Frob}_K$ to $\sqrt{-|k|}$ and $\psi$ is the irreducible faithful 2-dimensional representation of the dihedral group $D_e$.*

### 2.4.3 Elliptic curves with (potentially) multiplicative reduction

Let $E/K$ be a curve with multiplicative or additive, potentially multiplicative reduction. Let $c_4, c_6$ be the $c$-invariants of a minimal Weierstrass equation for $E$. Let $\mathrm{Sp}_2$ be the 2-dimensional special representation of $\mathrm{Gal}(\overline{K}/K)$, such that

$$\mathrm{Sp}_2(\mathrm{Frob}_K) = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}, \qquad \mathrm{Sp}_2(\sigma) = \begin{pmatrix} 1 & \tau_\ell(\sigma) \\ 0 & 1 \end{pmatrix} \ \forall \sigma \in I_K, \tag{2.19}$$

where $\tau_\ell$ is the $\ell$-adic tame character, i.e. the only character: $I_K \to \mathbb{Z}_\ell$ such that for $k \in \mathbb{Z}$, $k > 1$, $(\zeta_{\ell^k})$ compatible $\ell^k$-th roots of unity and $\sigma \in I_K$:

$$\sigma(\pi_K^{1/\ell^k}) = \zeta_{\ell^k}^{\tau_\ell(\sigma)} \pi_K^{1/\ell^k}. \tag{2.20}$$

**Theorem 2.13.** *Let $E/K$ have potentially multiplicative reduction. Let $\chi$ be the primitive character of $K(\sqrt{-c_4/c_6})/K$. Then $\rho_{E,\ell} = \chi \otimes \mathrm{Sp}_2$.*

Observe that $E/K$ has split multiplicative reduction if and only if the extension $K(\sqrt{-c_4/c_6})/K$ is trivial, in which case $\chi$ is the trivial character. Otherwise, $E$ acquires split multiplicative reduction over $K(\sqrt{-c_4/c_6})$, which is quadratic over $K$. Moreover, the extension is unramified if $E/K$ has non-split multiplicative reduction, and totally ramified if $E/K$ has additive potentially multiplicative reduction. For a proof see [24, V, §5, Lemma 5.2, Theorem 5.3, Exercise 5.11].

**Proof.** Let $E' = E$ if $E/K$ has split multiplicative reduction, and let $E'$ be the quadratic twist of $E$ by $K(\sqrt{-c_4/c_6})$ otherwise. Then $\rho_{E,\ell} = \chi \otimes \rho_{E',\ell}$, where $\chi$ is trivial if $K(\sqrt{-c_4/c_6}) = K$. By [24, V, §5, Theorem 5.3], $E'$ is isomorphic to a Tate curve (see [24, V, §3] for the definition), and we can use the theory of Tate curves to prove $\rho_{E',\ell} = \mathrm{Sp}_2$. This can be found in [24, V, §5, Exercise 5.13], or it follows from the classification of Weil-Deligne representations and the fact that if $E/K$ has potentially multiplicative reduction, the image of inertia is infinite, see [18, §15]. ■

## 2.5 Examples

The following two examples will be central in Chapters 3, 4 and 5.

**Example 2.14.** *Let $K$ be a local field with residue characteristic 3 and let $k$ be its residue field. Let $E/K$ be an elliptic curve such that the reduction $\tilde{E}$ over $k$ is $y^2 = x^3 - x$. In particular, $E$ has good reduction over $K$. We want to compute the eigenvalues of $\rho_{E,\ell}(\mathrm{Frob}_K)$, for a prime $\ell \neq 3$, as elements of $\mathbb{C}$.*

*First we assume that $k = \mathbb{F}_3$. Then the reduced curve $\tilde{E}$ has the following 4 points over $\mathbb{F}_3$: $\{O,(0,0),(1,0),(2,0)\}$, therefore, in the notation of Theorem 2.5, $a = 0$, $q = 3$ and the roots of $F(T)$, hence the eigenvalues of $\rho_{E,\ell}(\mathrm{Frob}_K)$, are $\pm\sqrt{-3}$. Here we identify $\sqrt{-3}$ with the complex number $i\sqrt{3}$.*

*If $[k : \mathbb{F}_3] = n \geq 1$, then $\rho_{E,\ell}(\mathrm{Frob}_K)$ acts as the $n$-th power of the linear operator described above, so its eigenvalues are $(\pm\sqrt{-3})^n$.*

**Example 2.15.** *Let $K$ be a local field with residue characteristic 2 and let $k$ be its residue field. Let $E/K$ be an elliptic curve such that the reduction $\tilde{E}$ over $k$ is $y^2 + y = x^3$. In particular, $E$ has good reduction over $K$. In this case we want to compute the eigenvalues of $\rho_{E,\ell}(\mathrm{Frob}_K)$, for a prime $\ell \neq 2$, as elements of $\mathbb{C}$.*

*As in the previous case, we first assume that $k = \mathbb{F}_2$. Then we have $\tilde{E}(\mathbb{F}_2) = \{O,(0,0),(0,1)\}$, so in the notation above, $a = 0$ and $q = 2$, giving that the characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_K)$ is $T^2 + 2$, with roots $\pm\sqrt{-2}$. Here we identify $\sqrt{-2}$ with the complex number $i\sqrt{2}$.*

*If $[k : \mathbb{F}_2] = n \geq 1$, then $\rho_{E,\ell}(\mathrm{Frob}_K)$ acts as the $n$-th power of the linear operator described above, so its eigenvalues are $(\pm\sqrt{-2})^n$.*

We now give examples of curves with tame potentially good reduction, one for each subcase of Theorem 2.12.

**Example 2.16.** *Let $E/\mathbb{Q}_7 : y^2 = x^3 + 7^3$. Then $E$ has type $I_0^*$, and acquires good reduction over $F = \mathbb{Q}_7(\sqrt{7})$. More precisely, $E$ is the quadratic twist by $F$ of the curve $E_7/\mathbb{Q}_7 : y^2 = x^3 + 1$. By Theorem 2.5 we have that $\rho_{E_7,\ell}(\mathrm{Frob}_F)$ has eigenvalues $-2 \pm \sqrt{-3}$, where as usual $\sqrt{-3}$ is identified with the complex number $i\sqrt{3}$. By Theorem 2.12 case (a), let $\chi_7$ be the quadratic character of $F/\mathbb{Q}_7$, then $\rho_{E,\ell} = \chi_7 \otimes \rho_{E_7,\ell}$. Since $\rho_{E_7,\ell}$ is unramified (trivial on inertia), the representation $\rho_{E,\ell}$ is completely determined.*

The following example shows concretely how to recover the $\ell$-adic Galois representation from the characteristic polynomial of two suitable Frobenius elements.

**Example 2.17.** *Let $E/\mathbb{Q}_7 : y^2 = x^3 + 7^2$. Then $E$ acquires good reduction over a totally ramified extension of degree 3, for example over $F = \mathbb{Q}_7(7^{1/3})$. Since $7 \equiv 1 \pmod 3$, $\mathbb{Q}_7$ contains the third roots of unity and $F/\mathbb{Q}_7$ is Galois and cyclic. Over $F$, we can define the change of variables*

$$\begin{cases} x &= (7^{1/3})^2 x', \\ y &= 7y', \end{cases} \tag{2.21}$$

*and we obtain a model for the base change $E_F$ of $E$ to $F$ given by $y^2 = x^3 + 1$. Let $\mathrm{Frob}_F$ be the arithmetic Frobenius of $F$, then by the computations in the previous example we have that the eigenvalues of $\rho_{E_F,\ell}(\mathrm{Frob}_F)$ are $-2 \pm \sqrt{-3}$.*

*Let $\mathrm{Frob}_K$ be the arithmetic Frobenius of $K$ that acts as $\mathrm{Frob}_F$, then we have $\rho_{E,\ell} = \psi_1 \oplus \psi_2$, where $\psi_i$ are 1-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_7/\mathbb{Q}_7)$ such that $\psi_1(\mathrm{Frob}_K) = -2 + \sqrt{-3}$ and $\psi_2(\mathrm{Frob}_K) = -2 - \sqrt{-3}$. We fix $\sigma \in I_{\mathbb{Q}_7}$ an element such that, when projected to the quotient $\mathrm{Gal}(F/\mathbb{Q}_7)$, we have $\sigma(7^{1/3}) = \zeta_3 7^{1/3}$, with $\zeta_3$ the third root of unity in $\mathbb{Q}_7$ such that $\zeta_3 \equiv 2 \pmod 7$. We only need to determine $\psi_1(\sigma)$ and $\psi_2(\sigma)$. These are primitive third roots of unity in $\overline{\mathbb{Q}}_\ell$, and one is the inverse of the other, as by the Weil pairing $\det(\rho_{E,\ell}(\sigma)) = 1$. As usual, we fix an embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$, and then we have that $\psi_1(\sigma) \in \left\{\frac{-1\pm\sqrt{-3}}{2}\right\}$. In order to determine which of these two numbers $\psi_1(\sigma)$ is, we fix $F' = \mathbb{Q}_7((3\cdot 7)^{1/3})$, as in Theorem 2.12 case (b.ii).*

**Claim 2.18.** *We have $\mathrm{Frob}_{F'} = \sigma^2 \mathrm{Frob}_F$.*

*In order to prove the claim, we observe that $\sigma^2 \mathrm{Frob}_F$ acts as $\mathrm{Frob}_F$ on the residue field (note both $F$ and $F'$ have the same residue field, namely $\mathbb{F}_7$), so we only need to prove that $\sigma^2 \mathrm{Frob}_F((3\cdot 7)^{1/3}) = (3\cdot 7)^{1/3}$. Note that $\frac{\sigma^2 \mathrm{Frob}_F((3\cdot 7)^{1/3})}{(3\cdot 7)^{1/3}}$ is a third root of unity, so it is sufficient to prove that it reduces to 1 in the residue field. We have*

$$\frac{\sigma^2 \mathrm{Frob}_F((3\cdot 7)^{1/3})}{(3\cdot 7)^{1/3}}) = \frac{\mathrm{Frob}_F(3^{1/3})}{3^{1/3}} \frac{\mathrm{Frob}_F(\zeta_3^2 7^{1/3})}{7^{1/3}} = 9\zeta_3^2, \tag{2.22}$$

*which reduces to $9 \cdot 4 = 1$ in $\mathbb{F}_7$. The first equality holds in $\overline{K}$ and it follows from the facts that $\sigma$ acts trivially on $3^{1/3}$, and that $\sigma$ and $\mathrm{Frob}_F$ commute, since they do when restricted to $F^{nr}$, and $\mathrm{Gal}(F^{nr}/K)$ is the direct product of the two abelian and (pro-)cyclic groups $\mathrm{Gal}(F/K)$ and $\mathrm{Gal}(K^{nr}/K)$.*

*Now, we compute the eigenvalues of $\rho_{E_{F'},\ell}(\mathrm{Frob}_{F'})$, where $E_{F'}$ is the base change of $E$ to $F'$. The change of variables*

$$\begin{cases} x &= ((21)^{1/3})^2 x', \\ y &= 21y', \end{cases} \tag{2.23}$$

*gives the model* $y^2 = x^3 + 1/9$*, which reduces to* $y^2 = x^3 + 4$ *over* $\mathbb{F}_7$*. Applying Theorem 2.5 again, we obtain that the eigenvalues of* $\rho_{E_{F'},\ell}(\mathrm{Frob}_{F'})$ *are* $\frac{5\pm\sqrt{-3}}{2}$*. Therefore we have*

$$\begin{cases} (-2+\sqrt{-3})\psi_1(\sigma)^2 = \dfrac{5+\sqrt{-3}}{2} \\ (-2-\sqrt{-3})\psi_2(\sigma)^2 = \dfrac{5-\sqrt{-3}}{2}, \end{cases} \tag{2.24}$$

*or*

$$\begin{cases} (-2+\sqrt{-3})\psi_1(\sigma)^2 = \dfrac{5-\sqrt{-3}}{2} \\ (-2-\sqrt{-3})\psi_2(\sigma)^2 = \dfrac{5+\sqrt{-3}}{2}. \end{cases} \tag{2.25}$$

*Direct computation shows that only the first system of equalities can hold, with* $\psi_1(\sigma)^2 = \dfrac{-1-\sqrt{-3}}{2}$*, i.e.* $\psi_1(\sigma) = \dfrac{-1+\sqrt{-3}}{2}$ *and* $\psi_2(\sigma) = \dfrac{-1-\sqrt{-3}}{2}$*.*

**Example 2.19.** *Let* $E/\mathbb{Q}_5 : y^2 = x^3 + 5^2$*. Similarly as in the previous example, this curve acquires good reduction over the degree* 3 *totally ramified extension* $F = \mathbb{Q}_5(5^{1/3})$*, with model* $y^2 = x^3 + 1$*. However, the extension* $F/\mathbb{Q}_5$ *is not Galois, so we are in case (b.ii) of Theorem 2.12. Therefore* $\rho_{E,\ell} = \chi \otimes \psi$*, where* $\chi$ *is the unramified character of* $\mathrm{Gal}(\overline{\mathbb{Q}}_5/\mathbb{Q}_5)$ *mapping* $\mathrm{Frob}_K$ *to* $\sqrt{-5}$ *and* $\psi$ *is the only representation of* $S_3$ *which is* 2*-dimensional and irreducible (and faithful).*

CHAPTER 3

# ELLIPTIC CURVES OVER A 3-ADIC FIELD WITH NON-ABELIAN INERTIA ACTION

This chapter is a modified version of the author's paper "Wild Galois Representations: elliptic curves over a 3-adic field", published in Acta Arithmetica ([2]). Here, we compute the Galois representation $\rho_{E,\ell}$ attached to an elliptic curve $E$ over a 3-adic field, which acquires good reduction over a non-abelian extension. We will prove the following result.

**Theorem 3.1.** *Let $E$ be an elliptic curve with potentially good reduction over a 3-adic field $K$, with Weierstrass equation of the form $y^2 = f(x)$ and discriminant $\Delta$. Fix a fourth root $\Delta^{1/4}$ of $\Delta$ and define $F$ to be the compositum of the splitting field of $f$ over $K$ and $K(\Delta^{1/4})$; let $F'$ be the Galois closure of $F/K$.*

*Let $\ell$ be a prime different from 3, and let $\rho_{E,\ell}$ be the $\ell$-adic Galois representation attached to $E$. Suppose that the image of the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ is isomorphic to $C_3 \rtimes C_4$.*

*Let $\chi$ be the unramified character of $\mathrm{Gal}(\overline{K}/K)$ (i.e. trivial on inertia) such that*

$$\chi(\mathrm{Frob}_K) = (\sqrt{-3})^n, \tag{3.1}$$

*where $n = [k : \mathbb{F}_3]$, and let $\psi$ be as follows. If $n$ is even, let $\psi$ be the representation of $\mathrm{Gal}(F'/K)$, which is isomorphic to $C_3 \rtimes C_4$, with character:*

(3.2)

| *class* | 1 | 2 | 3 | 4A | 4B | 6 |
|---|---|---|---|---|---|---|
| *size* | 1 | 1 | 2 | 3 | 3 | 2 |
| $\mathrm{tr}\,\psi$ | 2 | −2 | −1 | 0 | 0 | 1 |

*while if $n$ is odd then let $\psi$ be the representation of $\mathrm{Gal}(F'/K)$, which is isomorphic to $C_3 \rtimes D_4$,*

*with character:*

(3.3)

| *class* | 1 | $2A$ | $2B$ | $2C$ | 3 | 4 | $6A$ | $6B$ | $6C$ |
|---|---|---|---|---|---|---|---|---|---|
| *size* | 1 | 1 | 2 | 6 | 2 | 6 | 2 | 2 | 2 |
| $\operatorname{tr}\psi$ | 2 | $-2$ | 0 | 0 | $-1$ | 0 | $-\sqrt{-3}$ | $\sqrt{-3}$ | 1 |

*where the presentation of* $\mathrm{Gal}(F'/K)$ *and its conjugacy classes are as in Section 3.1.*

*Then* $\rho_{E,\ell}$ *factors as*

$$\rho_{E,\ell} = \chi \otimes \psi. \tag{3.4}$$

Part of this result follows immediately from [15, Theorem 1], [19, Theorem 2] and the classification of the representations of the groups $C_3 \rtimes C_4$ and $C_3 \rtimes D_4$ in [7]. The result for the case of odd $n$ is the most subtle, as there are two possibilities for $\psi$, and we will prove that only one of these occurs, via explicit computation.

The setting and the notation are the same as in Chapter 2. As usual, we are implicitly fixing an embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$, thus identifying the coefficients of the elements in the image of $\rho_{E,\ell}$ with complex numbers. More specifically, $\sqrt{-3}$ in the definition of $\chi$ and $\psi$ is the complex number $i\sqrt{3}$.

The structure of this chapter is as follows. In Section 3.1 we specialise to the case over 3-adic fields when the action of inertia is non-cyclic, giving the setup for the proof of Theorem 3.1. In particular, we fix a presentation for the group $\mathrm{Gal}(F'/K)$ that is mentioned in the theorem. The proof is divided into two parts: in Section 3.2 we give the proof for the case of even inertia degree $n$, and in Section 3.3 we assume that $n$ is odd.

## 3.1 Setup

Let $k$ be the residue field of $K$, and let $n = [k : \mathbb{F}_3]$. Then $n$ is even if and only if $K$ contains a primitive fourth root of unity, which we denote $\zeta_4$ (see [21, XIV, §3, Lemma 1]). The Galois representation changes substantially in these two cases. First of all, we describe the minimal field extension $L/K^{nr}$ where $E$ acquires good reduction. This is [15, Corollaire to Lemme 3].

**Lemma 3.2.** *With the notation as in §2, we have*

$$L = K^{nr}(E[2], \Delta^{1/4}), \tag{3.5}$$

*where* $\Delta^{1/4}$ *is any fourth root of* $\Delta$.

Let $F$ be the field extension of $K$ generated by $E[2]$ and a fixed fourth root of the discriminant, $\Delta^{1/4}$. Note that since $\mathrm{char}(K) = 0$, the curve $E$ can be written with a Weierstrass equation of the form $y^2 = f(x)$, where $f$ is a monic polynomial of degree 3. If $\alpha_1, \alpha_2, \alpha_3$ are the roots of $f$ in $\overline{K}$, $\Delta$

the discriminant of $E$, then $F = K(\alpha_1, \alpha_2, \alpha_3, \Delta^{1/4})$, for some choice of $\Delta^{1/4}$, and the discriminant $\Delta_f$ of the defining polynomial $f$, which is given by

$$\Delta_f = (\alpha_2 - \alpha_1)^2(\alpha_3 - \alpha_2)^2(\alpha_1 - \alpha_3)^2, \tag{3.6}$$

differs from $\Delta$ only by a factor 16; in particular we have that $\sqrt{\Delta_f}$ and therefore $\sqrt{\Delta}$ are in the field generated by 2-torsion.

**Remark 3.3.** *The extension $F/K$ is totally ramified of degree 12. Indeed, since $L = FK^{nr}$, $L/F$ is unramified and $L/K^{nr}$ is totally ramified of degree 12, we have that $F/K$ has a subextension which is totally ramified of degree 12. On the other hand, we have $[F : K] \mid 12$, since the extension of $K$ generated by 2-torsion has degree dividing 6 and it contains a square root of the discriminant, so $F$ is at most a quadratic extension of it. Therefore the degree is equal to 12 and the whole extension $F/K$ is totally ramified. Moreover, as it has good reduction over $L = FK^{nr}$, $E$ acquires good reduction over $F$.*

However $F/K$ is not necessarily Galois. In fact it is Galois, with Galois group isomorphic to $C_3 \rtimes C_4$, if and only if $\zeta_4 \in K$, i.e. $n$ is even. Otherwise, its Galois closure is $F(\zeta_4)$ and $\mathrm{Gal}(F(\zeta_4)/K)$ is isomorphic to the semidirect product $(C_3 \rtimes C_4) \rtimes C_2$. As follows from the classification in [7], this group is $C_3 \rtimes D_4$. We will now fix a presentation for the group $\mathrm{Gal}(F(\zeta_4)/K)$ in the two cases and show that this group is isomorphic to $C_3 \rtimes C_4$ for $n$ even, $C_3 \rtimes D_4$ for $n$ odd.

Suppose first that $n$ is even. With the notation used above, we define $\sigma$ and $\tau$ to be the generators of $\mathrm{Gal}(F/K)$ that act on $\alpha_1, \alpha_2, \alpha_3$ and $\Delta^{1/4}$ as follows:

$$\begin{aligned} \sigma: &\quad \alpha_1 \mapsto \alpha_2, \quad \alpha_2 \mapsto \alpha_3, \quad \alpha_3 \mapsto \alpha_1, \qquad \Delta^{1/4} \mapsto \Delta^{1/4}; \\ \tau: &\quad \alpha_1 \mapsto \alpha_1, \quad \alpha_2 \mapsto \alpha_3, \quad \alpha_3 \mapsto \alpha_2, \qquad \Delta^{1/4} \mapsto \zeta_4 \Delta^{1/4}. \end{aligned} \tag{3.7}$$

Then $\mathrm{Gal}(F/K)$ has the following presentation

$$\langle \sigma, \tau ; \sigma^3 = \tau^4 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle. \tag{3.8}$$

This group is isomorphic to $C_3 \rtimes C_4$, which is given by the presentation in [7], via the isomorphism from $C_3 \rtimes C_4$ to $\mathrm{Gal}(F/K)$ defined by $a \mapsto \sigma\tau^2$ and $b \mapsto \tau$; in fact it is easy to check that these elements satisfy $a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1}$.

Suppose now that $n$ is odd, i.e. $\zeta_4 \notin K$. Then the Galois closure of $F/K$ is given by $F(\zeta_4)$ and the subgroup generated by the elements $\sigma, \tau$ is the inertia subgroup of $\mathrm{Gal}(F(\zeta_4)/K)$. Furthermore, $\mathrm{Gal}(F(\zeta_4)/K)$ contains an extra unramified automorphism corresponding to the map $\zeta_4 \mapsto -\zeta_4$, which we call $\phi$. Therefore it is presented by the following relations:

$$\sigma^3 = 1;\ \tau^4 = 1;\ \phi^2 = 1;\ \sigma\phi = \phi\sigma;\ \phi\tau\phi = \tau^{-1};\ \tau\sigma\tau^{-1} = \sigma^2. \tag{3.9}$$

Now $C_3 \rtimes D_4 = \langle a, b, c | a^3 = b^4 = c^2 = 1, bab^{-1} = cac = a^{-1}, cbc = b^{-1} \rangle$ (see [7]). The map from $C_3 \rtimes D_4$ to $\mathrm{Gal}(F(\zeta_4)/K)$ given by $a \mapsto \sigma$, $b \mapsto \tau$ and $c \mapsto \tau\phi$ is an isomorphism.

We denote the conjugacy classes of the group obtained in the two cases as follows (for the sake of completeness, we will use both the notation of [7] and the one introduced in this chapter):

- if $n$ is even, the conjugacy classes of $\mathrm{Gal}(F/K) \cong C_3 \rtimes C_4$ are $1 = [e]$, $2 = [\tau^2 = b^2]$, $3 = [\sigma = ab^2]$, $4A = [\tau = b]$, $4B = [\sigma\tau = ab^{-1}]$, $6 = [\sigma\tau^2 = a]$;

- if $n$ is odd, the conjugacy classes of $\mathrm{Gal}(F(\zeta_4)/K) \cong C_3 \rtimes D_4$ are $1 = [e]$, $2A = [\tau^2 = b^2]$, $2B = [\phi = b^{-1}c]$, $2C = [\tau\phi = c]$, $3 = [\sigma = a]$, $4 = [\tau = b]$, $6A = [\sigma\phi = ab^{-1}c]$, $6B = [\sigma^2\phi = a^2b^{-1}c]$, $6C = [\sigma\tau^2 = ab^2]$.

We can now prove Theorem 3.1.

## 3.2 Proof of the Main Theorem: the case of even inertia degree

**Proof of Theorem 3.1, even case.** Let us first consider the case $n$ is even, i.e. $\zeta_4 \in K$. Then, if $F$ is as at the beginning of Section 3.1, we showed that $F/K$ is Galois with Galois group isomorphic to $C_3 \rtimes C_4$. But then $F^{nr}/K$ is the compositum of the Galois extensions $F/K$ and $K^{nr}/K$, which intersect in $K$ since $F/K$ is totally ramified and $K^{nr}/K$ is unramified. So $\mathrm{Gal}(F^{nr}/K) \cong \mathrm{Gal}(F/K) \times \mathrm{Gal}(K^{nr}/K)$. In particular the Frobenius element, which generates $\mathrm{Gal}(K^{nr}/K)$, commutes with every element of this group, therefore its image under $\rho_{E,\ell}$ can be represented as a scalar matrix. By Lemma 3.6, proved in §3.3, $E$ reduces to $y^2 = x^3 - x$ on the residue field. We computed in Example 2.14 the eigenvalues of the Frobenius element of $F$, which coincide and are equal to $(-3)^{n/2}$ for every even $n$. As $F/K$ is totally ramified, we can fix the Frobenius element of $K$ to be $\mathrm{Frob}_F$, so it has the same eigenvalues.

Now define the following unramified character:

$$\begin{aligned} \chi(\mathrm{Frob}_K) &= (-3)^{n/2}; \\ \chi|_{I_K} &= 1. \end{aligned} \tag{3.10}$$

Then $\rho_{E,\ell}(\mathrm{Frob}_K) = \chi(\mathrm{Frob}_K)\mathrm{Id}_2$ and there exists a representation $\psi$ such that $\rho_{E,\ell} = \chi \otimes \psi$. The representation $\psi$ is irreducible of dimension 2, since $\rho_{E,\ell}$ is, it is trivial on $\mathrm{Frob}_K$ and coincides with $\rho_{E,\ell}$ on inertia; therefore it factors through $\mathrm{Gal}(F/K) \cong C_3 \rtimes C_4$ and, as a representation of this finite group, it is faithful. The group $C_3 \rtimes C_4$ has only one irreducible faithful 2-dimensional representation (see [7]), so the Galois representation is completely described by it; namely the character of $\psi$ in this case is:

| class | 1 | 2 | 3 | 4A | 4B | 6 |
|---|---|---|---|---|---|---|
| size | 1 | 1 | 2 | 3 | 3 | 2 |
| $\mathrm{tr}\,\psi$ | 2 | −2 | −1 | 0 | 0 | 1 |

as claimed. ∎

## 3.3 Proof of the Main Theorem: the case of odd inertia degree

**Lemma 3.4.** *Let $F(\zeta_4)$ be the Galois closure of $F$. Then:*

$$F(\zeta_4) = K(\sqrt{\alpha_2-\alpha_1}, \sqrt{\alpha_3-\alpha_2}, \sqrt{\alpha_1-\alpha_3}, \sqrt{\alpha_1-\alpha_2}, \sqrt{\alpha_2-\alpha_3}, \sqrt{\alpha_3-\alpha_1}). \tag{3.11}$$

**Proof.** Let

$$F' = K(\sqrt{\alpha_2-\alpha_1}, \sqrt{\alpha_3-\alpha_2}, \sqrt{\alpha_1-\alpha_3}, \sqrt{\alpha_1-\alpha_2}, \sqrt{\alpha_2-\alpha_3}, \sqrt{\alpha_3-\alpha_1}). \tag{3.12}$$

First of all, we prove that $F(\zeta_4) \subseteq F'$. Indeed $\alpha_1, \alpha_2, \alpha_3$ are clearly in $F'$; $\dfrac{\sqrt{\alpha_2-\alpha_1}}{\sqrt{\alpha_1-\alpha_2}}$ is a primitive fourth root of unity contained in $F'$; finally one possible choice for $\Delta^{1/4}$ is given by the product $2\sqrt{(\alpha_2-\alpha_1)(\alpha_3-\alpha_2)(\alpha_1-\alpha_3)}$, which is in $F'$. Since $F'$ contains this element and a primitive fourth root of unity, then also all the other fourth roots of $\Delta$ (which are in $F(\zeta_4)$) are in $F'$. To prove that $F' \subseteq F(\zeta_4)$, let $B = K(\alpha_1, \alpha_2, \alpha_3)$; we show that $[F' : B] \mid [F(\zeta_4) : B]$. The extension $F(\zeta_4)/B$ is of degree 4, with an unramified subextension of degree 2 and a totally tamely ramified subextension of degree 2. Therefore $\mathrm{Gal}(F(\zeta_4)/B) \cong C_2 \times C_2$. The extension $F'/B$ is the compositum of some quadratic extensions, so it is abelian of exponent 2. By [21, XIV, §4, Exercise 3], we have $|B^\times/(B^\times)^2| = 4$, hence $B^\times/(B^\times)^2 \cong C_2 \times C_2$, and by Kummer theory, the abelian extensions of $B$ of exponent 2 are in bijection with the subgroups of $B^\times/(B^\times)^2$, which are five, namely $B$, three quadratic extensions and the biquadratic; therefore $[F' : B] \mid 4$. ∎

We now want to compute the action of $\phi$ on the generators of $F'$; for any choice of the square roots, we know that $\phi(\sqrt{\alpha_2-\alpha_1}) = \pm\sqrt{\alpha_2-\alpha_1}$ and similarly $\phi(\sqrt{\alpha_1-\alpha_2}) = \pm\sqrt{\alpha_1-\alpha_2}$. On the other hand, $\phi$ changes the sign of $\dfrac{\sqrt{\alpha_1-\alpha_2}}{\sqrt{\alpha_2-\alpha_1}}$ for it is a primitive fourth root of unity. Therefore, we have either:

- $\phi(\sqrt{\alpha_2-\alpha_1}) = \sqrt{\alpha_2-\alpha_1}$ and $\phi(\sqrt{\alpha_1-\alpha_2}) = -\sqrt{\alpha_1-\alpha_2}$, or
- $\phi(\sqrt{\alpha_2-\alpha_1}) = -\sqrt{\alpha_2-\alpha_1}$ and $\phi(\sqrt{\alpha_1-\alpha_2}) = \sqrt{\alpha_1-\alpha_2}$.

Without loss of generality the first condition holds, so $\sqrt{\alpha_2-\alpha_1} \in F$. Similarly, using the relations between the generators of $\mathrm{Gal}(F'/K)$, we have that $\phi$ fixes $\sqrt{\alpha_3-\alpha_2}, \sqrt{\alpha_1-\alpha_3}$ and changes sign to the other generators of $F'$; therefore $F$, which is the subfield of $F'$ fixed by $\phi$, satisfies

$$F = K(\sqrt{\alpha_2-\alpha_1}, \sqrt{\alpha_3-\alpha_2}, \sqrt{\alpha_1-\alpha_3}).$$

**Lemma 3.5.** *Let $\mathcal{O}_F$ be the ring of integers of $F$, with maximal ideal $\mathfrak{m}_F$. Then with the same notation as above, we have*

$$\frac{\sigma(x)}{x} \equiv 1 \pmod{\mathfrak{m}_F}, \tag{3.13}$$

*for all $x \in \mathcal{O}_F \setminus \{0\}$.*

**Proof.** As $\sigma$ is in the wild inertia subgroup of $\mathrm{Gal}(F'/K)$, which is equal to the first ramification group by [21, IV, §2, Corollary 1 to Proposition 7], we have $\sigma(x) \equiv x \pmod{\mathfrak{m}_F^2}$. If $x \in \mathcal{O}_F^\times$ (i.e. if $x$ is a unit), then $\sigma(x)/x \equiv 1 \pmod{\mathfrak{m}_F^2}$, hence modulo $\mathfrak{m}_F$; if $x = \pi_F$ is a uniformiser of $O_F$ of $F$ then by [21, IV, §2, Proposition 5] we have $\sigma(x)/x \equiv 1 \pmod{\mathfrak{m}_F}$. In general $x = \pi_F^a u$ where $a$ is a non-negative integer and $u \in \mathcal{O}_F^\times$, so $\sigma(x)/x = (\sigma(\pi_F)/\pi_F)^a \sigma(u)/u \equiv 1 \pmod{\mathfrak{m}_F}$. ■

**Lemma 3.6.** *Let $E$ be as before. Then the reduction of some minimal model for $E/F$ on the residue field is*

$$\tilde{E}/k : y^2 = x^3 - x. \tag{3.14}$$

**Proof.** First note that we can write, over $F$, the equation for $E$ as follows:

$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3). \tag{3.15}$$

Now, operating the following change of variables (well-defined over $F$):

$$\begin{cases} x &= x'(\alpha_2-\alpha_1)+\alpha_1, \\ y &= y'(\sqrt{\alpha_2-\alpha_1})^3, \end{cases} \tag{3.16}$$

we obtain the new equation

$$(y')^2 = x'(x'-1)(x'-\lambda), \tag{3.17}$$

where $\lambda = \dfrac{\alpha_3-\alpha_1}{\alpha_2-\alpha_1}$. Finally, note that $\alpha_1 - \alpha_3 = \sigma^2(\alpha_2-\alpha_1)$, and since $\sigma$ is an element of the wild inertia subgroup of $\mathrm{Gal}(F'/K)$ then by Lemma 3.5, $\dfrac{\sigma^2(\alpha_2-\alpha_1)}{\alpha_2-\alpha_1} \equiv 1$ in the residue field. So the reduction in $k$ of $\lambda$ is the same as the reduction of $-\dfrac{\sigma^2(\alpha_2-\alpha_1)}{\alpha_2-\alpha_1}$, i.e. $-1$. With simplified notation, the reduction of $E$ in $k$ is therefore $y^2 = x^3 - x$. ■

**Proof of Theorem 3.1, odd case.** In Example 2.14 we computed the eigenvalues of the Frobenius element of $F$, and hence of $K$ (as $F/K$ is totally ramified), acting on $E$, which are $(\pm\sqrt{-3})^n$. In particular, since $n$ is odd, they are complex conjugate and the trace of Frobenius is 0.

Let $\chi$ be the following unramified character of $\mathrm{Gal}(\overline{K}/K)$:

$$\begin{aligned} \chi(\mathrm{Frob}_K) &= \sqrt{-3}^n; \\ \chi_{|_{I_K}} &= 1. \end{aligned} \tag{3.18}$$

Then $\rho_{E,\ell}(\mathrm{Frob}_K) = \chi(\mathrm{Frob}_K)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\rho_{E,\ell}(\mathrm{Frob}_K^2) = \chi(\mathrm{Frob}_K)^2\,\mathrm{Id}_2$. Let $F_2$ be the field extension of $K$ fixed by $\mathrm{Frob}_K^2$: then it is an unramified extension of $K$ of degree 2, i.e. $F_2 = K(\zeta_4)$. Also, in the notation used above, $F' = F(\zeta_4) = FF_2$. So the Galois group described before,

$\mathrm{Gal}(F(\zeta_4)/K)$, is generated by $\sigma, \tau$ and the class of $\mathrm{Frob}_K$ modulo $\mathrm{Frob}_K^2$, which we can identify with $\phi$. Moreover, there exists an irreducible representation $\psi$ of $\mathrm{Gal}(\overline{K}/K)$ such that

$$\rho_{E,\ell} = \chi \otimes \psi; \tag{3.19}$$

in order to find it, since $\chi$ is a character, it is sufficient to consider $\psi(g) = \dfrac{1}{\chi(g)}\rho_{E,\ell}(g)$. The kernel of this representation $\psi$ is precisely $\mathrm{Gal}(\overline{K}/F(\zeta_4))$, so $\psi$ factors through the finite group $\mathrm{Gal}(F(\zeta_4)/K)$ and it is indeed an irreducible faithful representation of the finite group $C_3 \rtimes D_4$.

By looking at the character table of $C_3 \rtimes D_4$ (again, see [7]) it follows that there are precisely two irreducible faithful representations of this group of dimension 2, and they only differ for the character of the two conjugacy classes generated by the elements $\sigma\phi$ and $\sigma^2\phi$. To uniquely determine $\psi$ we therefore have to compute the trace of the element $\psi(\sigma\phi)$, and see whether it is $\sqrt{-3}$ or $-\sqrt{-3}$.

We know from Lemma 3.6 that, over $F$, the equation for $E$ is

$$E : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \tag{3.20}$$

and under the change of variables

$$\begin{cases} x &= x'(\alpha_2-\alpha_1)+\alpha_1; \\ y &= y'(\sqrt{\alpha_2-\alpha_1})^3, \end{cases} \tag{3.21}$$

we find the minimal model

$$E_{min} : y^2 = x(x-1)(x-\lambda), \tag{3.22}$$

that reduces to

$$\tilde{E} : y^2 = x^3 - x \tag{3.23}$$

over the residue field. Now let $\beta(x,y) = (x',y')$ be the change of variables above, red be the reduction map: $E_{min}(\overline{K}) \to \tilde{E}(\overline{k})$ and $\mathrm{lift} : \tilde{E}(\overline{k}) \to E_{min}(\overline{K})$ be any section of red. Then we can compute the action of any Galois automorphism $\gamma$ on the reduced curve $\tilde{E}(\overline{k})$ via the following composition:

$$\mathrm{red} \circ \beta \circ \gamma \circ \beta^{-1} \circ \mathrm{lift}. \tag{3.24}$$

So in particular for $\gamma = \sigma\,\mathrm{Frob}_K$ we have (recall $|k| = 3^n$):

$$\begin{aligned} (\tilde{x},\tilde{y}) &\xrightarrow{\text{lift}} (x,y) \xrightarrow{\beta^{-1}} \left(x(\alpha_2-\alpha_1)+\alpha_1, y(\sqrt{\alpha_2-\alpha_1})^3\right) \\ &\xrightarrow{\sigma\,\mathrm{Frob}_K} \left(\sigma(x)^{3^n}\sigma(\alpha_2-\alpha_1)+\alpha_2, \sigma(y)^{3^n}(\sigma(\sqrt{\alpha_2-\alpha_1}))^3\right) \\ &\xrightarrow{\beta} \left(\frac{\sigma(x)^{3^n}\sigma(\alpha_2-\alpha_1)+\alpha_2-\alpha_1}{\alpha_2-\alpha_1}, \sigma(y)^{3^n}\frac{(\sigma(\sqrt{\alpha_2-\alpha_1}))^3}{(\sqrt{\alpha_2-\alpha_1})^3}\right) \\ &= \left(\sigma(x)^{3^n}\frac{\sigma(\alpha_2-\alpha_1)}{\alpha_2-\alpha_1}+1, \sigma(y)^{3^n}\frac{(\sigma(\sqrt{\alpha_2-\alpha_1}))^3}{(\sqrt{\alpha_2-\alpha_1})^3}\right) \xrightarrow{\text{red}} \left(\tilde{x}^{3^n}+1, \tilde{y}^{3^n}\right) \end{aligned} \tag{3.25}$$

Note that:

- the reductions of $\dfrac{\sigma(\alpha_2-\alpha_1)}{\alpha_2-\alpha_1}$ and $\dfrac{\sigma(\sqrt{\alpha_2-\alpha_1})}{\sqrt{\alpha_2-\alpha_1}}$ are 1 by Lemma 3.5;
- $\mathrm{Frob}_K$ fixes $F$, therefore it acts trivially on the elements $\alpha_2-\alpha_1$ and $\sqrt{\alpha_2-\alpha_1}$;
- since $\sigma$ is an inertia element, $\sigma(x)\equiv x$ and $\sigma(y)\equiv y$ in $\overline{k}$.

Now, to compute the trace of $\rho_{E,\ell}(\sigma\,\mathrm{Frob}_K)$ we use the formula

$$\mathrm{tr}(\rho_{E,\ell}(\gamma)) = \deg(\gamma)+1-\deg(1-\gamma); \tag{3.26}$$

in our case $\deg(\gamma)=\det\rho_{E,\ell}(\sigma\,\mathrm{Frob}_K)=3^n$ and $\deg(1-\gamma)$ is the number of points fixed by $\sigma\,\mathrm{Frob}_K$, i.e. the number of solutions (including the point at infinity) of

$$\begin{cases} x &= x^{3^n}+1 \\ y &= y^{3^n} \\ y^2 &= x^3-x. \end{cases} \tag{3.27}$$

Let us first consider the case $n=1$. There are no solutions over $\overline{k}$ to this system of equations, therefore $\mathrm{tr}(\rho_{E,\ell}(\sigma\,\mathrm{Frob}_K))=3$. But then

$$\mathrm{tr}(\psi(\sigma\phi)) = \frac{1}{\sqrt{-3}}3 = -\sqrt{-3}. \tag{3.28}$$

In general, we know that $\mathrm{tr}(\psi(\sigma\,\mathrm{Frob}_K))=\varepsilon\sqrt{-3}$ for some $\varepsilon\in\{\pm1\}$, and $\mathrm{tr}(\rho_{E,\ell}(\sigma\,\mathrm{Frob}_K))=\varepsilon\sqrt{-3}\chi(\sigma\,\mathrm{Frob}_K)=\varepsilon\sqrt{-3}\sqrt{-3}^n=\varepsilon(-3)^{(n+1)/2}$. The value of $\varepsilon$ can be determined by solving the system of equations above, but for a general $n$, it cannot be solved directly. However, the number of solutions is independent of the curve we use, so it is sufficient to work with a fixed curve. Consider for example the elliptic curve over $\mathbb{Q}_3$

$$E: y^2 = x^3+9. \tag{3.29}$$

Since its reduction modulo 3 is $y^2=x^3$, the valuation of the discriminant is 7 and the $j$-invariant is 0, this curve has potentially good reduction, and its Néron type is $IV$, so we are in the last case of Theorem 2.8. Hence the image of inertia is isomorphic to $C_3\rtimes C_4$.

Let us fix a basis for $\overline{\mathbb{Q}}_\ell^2$ (with $\overline{\mathbb{Q}}_\ell$ considered as embedded in $\mathbb{C}$), where the action of Frobenius is given by the matrix

$$\rho_{E,\ell}(\mathrm{Frob}_K) = \begin{pmatrix} \sqrt{-3} & 0 \\ 0 & -\sqrt{-3} \end{pmatrix}; \tag{3.30}$$

then the image of $\sigma$ is either $\begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}$ or its inverse, where $\zeta_3\in\overline{\mathbb{Q}}_\ell$ is the primitive third root of unit $\dfrac{-1+\sqrt{-3}}{2}$. By the computation done for the case $n=1$, we know $\mathrm{tr}(\rho_{E,\ell}(\sigma\,\mathrm{Frob}_K))=3$ and

a simple check shows that then $\rho_{E,\ell}(\sigma) = \begin{pmatrix} \zeta_3^{-1} & 0 \\ 0 & \zeta_3 \end{pmatrix}$. Now let $K$ be an unramified extension of $\mathbb{Q}_3$ of odd degree $n$, so the residue field $k$ is a degree $n$ extension of $\mathbb{F}_3$ and the reduction type and Galois representation of the curve $E$ base-changed to $K$, restricted to inertia, is exactly the same as above. Then $\rho_{E,\ell}(\sigma \operatorname{Frob}_K) = \begin{pmatrix} \zeta_3^{-1}\sqrt{-3}^n & 0 \\ 0 & -\zeta_3\sqrt{-3}^n \end{pmatrix}$, with trace $-(-3)^{(n+1)/2}$. Incidentally, this argument proves the following.

**Lemma 3.7.** *The number of solutions of the system of equations* (3.27) *above is* $3^n + (-3)^{(n+1)/2}$.

**Proof.** We have $\operatorname{tr}(\rho_{E,\ell}(\sigma \operatorname{Frob}_K)) = -(-3)^{(n+1)/2}$. On the other hand, we know

$$\operatorname{tr}(\rho_{E,\ell}(\sigma \operatorname{Frob}_K)) = |k| + 1 - (1 + |\{\text{solutions to (3.27)}\}|) = \tag{3.31}$$

$$= 3^n - |\{\text{solutions to (3.27)}\}|, \tag{3.32}$$

so the number of solutions to (3.27) is precisely $3^n - \operatorname{tr}(\rho_{E,\ell}(\sigma \operatorname{Frob}_K)) = 3^n + (-3)^{(n+1)/2}$. □

So, with the notation above, we have $\varepsilon = -1$, and the character of $\psi$ is the following:

| class | 1 | $2A$ | $2B$ | $2C$ | 3 | 4 | $6A$ | $6B$ | $6C$ |
|---|---|---|---|---|---|---|---|---|---|
| size | 1 | 1 | 2 | 6 | 2 | 6 | 2 | 2 | 2 |
| $\operatorname{tr}\psi$ | 2 | $-2$ | 0 | 0 | $-1$ | 0 | $-\sqrt{-3}$ | $\sqrt{-3}$ | 1 |

as claimed. In particular, in the proof we computed the character of an element of the class $6A$. ■

CHAPTER 4

# ELLIPTIC CURVES OVER A 2-ADIC FIELD WITH NON-ABELIAN INERTIA ACTION

This chapter is a modified version of the author's paper "Wild Galois Representations: elliptic curves over a 2-adic field with non-abelian inertia action", published in International Journal of Number Theory ([3]).

The notation is the same as in Chapter 2, with $p = 2$; in particular let $K$ be a 2-adic field and let $E/K$ be an elliptic curve. Since $\mathrm{char}(K) = 0$, we can always assume that $E$ is in short Weierstrass form, $E : y^2 = x^3 + a_4x + a_6$, for $a_4, a_6 \in K$. Let $k$ be the residue field of $K$ and let $n = [k : \mathbb{F}_2]$. Suppose that $E/K$ has potentially good reduction; we want to study the representation $\rho_{E,\ell}$ on the $\ell$-adic Tate module $T_\ell(E)$; as usual, we fix a basis for $T_\ell(E) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$ so we can identify $\mathrm{Aut}(T_\ell(E) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell)$ with $\mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$. The image of restriction of $\rho_{E,\ell}$ to the inertia subgroup $I_K$ of $\mathrm{Gal}(\overline{K}/K)$ is isomorphic to $\mathrm{Gal}(L/K^{nr})$, where $L$ is the minimal extension of $K^{nr}$ over which $E$ acquires good reduction. Moreover, since $K$ is a 2-adic field, the image of inertia, which we denote by $I$, can only be one of the following:

$$C_2, C_3, C_4, C_6, Q_8, \mathrm{SL}_2(\mathbb{F}_3). \tag{4.1}$$

In this chapter we focus on the cases where $I$ is non-abelian (equivalently non-cyclic), hence it is either $Q_8$ or $\mathrm{SL}_2(\mathbb{F}_3)$.

As in the previous chapters, we call an arithmetic Frobenius of $K$, and denote by $\mathrm{Frob}_K$, any fixed choice of an element of $\mathrm{Gal}(\overline{K}/K)$ that reduces to the Frobenius element modulo $I_K$. In order to compute explicitly the elements in the image of $\rho_{E,\ell}$, let us fix an embedding $\overline{\mathbb{Q}}_\ell \to \mathbb{C}$; in particular we will identify the element $\sqrt{-2}$ of $\overline{\mathbb{Q}}_\ell$ with $i\sqrt{2} \in \mathbb{C}$.

We will prove the following result. We refer to [7] for the notation used for group names and character tables; in particular we denote each conjugacy class by the order of its elements, followed by a letter if there is more than one class with the same order.

**Theorem 4.1.** *Let $E/K$ be an elliptic curve with potentially good reduction over a 2-adic field, let $\ell$ be a prime different from 2 and let $\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ be the $\ell$-adic Galois representation attached to $E$. Suppose that $I = \rho_{E,\ell}(I_K)$ is non-abelian. Let $\Delta$ be the discriminant of a (not necessarily minimal) equation for $E$ and let $n$ be the inertia degree of $K/\mathbb{Q}_2$. Then $\rho_{E,\ell}$ factors as*

$$\rho_{E,\ell} = \chi \otimes \psi \tag{4.2}$$

*where $\chi : \mathrm{Gal}(\overline{K}/K) \to \overline{\mathbb{Q}}_\ell^\times$ is the unramified character mapping the arithmetic Frobenius of $K$ to $(\sqrt{-2})^n$, and $\psi$ is the irreducible 2-dimensional representation of the group $G = \mathrm{Gal}(K(E[3])/K)$ given as follows.*

- *If $n$ is even and $\Delta$ is a cube in $K$, then $\psi$ is the representation of $G = Q_8$ with character*

| *class* | 1 | 2 | $4A$ | $4B$ | $4C$ |
|---|---|---|---|---|---|
| *size* | 1 | 1 | 2 | 2 | 2 |
| $\mathrm{tr}\,\psi$ | 2 | −2 | 0 | 0 | 0 |

- *If $n$ is even and $\Delta$ is not a cube in $K$, then $\psi$ is the representation of $G = \mathrm{SL}_2(\mathbb{F}_3)$ with character*

| *class* | 1 | 2 | $3A$ | $3B$ | 4 | $6A$ | $6B$ |
|---|---|---|---|---|---|---|---|
| *size* | 1 | 1 | 4 | 4 | 6 | 4 | 4 |
| $\mathrm{tr}\,\psi$ | 2 | −2 | −1 | −1 | 0 | 1 | 1 |

  *Moreover the image of inertia is $Q_8$ if $\Delta$ is a cube in $K^{nr}$ and $\mathrm{SL}_2(\mathbb{F}_3)$ otherwise.*

- *If $n$ is odd and $\Delta$ is a cube in $K$ (equivalently the image of inertia is $Q_8$), then $\psi$ is the representation of $G = SD_{16}$ with character*

| *class* | 1 | $2A$ | $2B$ | $4A$ | $4B$ | $8A$ | $8B$ |
|---|---|---|---|---|---|---|---|
| *size* | 1 | 1 | 4 | 2 | 4 | 2 | 2 |
| $\mathrm{tr}\,\psi$ | 2 | −2 | 0 | 0 | 0 | $\sqrt{-2}$ | $-\sqrt{-2}$ |

- *If $n$ is odd and $\Delta$ is not a cube in $K$ (equivalently the image of inertia is $\mathrm{SL}_2(\mathbb{F}_3)$), then $\psi$ is the representation of $G = \mathrm{GL}_2(\mathbb{F}_3)$ with character*

| *class* | 1 | $2A$ | $2B$ | 3 | 4 | 6 | $8A$ | $8B$ |
|---|---|---|---|---|---|---|---|---|
| *size* | 1 | 1 | 12 | 8 | 6 | 8 | 6 | 6 |
| $\mathrm{tr}\,\psi$ | 2 | −2 | 0 | −1 | 0 | 1 | $\sqrt{-2}$ | $-\sqrt{-2}$ |

*In the last two cases a generator for the class $8A$ can be described explicitly (it is $\phi\sigma$ in the proof of Theorem 4.7).*

This theorem is almost completely proved in [9, §5]. In particular the cases where $n$ is even are already known, and here we present a proof for completeness. The cases where $n$ is odd are more subtle. Although it can be easily proved that the representation $\psi$ can only be either the one described above or the one which has the same character values for every conjugacy class except for the classes $8A$ and $8B$, which are swapped, it is not trivial to identify which of these two is equal to $\psi$. In this chapter we prove that, with the definition of $\chi$ made in the statement of Theorem 4.1, only one of the two possible cases occurs for elliptic curves. The method of proof consists of describing explicitly a generator of the class $8A$ and computing the trace of $\psi$ on it.

## 4.1 The good model

In the following, $E$ is an elliptic curve over a 2-adic field $K$, with potentially good reduction, such that the Galois action attached to it has non-abelian inertia image $I$.

**Lemma 4.2.** *Let $F$ be the field obtained from $K$ by adjoining the coordinates of one point of exact order 3 and a cube root of the discriminant $\Delta$ of $E$. Then $E$ acquires good reduction over $F$ and it reduces to $\tilde{E}_F : y^2 + y = x^3$ on the residue field.*

**Proof.** Let $P = (x_P, y_P)$ be a non-trivial 3-torsion point with coordinates in $F$ and let $\lambda_P$ be the slope of the tangent line at $P$. Then after applying the change of coordinates

$$\begin{cases} x & \mapsto & x + x_P \\ y & \mapsto & y + \lambda_P x + y_P \end{cases} \tag{4.3}$$

we get an equation for $E$ over $F$ with the same discriminant $\Delta$, of the form

$$y^2 + Axy + By = x^3, \tag{4.4}$$

with $B \neq 0$ (for a detailed computation see [17, §2, Proposition 2.22 and Corollary 2.23]).

Next we prove that $B$ is a cube in $F$. Note that the discriminant of equation (4.4) is given by

$$\Delta = -27B^4 + (AB)^3; \tag{4.5}$$

since $\Delta$ and $-B^3$ are cubes in $F$, we have that also $27B - A^3 = 27B\left(1 - \frac{A^3}{27B}\right)$ is a cube in $F$. If we show that the quantity $1 - \frac{A^3}{27B}$ is a cube in $F$, then also $B$ is. To prove this claim, it is sufficient to show that the valuation in $F$ of $\frac{A^3}{27B}$ is strictly positive. Then we conclude using Hensel's Lemma that the polynomial $z^3 - \left(1 - \frac{A^3}{27B}\right)$ has a root in $F$.

We know by [19, §2, Corollary 2] that $E$ acquires good reduction over the field $K(E[3])$. We write $v'$ for the normalized valuation on this field, and $v_F$ for the normalized valuation on $F$. As shown in the proof of Theorem 2 in [19], the image of inertia under the Galois action injects into $\mathrm{Aut}(\tilde{E}_{K(E[3])})$, therefore by the classification of the automorphisms of an elliptic curve over a field of characteristic 2 (see [23, III, §10, Theorem 10.1]) it can be non-abelian only if $v'(j) > 0$, where $j$ is the $j$-invariant of the curve, and therefore we have $v_F(j) > 0$.

Assume by contradiction that $v_F\left(\frac{A^3}{27B}\right) \leq 0$, or equivalently $3v_F(A) \leq v_F(B)$. By direct computation,

$$j = \frac{A^3(A^3-24B)^3}{B^3(A^3-27B)} \tag{4.6}$$

so we have that the valuation of the numerator is $12v_F(A)$, and the valuation of the denominator is at least $3v_F(B)+3v_F(A)$. Now

$$v_F(j) \leq 12v_F(A) - 3(v_F(B)+v_F(A)) = 3(3v_F(A)-v_F(B)) \leq 0, \tag{4.7}$$

contradicting the fact that $v_F(j) > 0$.

Therefore $B$ is a cube in $F$ and the following is a well-defined change of variables over the field $F$.

$$\begin{cases} x & \mapsto & (B^{1/3})^2 x \\ y & \mapsto & (B^{1/3})^3 y \end{cases} \tag{4.8}$$

After applying this transformation to the curve (4.4), we get the model $y^2 + A'xy + y = x^3$, with $A' = A/B^{1/3}$. By the computation above, $v_F(A) > v_F(B)/3$, so $v_F(A') > 0$ and the valuation of the discriminant is $v_F(-27B^4 + (AB)^3) - 12v_F(B^{1/3}) = 0$. Therefore this model reduces to $y^2 + y = x^3$ on the residue field of $F$, and in particular $E$ acquires good reduction over $F$. ■

Computationally it is possible to find the values $x_P, y_P, \lambda_P$ using the following modified version of the 3-division polynomial, whose roots are precisely the slopes of all tangent lines at the non-trivial 3-torsion points (for a proof, see [8, Theorem 1]):

$$\gamma(t) = t^8 + 18a_4t^4 + 108a_6t^2 - 27a_4^2. \tag{4.9}$$

If $\lambda_P$ is a root of $\gamma$, then the corresponding point $P$ has coordinates $x_P = \frac{\lambda_P^2}{3}$, $y_P = \frac{\lambda_P^4+3a_4}{6\lambda_P}$.

Let $F^{nr}$ be the maximal unramified extension of $F$, which is equal to the compositum of $F$ and $K^{nr}$. Note that $F^{nr}$ is the minimal extension of $K^{nr}$ where the curve $E$ acquires good reduction. Indeed if $L$ is such an extension, then by [19, §2, Corollary 2], we have that $L = K^{nr}(E[3])$ and so it clearly contains the coordinates of any 3-torsion point and any cube root of $\Delta$, which by an easy computation can be expressed in terms of these coordinates, so $F^{nr} \subseteq L$ (see [17, §2, Lemma 2.20]). On the other hand, E does acquire good reduction over $F$, hence on $F^{nr}$, so $L = F^{nr}$ by minimality. Also note that $\ker(\rho_{E,\ell}) = \mathrm{Gal}(\overline{K}/L)$ and so the representation factors through $\mathrm{Gal}(L/K)$ and the representation induced here is injective.

We have that $[L:K^{nr}] \mid [F:K]$, and since we are assuming that $I$ is non-abelian then $[L:K^{nr}]$ is either 8 or 24, so $8 \mid [F:K]$. This occurs precisely when the extension given by adjoining the coordinates of $P$ is totally ramified of degree 8, i.e. when the polynomial $\gamma$ defined above is irreducible over $K^{nr}$.

There are several cases to consider:

- if $\Delta$ is a cube in $K$, then the degree of $F/K$ is exactly 8;
- if $\Delta$ is a cube in $K^{nr}$ but not in $K$, then $[L:K^{nr}]=8$ and $[F:K]=24$;
- if $\Delta$ is not a cube in $K^{nr}$, then $[L:K^{nr}]=[F:K]=24$.

Moreover the Galois closure of $F/K$ is given by $K(E[3])=F(\zeta_3)$, where $\zeta_3$ is a primitive third root of unity; since if $\zeta_3\notin K$ it generates a degree 2 unramified extension, we have that $F/K$ is not Galois if and only if the inertia degree $n$ of $K$ over $\mathbb{Q}_2$ is odd. Note that this cannot occur if $\Delta$ is a cube in $K^{nr}$ but not in $K$, otherwise the extension $K(\Delta^{1/3},\zeta_3)$ would be unramified and not cyclic.

## 4.2 Proof of the main theorem

We will use the same notation as in Section 4.1. Since $I$ is non-abelian, then the group $\mathrm{Gal}(L/K)$ is also non-abelian. By [9, §2, Lemma 1], the representation $\rho_{E,\ell}$ factors as $\chi\otimes\psi$, where $\chi$ is the following character:

$$\begin{aligned}\chi:\mathrm{Gal}(\overline{K}/K) &\to \overline{\mathbb{Q}}_\ell^\times\\ \mathrm{Frob}_K &\mapsto (\sqrt{-2})^n;\\ I_K &\mapsto 1,\end{aligned}\tag{4.10}$$

and $\psi:\mathrm{Gal}(\overline{K}/K)\to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ factors through the finite group $G=\mathrm{Gal}(F(\zeta_3)/K)$, which is either $Q_8$ or $\mathrm{SL}_2(\mathbb{F}_3)$ if $n$ is even, $SD_{16}$ or $\mathrm{GL}_2(\mathbb{F}_3)$ if $n$ is odd. As a $G$-representation, $\psi$ is irreducible and faithful, and it is given by $\psi(g)=\dfrac{1}{\chi(g)}\rho_{E,\ell}(g)$. The definition of $\chi$ is suggested by the following lemma.

**Lemma 4.3.** *Let* $\mathrm{Frob}_F$ *be the arithmetic Frobenius of* $F$*; then the eigenvalues of* $\rho_{E,\ell}(\mathrm{Frob}_F)$ *are* $(\pm\sqrt{-2})^{f_{F/\mathbb{Q}_2}}$*; in particular these are real and equal if* $f_{F/\mathbb{Q}_2}$ *is even, complex conjugate if* $f_{F/\mathbb{Q}_2}$ *is odd.*

**Proof.** By Lemma 4.2 we can compute the characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_F)$ via point-counting on the reduced curve $y^2+y=x^3$, so by Example 2.15, for odd $f_{F/\mathbb{Q}_2}$ we get eigenvalues $\sqrt{-2}^{f_{F/\mathbb{Q}_2}}$, $-\sqrt{-2}^{f_{F/\mathbb{Q}_2}}$, and for even $f_{F/\mathbb{Q}_2}$ there is only one double eigenvalue $(-2)^{f_{F/\mathbb{Q}_2}/2}$. ■

We have that, for even $n=f_{K/\mathbb{Q}_2}$, $F(\zeta_3)=F$ and so $\mathrm{Frob}_F$ is central in the group $\mathrm{Gal}(L/K)$, so it acts as a scalar matrix, with eigenvalue given by Lemma 4.3. Moreover, for any $n$, if $\Delta^{1/3}\notin K^{nr}\setminus K$, then $F$ and $K$ have the same residue field and so $f_{F/\mathbb{Q}_2}=n$; in this case $\rho_{E,\ell}(\mathrm{Frob}_K)=\rho_{E,\ell}(\mathrm{Frob}_F)$. Otherwise, the unramified part of the extension $F/K$ is given by adjoining $\Delta^{1/3}$ and therefore it has degree 3, so $f_{F/\mathbb{Q}_2}=3n$. In particular $\rho_{E,\ell}(\mathrm{Frob}_F)=\rho_{E,\ell}(\mathrm{Frob}_K)^3$.

Suppose first that $n$ is even and that $\Delta^{1/3}\notin K^{nr}\setminus K$. Then we have the following.

**Theorem 4.4.** *If $K$ is a 2-adic field with even inertia degree $n$ over $\mathbb{Q}_2$, then Theorem 4.1 is true for any elliptic curve $E/K$ with potentially good reduction such that the image of inertia under $\rho_{E,\ell}$ is non-abelian and $\Delta^{1/3} \notin K^{nr} \setminus K$.*

**Proof.** Since $n$ is even, $G$ is equal to its inertia subgroup since either $\Delta^{1/3} \in K$ or $\Delta^{1/3} \notin K^{nr}$. As noticed above, $\mathrm{Frob}_K$ acts as the multiplication by a scalar with eigenvalue $(-2)^{n/2} = \chi(\mathrm{Frob}_K)$, therefore $\psi$ is given by the representation $\rho_{E,\ell}$ restricted to inertia, hence it is a faithful, irreducible 2-dimensional representation of $G$ (which is either $Q_8$ or $\mathrm{SL}_2(\mathbb{F}_3)$). Moreover by [19, §2, Theorem 2.ii], the character of this representation has values in $\mathbb{Z}$. By inspecting the character tables of $Q_8$ and $\mathrm{SL}_2(\mathbb{F}_3)$ on [7], we deduce that each of these groups only has one such representation, namely the one given in the statement. ■

For the case $\Delta^{1/3} \in K^{nr} \setminus K$, the image of inertia is strictly smaller than $\mathrm{Gal}(F/K)$, so the argument that the character values are in $\mathbb{Z}$ does not apply directly. However it is still possible to compute $\psi$, getting a result surprisingly similar to the one in Theorem 4.4.

**Theorem 4.5.** *If $K$ is a 2-adic field with even inertia degree over $\mathbb{Q}_2$ and $E$ is an elliptic curve with potentially good reduction over $K$ such that the image of inertia under $\rho_{E,\ell}$ is non-abelian and $\Delta^{1/3} \in K^{nr} \setminus K$, then Theorem 4.1 holds for $E$.*

**Proof.** The difference between $G$ and its inertia subgroup is determined by $\mathrm{Frob}_K$. We will show that the trace of $\psi(\mathrm{Frob}_K)$ is integer and so the result will follow from the proof of Theorem 4.4.

Recall that $\chi$ is the unramified character given by $\chi(\mathrm{Frob}_K) = (-2)^{n/2}$; then, since the inertia degree of $F/K$ is 3, we have $\rho_{E,\ell}(\mathrm{Frob}_F) = \rho_{E,\ell}(\mathrm{Frob}_K)^3$, therefore using the relation $\rho_{E,\ell} = \chi \otimes \psi$ and the fact that $\rho_{E,\ell}(\mathrm{Frob}_F)$ is a scalar, we have:

$$(-2)^{3n/2}\,\mathrm{Id}_2 = ((-2)^{n/2}\psi(\mathrm{Frob}_K))^3; \tag{4.11}$$

so the eigenvalues of $\psi(\mathrm{Frob}_K)$ are third roots of unity (not necessarily primitive) in $\overline{\mathbb{Q}}_\ell$; moreover the order of $\psi(\mathrm{Frob}_K)$ is exactly 3, since $\psi$ is faithful as a representation of $G$, so not both the eigenvalues can be 1. Computing the determinant on both sides, we obtain that $\det(\psi(\mathrm{Frob}_K)) = 1$, therefore the eigenvalues of $\psi(\mathrm{Frob}_K)$ can only be the two distinct primitive third roots of unity, with trace $-1$. Hence the representation $\psi$ of $\mathrm{SL}_2(\mathbb{F}_3)$ is the one given in the statement. ■

From this moment on, we assume that $n$ is odd or equivalently that $F/K$ is not Galois. Then $\psi$ is an irreducible faithful representation of dimension 2 of $G$, which is either $SD_{16}$ if $\Delta$ is a cube in $K$, or $\mathrm{GL}_2(\mathbb{F}_3)$ otherwise. Again, by looking at the character tables of these two groups in [7], we obtain two possible such representations, both of which extend the representation of inertia described in the proof of Theorem 4.4. These two representations only differ for the character value on the elements of order 8. So we need a more explicit description of the action of this group to deduce which one is the correct representation. Note that we will only concentrate on

the wild inertia subgroup of $G$, so we may assume for simplicity that the whole group is $SD_{16}$. If $G = \mathrm{GL}_2(\mathbb{F}_3)$, then the wild inertia subgroup does not change, since this Galois group differs from the previous one by a cubic totally ramified (hence tame) field extension, and the parity of $n$ is not affected.

First, we need to describe explicitly this wild group. Recall that if $\tilde{E}_F$ is the reduced curve of the good model for $E$ over $F$, then there is an injection of the image of inertia into $\mathrm{Aut}(\tilde{E}_F)$, that is $\mathrm{SL}_2(\mathbb{F}_3)$. This injection is obtained as follows: fix an element $\sigma$ of inertia, and a point $(\tilde{x}, \tilde{y})$ on the reduced curve, then lift it to a point $(x, y)$ of $E_F$, which has coordinates in $F$, apply $\sigma$ to each coordinate, and then reduce to another point which again lies on $\tilde{E}_F$. The group $G$ contains a copy of the image of inertia and an extra element $\phi$ of order 2; applying the same construction, we see that $\phi$ acts as Frobenius on the reduced curve. This describes a faithful representation of $G$ with values in $\mathrm{GL}_2(\mathbb{F}_3)$.

Now fix $\ell = 3$ and consider the representation $\overline{\rho_{E,\ell}}$: with this notation we mean the modulo 3 Galois representation attached to $E$, i.e. the one given by the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[3]$; this is equal to the reduction modulo 3 of $\rho_{E,\ell}$; notice that, after fixing a basis $\{P, Q\}$ for $E[3]$ as a $\mathbb{F}_3$-vector space, $\overline{\rho_{E,\ell}}$ takes values in $\mathrm{GL}_2(\mathbb{F}_3)$, and by construction it factors through $G$. In [17, §4, Figure 4.2] there is a visual interpretation of this action. The two representations described above are identical, since they are both induced by the action of the Galois group on elements of $F(\zeta_3)$. We will use both interpretations to find the character of the generators of the group $G$ under $\psi$.

**Lemma 4.6.** *There exists a basis $\{P, Q\}$ of $E[3]$ where the matrix representing the image of Frobenius modulo 3 is* $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

**Proof.** Let $P$ be as in the proof of Lemma 4.2. Then $P$ and $-P$ are the only points of exact order 3 with coordinates in $F$. Otherwise if $Q = (x_Q, y_Q)$ is another point of order 3 and $x_Q, y_Q \in F$, then the coordinates of every other point of order 3 would be rational functions with rational coefficients of $x_P, y_P, x_Q, y_Q$, since $E[3] = \{O, \pm P, \pm Q, \pm P \pm Q\}$, hence these coordinates would be in $F$, thus $F/K$ would be Galois, contradiction.

We know that the good model for $E_F$ reduces to $y^2 + y = x^3$, and by direct computation this curve has the following 8 points of exact order 3:

$$(0,0),(0,1),(\overline{\zeta_3},\overline{\zeta_3}),(\overline{\zeta_3},\overline{\zeta_3}^2),(1,\overline{\zeta_3}),(1,\overline{\zeta_3}^2) \text{ and } (\overline{\zeta_3}^2,\overline{\zeta_3}),(\overline{\zeta_3}^2,\overline{\zeta_3}^2), \tag{4.12}$$

where $\overline{\zeta_3}$ is a third root of unity in $\overline{K}$.

After applying the change of coordinates described in Lemma 4.2, $P$ reduces to $(0,0)$ and $-P$ to $(0,1)$. Let $Q$ be the 3-torsion point of $E(F(\zeta_3))$ reducing to $(1,\overline{\zeta_3})$. Then under $\overline{\rho_{E,\ell}}$ (recall $\ell = 3$), Frobenius acts trivially on $P$ and maps $Q$ to $-Q$, that is to the only point that has the

same abscissa of $Q$, which is in $F$. Therefore if we complete $P$ to the basis $\{P,Q\}$ of $E[3]$ with $Q$ as above, the matrix expressing the Frobenius in this basis is $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, as claimed. ■

**Theorem 4.7.** *If $K$ is a 2-adic field with odd inertia degree $n$ over $\mathbb{Q}_2$, then Theorem 4.1 is true for any elliptic curve $E/K$ with potentially good reduction such that the image of inertia under $\rho_{E,\ell}$ is non-abelian.*

**Proof.** We will denote by $b$ the matrix $\overline{\rho_{E,\ell}}(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3)$. Now let us choose an element $\sigma$ in the inertia subgroup, of order 4, for example

$$\begin{aligned} P &\mapsto Q-P \\ Q &\mapsto P+Q. \end{aligned} \tag{4.13}$$

It exists since $Q_8$ is contained in the image of inertia under $\overline{\rho_{E,\ell}}$, therefore every element of $\mathrm{GL}_2(\mathbb{F}_3)$ with determinant 1 and 2-power order is in the image of inertia. Then $\overline{\rho_{E,\ell}}(\sigma)$ is given by the matrix $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. The element $\phi\sigma$ is an element of order 8 of the group $G$ and so if we determine $\mathrm{tr}\,\psi(\phi\sigma)$, we determine the irreducible representation $\psi$. To compute this trace, we look at the trace of $\rho_{E,\ell}(\mathrm{Frob}_K\sigma)$. Let $a$ be the reduction of $\rho_{E,\ell}(\mathrm{Frob}_K\sigma)$ modulo 3. Then $a = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$, with trace 1. This means that $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_K\sigma)) \equiv 1 \pmod 3$. Note that $a,b$, with the relations $a^8 = b^2 = 1, bab = a^3$ generate $SD_{16}$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ (see the presentation of $SD_{16}$ in [7]).

By looking at the character table of the group $SD_{16}$ in [7], we deduce that $\mathrm{tr}\,\psi(\phi\sigma)$ is either $\sqrt{-2}$ or $-\sqrt{-2}$, so

$$\mathrm{tr}\,\rho_{E,\ell}(\mathrm{Frob}_K\sigma) = \chi(\mathrm{Frob}_K)\,\mathrm{tr}(\psi(\phi\sigma)) \in \{\sqrt{-2}^n \cdot (\pm\sqrt{-2})\}. \tag{4.14}$$

Only one of this two numbers is congruent to 1 modulo 3, namely the one we obtain if $\mathrm{tr}\,\psi(\phi\sigma) = +\sqrt{-2}$. Therefore we have the following character for $\psi$ (note that only the generators of the conjugacy classes of elements outside inertia, which identify the correct representation, are explicitly written).

| class | 1 | 2A | 2B | 4A | 4B | 8A | 8B |
|---|---|---|---|---|---|---|---|
| size | 1 | 1 | 4 | 2 | 4 | 2 | 2 |
| generator | | | $\phi$ | | | $\phi\sigma$ | $\phi\sigma^{-1}$ |
| $\mathrm{tr}\,\psi$ | 2 | −2 | 0 | 0 | 0 | $\sqrt{-2}$ | $-\sqrt{-2}$ |

Similarly if the inertia image is $\mathrm{SL}_2(\mathbb{F}_3)$, we get the following character for $\psi$:

| class | 1 | 2A | 2B | 3 | 4 | 6 | 8A | 8B |
|---|---|---|---|---|---|---|---|---|
| size | 1 | 1 | 12 | 8 | 6 | 8 | 6 | 6 |
| generator | | | $\phi$ | | | | $\phi\sigma$ | $\phi\sigma^{-1}$ |
| $\mathrm{tr}\,\psi$ | 2 | −2 | 0 | −1 | 0 | 1 | $\sqrt{-2}$ | $-\sqrt{-2}$ |

as stated. ■

CHAPTER 5

# ELLIPTIC CURVES WITH WILD CYCLIC REDUCTION

In this chapter, we describe the Galois representation $\rho_{E,\ell}$ attached to an elliptic curve which has wild potentially good reduction, and such that the image of inertia $I = \rho_{E,\ell}(I_K)$ is cyclic. In other words, we consider all the cases that we have not dealt with in Chapters 2, 3 and 4.

As usual, let $K$ be a non-archimedean local field of characteristic 0 and residue characteristic $p \in \{2,3\}$, with uniformiser $\pi_K$, normalised valuation $v$ and residue field $k$. Let $E/K$ be an elliptic curve given by a minimal Weierstrass equation, with discriminant $\Delta$. Let $\ell$ be a prime different from $p$ and $\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E))$ be the $\ell$-adic Galois representation. We view $\mathrm{Aut}(T_\ell(E))$ as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ by tensoring over $\mathbb{Z}_\ell$ with $\overline{\mathbb{Q}}_\ell$, and we fix an embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$.

## 5.1 The case $p = 3$

We assume for this section that $p = 3$. Then, by Theorem 2.8, we have that $E$ has wild potentially good reduction with cyclic inertia image (wild cyclic reduction for simplicity) exactly when $v(\Delta)$ is even and $E$ has Néron type different from $I_0^*$, or equivalently, by Lemma 3.2, if $v(\Delta)$ is even and $E$ has a 2-torsion point not defined over $K^{nr}$. In fact if $v(\Delta)$ is even then $[L : K^{nr}] < 12$, and if there exists a non-trivial 2-torsion point not defined over $K^{nr}$ then it gives at least a cubic extension, so $3 \mid [L : K^{nr}]$ and hence $\mathrm{Gal}(L/K^{nr})$, that is a subgroup of $C_3 \rtimes C_4$, is cyclic of order 3 or 6. Conversely, if $E$ has wild cyclic reduction then $3 \mid [L : K^{nr}]$ and so there is at least one 2-torsion point not defined over $K^{nr}$, and by the above $v(\Delta)$ is even. Fix a Weierstrass equation for $E$, of the form $y^2 = f(x)$, and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f$ in $\overline{K}$. Notice that, since $E$ has potentially good reduction, the differences $\alpha_i - \alpha_j$ for $i \neq j$ all have the same valuation over their field of definition (see also Remark 6.9), therefore adjoining any of $\alpha_1$, $\alpha_2$, $\alpha_3$ to $K^{nr}$ gives an

extension of the same degree.

Let $F = K(\alpha_1)$. Then the Galois closure of $F/K$ is $K(E[2])$.

If $v(\Delta) \equiv 0 \pmod 4$, we fix $\mathrm{Frob}_K$ to be the Frobenius element of $\mathrm{Gal}(\overline{K}/K)$ that fixes $F$ point-wise. If $v(\Delta) \equiv 2 \pmod 4$ and $E$ has type different from $I_0^*$, we fix $\mathrm{Frob}_K$ to be the Frobenius element of $\mathrm{Gal}(\overline{K}/K)$ that fixes $F$ point-wise and a square root $\sqrt{\pi_K}$ of the uniformiser of $K$.

We will prove the following result.

**Theorem 5.1.** *Let $K$ be a 3-adic field and let $E/K$ have wild cyclic reduction. Let $\chi$ be the unramified character of $\mathrm{Gal}(\overline{K}/K)$ that sends $\mathrm{Frob}_K$ to $\sqrt{-|k|}$ (which we identify with $i\sqrt{|k|} \in \mathbb{C}$).*

*(a) If $v(\Delta) \equiv 0 \pmod 4$ and $[K(E[2]) : K] = 6$, then $\rho_{E,\ell} = \chi \otimes \psi$, where $\psi$ is the unique irreducible 2-dimensional representation of $S_3$.*

*(b) If $v(\Delta) \equiv 0 \pmod 4$ and $[K(E[2]) : K] = 3$, then:*

*(i) if there are $\alpha_i$ and $\alpha_j$ such that $\alpha_i - \alpha_j$ is a square in $K(E[2])$, let $\sigma \in I_K$ be the element of order 3 that acts on the roots of $f$ as $\sigma(\alpha_j) = \alpha_i$, and let*

$$\begin{aligned} \psi : \quad & I_K \to \overline{\mathbb{Q}}_\ell^\times \\ & \sigma \mapsto \frac{-1-\sqrt{-3}}{2}; \end{aligned} \tag{5.1}$$

*then $\rho_{E,\ell} = \chi \otimes \psi \oplus \overline{\chi} \otimes \overline{\psi}$, where $\overline{\bullet}$ denotes complex conjugation;*

*(ii) otherwise, let $\sigma \in I_K$ permute cyclically the roots of $f$, with $\sigma(\alpha_1) = \alpha_2$, and let $\psi$ be defined analogously as in case (b.i), then $\rho_{E,\ell} = \overline{\chi} \otimes \psi \oplus \chi \otimes \overline{\psi}$.*

*(c) If $v(\Delta) \equiv 2 \pmod 4$ and $E$ has Néron type different from $I_0^*$, let $\chi_\pi$ be the quadratic character of $K(\sqrt{\pi_K})/K$. Then $E_\pi$, the quadratic twist of $E$ by $K(\sqrt{\pi_K})$, has wild cyclic reduction and satisfies $v(\Delta) \equiv 0 \pmod 4$. We have $\rho_{E,\ell} = \rho_{E_\pi,\ell} \otimes \chi_\pi$.*

In the rest of this section, we prove each case separately.

**Proof of case (a)** Since $F/K$ is totally ramified of degree 3, and by Theorem 2.8 we know that $I = \rho_{E,\ell}(I_K) \cong C_3$, then $E$ acquires good reduction over $F$. Then as $[K(E[2]) : K] = 6$ we have that $K(E[2])/F$ is quadratic and unramified. The same proof as the one for Theorem 2.12, case (b.ii), shows that $\rho_{E,\ell}(\mathrm{Frob}_K)$ has eigenvalues $\pm\sqrt{-|k|}$. Let $\chi$ be as in the statement. Then $\psi = \rho_{E,\ell} \otimes \chi^{-1}$ factors through $\mathrm{Gal}(K(E[2])/K)$, which is isomorphic to $S_3$. Since $\psi\big|_{I_K}$ acts with image isomorphic to $C_3$, and seen as a representation of $C_3$ it is faithful, by direct inspection of the 2-dimensional representations of $S_3$ we deduce that $\psi$ is irreducible, so as a representation of $S_3$ it is the unique 2-dimensional irreducible (and faithful) representation of $S_3$. ■

For the proof of case (b.i), we assume first that $n = [k : \mathbb{F}_3]$ is odd. At the end of the proof, we will highlight what changes if $n$ is even.

**Proof of case (b.i).** Assume that $n = [k : \mathbb{F}_3]$ is odd. Up to relabeling, suppose that $\alpha_2 - \alpha_1$ is a square in $F = K(E[2])$, and fix a square root $\sqrt{\alpha_2 - \alpha_1} \in F$. The following change of variables

$$\begin{cases} x &= (\alpha_2 - \alpha_1)x' + \alpha_1, \\ y &= \sqrt{(\alpha_2 - \alpha_1)^3}\, y' \end{cases} \tag{5.2}$$

is defined over $F$ and gives a model for the base change of $E$ to $F$ that reduces to $\tilde{E} : y^2 = x^3 - x$ over $k$ (for the proof, see Lemma 3.6). Therefore, by Example 2.14, the eigenvalues of $\rho_{E,\ell}(\mathrm{Frob}_K)$ are $\pm\sqrt{-|k|}$. We fix $\sigma \in I_K$ that permutes cyclically $\alpha_1, \alpha_2, \alpha_3$ and satisfies $\sigma(\alpha_1) = \alpha_2$, as in the statement. Then $\rho_{E,\ell}(\sigma)$ has determinant 1 (by the properties of the Weil pairing) and order 3, so it has eigenvalues given by the two primitive third roots of unity.

Since the image of $\rho_{E,\ell}$ is abelian, being isomorphic to $\mathrm{Gal}(F^{nr}/K)$ which is the direct product of $\mathrm{Gal}(F/K)$ and $\mathrm{Gal}(K^{nr}/K)$, we have a splitting of the form $\rho_{E,\ell} = \rho_1 \oplus \rho_2$, where the $\rho_i$'s are 1-dimensional. From the above, we know that, up to relabeling, $\rho_1(\mathrm{Frob}_K) = \chi(\mathrm{Frob}_K) = \sqrt{-|k|}$, $\rho_2(\mathrm{Frob}_K) = \overline{\chi}(\mathrm{Frob}_K) = -\sqrt{-|k|}$ and $\rho_1(\sigma)$, $\rho_2(\sigma)$ are the two primitive third roots of unity, and it is only necessary to distinguish between the two.

The same argument as in the proof of Theorem 3.1 (more precisely in Section 3.3) can be applied here, and it shows that $\rho_1(\sigma) = \dfrac{-1-\sqrt{-3}}{2}$, and $\rho_2(\sigma) = \dfrac{-1+\sqrt{-3}}{2}$. So, if we define $\psi : I_K \to \overline{\mathbb{Q}}_\ell^\times$ such that $\psi(\sigma) = \dfrac{-1-\sqrt{-3}}{2}$, we have

$$\rho_{E,\ell} = \chi \otimes \psi \oplus \overline{\chi} \otimes \overline{\psi}, \tag{5.3}$$

as claimed. ∎

**Remark 5.2.** *If $n = [k : \mathbb{F}_3]$ is even, we still have the same good model for $E$ over $F$, and we can compute the eigenvalues of Frobenius as in Example 2.14, obtaining two identical real values, namely $(-3)^{n/2}$. In this case, we simply have $\rho_{E,\ell} = \chi \otimes (\psi \oplus \overline{\psi})$, for $\psi$ defined as in the statement. Since $\chi = \overline{\chi}$, we still recover $\rho_{E,\ell} = \chi \otimes \psi \oplus \overline{\chi} \otimes \overline{\psi}$.*

**Proof of case (b.ii).** If all the $\alpha_i - \alpha_j$'s are not squares in $F = K(E[2])$, then $F(\sqrt{\alpha_2 - \alpha_1})$ is quadratic and unramified over $F$. In fact, we have $v(\Delta) \equiv 0 \pmod 4$ by assumption, and if $v_F$ is the normalised valuation on $F$, we have $v(\Delta) = v_F(\Delta)/3 = 2v_F(\alpha_2 - \alpha_1)$, since $E$ has potentially good reduction. Therefore $v_F(\alpha_2 - \alpha_1)$ is even, so we can write $\alpha_2 - \alpha_1 = \pi_F^{2a}\epsilon$, where $\pi_F$ is a uniformiser of $F$, $a \in \mathbb{Z}$ and $\epsilon \in \mathcal{O}_F^\times$ is not a square. Moreover, we can take $\pi_F$ and $\epsilon$ so that $\epsilon \in \mathcal{O}_K^\times$. Let $E_\epsilon$ be the twist of $E$ be $K(\sqrt{\epsilon})$, then $E_\epsilon$ is as in case (b.i) of the theorem. In fact, since $K(\sqrt{\epsilon})/K$ is unramified, $E_\epsilon$ also has wild cyclic reduction over $K$ with image of inertia $C_3$, moreover an equation for $E_\epsilon$ is

$$y^2 = (x - \epsilon\alpha_1)(x - \epsilon\alpha_2)(x - \epsilon\alpha_3), \tag{5.4}$$

so $\epsilon\alpha_2 - \epsilon\alpha_1 = \epsilon^2\pi_F^{2a}$ is a square in $F$.

By case (b.i), we have $\rho_{E_\epsilon,\ell} = \chi \otimes \psi \oplus \overline{\chi} \otimes \overline{\psi}$, where $\chi$ and $\psi$ are as in the statement. Let $\eta : \mathrm{Gal}(\overline{K}/K) \to \{\pm 1\}$ be the unramified quadratic character of $\mathrm{Gal}(\overline{K}/K)$. Then $\rho_{E_\epsilon,\ell} = \rho_{E,\ell} \otimes \eta$, and an immediate computation shows that

$$\rho_{E,\ell} = \overline{\chi} \otimes \psi \oplus \chi \otimes \overline{\psi}, \tag{5.5}$$

as claimed. ■

**Proof of case (c).** In this case, by Theorem 2.8, we have $I = \rho_{E,\ell}(I_K) \cong C_6$. Let $E_\pi$ be the twist of $E$ by $K(\sqrt{\pi_K})$. Then the discriminant of $E_\pi$ is equal to $\pi_K^6 \Delta$, and $v(\pi^6\Delta) = 6 + v(\Delta) \equiv 0 \pmod 4$. Therefore, if $\chi_\pi$ is the quadratic character of $\mathrm{Gal}(K(\sqrt{\pi_K})/K)$, we have $\rho_{E,\ell} = \rho_{E_\pi,\ell} \otimes \chi_\pi$, where $\rho_{E_\pi,\ell}$ is given by one of cases (a), (b.i) or (b.ii). ■

## 5.2 The case $p = 2$

We assume for this section that $p = 2$. Recall that $E/K$ has wild cyclic reduction exactly when the image of inertia $I = \rho_{E,\ell}(I_K)$ is one of $C_2$, $C_4$ or $C_6$, and Theorem 2.9 classifies these three cases.

We first consider the problem of the restriction to inertia of $\rho_{E,\ell}$ for $I \cong C_2$ or $C_6$. In order to do so, we start by viewing $E$ as an elliptic curve over $K^{nr}$, since the reduction type and the action of inertia do not change. In particular, we have $\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K^{nr}) \to \mathrm{Aut}(T_\ell(E))$.

**Lemma 5.3.** *Let $E/K^{nr}$ be an elliptic curve with wild cyclic reduction and $I \ncong C_4$. Then:*

- *if $I \cong C_2$ then $E$ is a quadratic ramified twist of an elliptic curve with good reduction;*
- *if $I \cong C_6$ then $E$ is a quadratic ramified twist of an elliptic curve with tame potentially good reduction.*

The proof is essentially [6, Proposition 4.3].

**Proof.** Assume first that $I \cong C_2$.

Let $L = K^{nr}(E[3])$. Then, by Theorem 2.10, we have $I \cong \mathrm{Gal}(L/K^{nr})$, so $L/K^{nr}$ is quadratic. Then the quadratic twist $E'$ of $E$ by $L$ has good reduction.

Assume now that $I \cong C_6$ and let $L$ be as above. Then $L/K^{nr}$ is cyclic of order 6 and there is a unique quadratic subextension $M/K^{nr}$. The quadratic twist of $E$ by $M$ has tame potentially good reduction (achieved over $L$), with inertia image that is cyclic of order 3. ■

We now show that, in fact, there exists a quadratic extension of the base field $K$, over which $E$ acquires good or tame reduction.

**Lemma 5.4.** *Let $E/K$ be an elliptic curve with wild cyclic reduction and $I \ncong C_4$. Then:*

- *if $I \cong C_2$ then $E$ is a quadratic ramified twist of an elliptic curve with good reduction;*

- *if $I \cong C_6$ then $E$ is a quadratic ramified twist of an elliptic curve with tame potentially good reduction.*

**Proof.** Assume that $I \cong C_2$ and let $L = K^{nr}(E[3])$ as in the proof of Lemma 5.3. Then $\mathrm{Gal}(L/K)$ has inertia subgroup isomorphic to $C_2$, and the quotient is the procyclic group $\hat{\mathbb{Z}}$. Therefore, $\mathrm{Gal}(L/K)$ is a semidirect product $C_2 \rtimes \hat{\mathbb{Z}}$, with $C_2$ normal in $\mathrm{Gal}(L/K)$; but then the action of $\hat{\mathbb{Z}}$ can only be trivial, so in fact $\mathrm{Gal}(L/K) = C_2 \times \hat{\mathbb{Z}}$. In particular, we can consider the intermediate extension $F/K$ which is fixed by $\hat{\mathbb{Z}}$: this is Galois, quadratic and totally ramified, with $L/F$ unramified, therefore $E$ acquires good reduction over $F$.

If $I \cong C_6$, let $L$ and $M$ be as in the proof of Lemma 5.3, then $\mathrm{Gal}(M/K)$ is isomorphic to the direct product $C_2 \times \hat{\mathbb{Z}}$ as in the previous case, and again by taking $F$ to be the fixed field of $\hat{\mathbb{Z}}$ we conclude. ■

Notice that Lemma 5.4 shows the existence of a quadratic extension of $K$ over which the curve acquires good or tame reduction, but it does not give an algorithmic result to compute it. Indeed, if $p = 2$, there are several quadratic ramified extensions of $K$ and we need to consider one such that its maximal unramified extension is equal to the field $L$ in the proof of Lemma 5.4 above. Determining explicitly this extension is a non-trivial problem, which we do not tackle here. However, some partial explicit results are available if we restrict to $K = \mathbb{Q}_2$, namely [14, §4.1, Lemma 2].

Assuming we have computed a quadratic twist $E'/K$ of $E$ with good or tame reduction, and if $\eta$ is the corresponding quadratic character, then $\rho_{E,\ell} = \rho_{E',\ell} \otimes \eta$, and $\rho_{E',\ell}$ is determined by Theorem 2.5 if $I \cong C_2$ and Theorem 2.12 case (b) if $I \cong C_6$.

For the rest of the section, we focus on the remaining wild cyclic case, that is $I \cong C_4$. We fix an arithmetic Frobenius element $\mathrm{Frob}_K$ of $\mathrm{Gal}(\overline{K}/K)$. We will specify which Frobenius we choose when the choice is relevant. Let $n = [k : \mathbb{F}_2]$ be the absolute inertia degree of $K$. We define the following unramified character of $\mathrm{Gal}(\overline{K}/K)$:

$$\begin{aligned} \chi : \quad & \mathrm{Gal}(\overline{K}/K) \to \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C} \\ & \mathrm{Frob}_K \mapsto (\sqrt{-2})^n \mapsto (i\sqrt{2})^n. \end{aligned} \tag{5.6}$$

Let $G = \mathrm{Gal}(K(E[3])/K)$. Then $G$ is naturally embedded into $\mathrm{GL}_2(\mathbb{F}_3)$, with the embedding given by fixing a basis for $E[3]$ as a $\mathbb{F}_3$-vector space. We will show that $\rho_{E,\ell} \otimes \chi^{-1}$ factors through $G$, and more precisely we will prove the following result.

**Theorem 5.5.** *Let $G = \mathrm{Gal}(K(E[3])/K)$ and suppose $I \cong C_4$. Then one of the following holds.*

*(a) $G \cong C_4$ and $\rho_{E,\ell} = \chi \otimes (\psi \oplus \overline{\psi})$, where*

$$\begin{aligned} \psi : \quad & G \to \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C} \\ & \sigma \mapsto i \end{aligned} \tag{5.7}$$

*for any fixed choice of a generator $\sigma$ of $G$;*

*(b)* $G \cong Q_8$ *or* $D_4$ *and* $\rho_{E,\ell} = \chi \otimes \psi$*, where* $\psi$ *is the only irreducible faithful* 2*-dimensional representation of* $G$*;*

*(c)* $G \cong C_8$ *and* $\rho_{E,\ell} = \chi \otimes (\psi \oplus \overline{\psi})$*, where* $\psi$ *is the faithful character of* $C_8$ *that maps* $g$ *to the* 8*-th root of unity* $\dfrac{-\sqrt{2}+\sqrt{-2}}{2}$*, and* $g$*, seen as an element of* $\mathrm{GL}_2(\mathbb{F}_3)$*, is* $\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$.

**Remark 5.6.** *Determining which of cases (a), (b) or (c) occurs can be done, for instance, via [9, §3, Proposition 2 and Lemma 3].*

**Proof.** By definition, $I = \rho_{E,\ell}(I_K)$ is the image of the absolute inertia subgroup via $\rho_{E,\ell}$. Then we know, by Theorem 2.10, that $I \cong \mathrm{Gal}(K^{nr}(E[3])/K^{nr})$, so $I$ is isomorphic to the inertia subgroup of $G$. Therefore, $I$ is a normal subgroup of $G$ with cyclic quotient. By the classification in [9, §3, Proposition 2], it follows that there are only four possibilities for $G$ in order to have $I \cong C_4$, namely $G$ is one of $C_4, Q_8, D_4$ or $C_8$. Notice, in particular, that in each of these cases $K$ contains a third root of the discriminant of $E$, and we have that $n$ is even if $G \cong C_4, Q_8$, while $n$ is odd if $G \cong D_4$ or $C_8$.

Suppose first that $G \cong I \cong C_4$. Then $K(E[3])$ is a quartic extension of $K$, generated by the coordinates of one point of $E$ of order 3, and following the proof of Lemma 4.2 we obtain that there exists a model for the base change of $E$ to $K(E[3])$ that reduces to $y^2 + y = x^3$ over the residue field $k$. In particular, if we fix $\mathrm{Frob}_K$ to be the arithmetic Frobenius that fixes $K(E[3])$ point-wise, we have that $\rho_{E,\ell}(\mathrm{Frob}_K)$ has eigenvalues $(\pm\sqrt{-2})^n$, and since $n$ is even this means that $\rho_{E,\ell}(\mathrm{Frob}_K)$ is the scalar matrix $(-2)^{n/2}\,\mathrm{Id}_2$. Therefore, $\rho_{E,\ell} \otimes \chi^{-1}$ factors through $G \cong I$, and as a representation of $I$ it is faithful with trivial determinant. By direct inspection on the character table of the group $C_4$ (see [7]), we deduce that $\rho_{E,\ell} \otimes \chi^{-1}$ is the direct sum of the two one-dimensional faithful representations of $C_4$, hence it is $\psi \oplus \overline{\psi}$ where $\psi$ is as in the statement.

Now suppose that $G \cong Q_8$ or $D_4$. Then $G$ is non-abelian, so by [9, §2, Lemma 1] we have that $\rho_{E,\ell} \otimes \chi^{-1}$ factors through $G$, and as a representation of $G$ it is irreducible and faithful. Since both $Q_8$ and $D_4$ have only one 2-dimensional irreducible representation (which is also faithful), case (b) of the theorem holds.

Finally we assume that $G \cong C_8$. In this case, since $G$ is cyclic, there exists a unique subextension of $K(E[3])$ of degree 2 over $K$, namely the unramified extension $K_2$ generated by a primitive third root of unity in $\overline{K}$. Notice that, in particular, this means that $K(E[3])$ is not the compositum of a quartic totally ramified extension of $K$ with a quadratic unramified extension of $K$, because every extension of $K$ contains $K_2$, hence it is not totally ramified.

We have that $I \cong \mathrm{Gal}(K(E[3])/K_2)$, and the restriction $\rho_{E,\ell}\big|_{I_K}$ factors through $I$. By [17, Figure 4.3] we know that the 3-division polynomial of $E$ over $K_2$ factors as the product of two quadratic factors, so there are two points $P, Q \in E[3] \setminus \{O\}$ such that the abscissas $x_P, x_Q$ are different but in the same $I$-orbit.

We fix the following generator $\sigma$ of $I$: it is the element that acts on $E[3]$ as

$$\begin{cases} P & \mapsto & Q, \\ Q & \mapsto & -P; \end{cases} \tag{5.8}$$

so if we fix $\{P, Q\}$ as a basis for $E[3]$ over $\mathbb{F}_3$ we identify $\sigma$ with the matrix

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}. \tag{5.9}$$

We now want to fix a generator $g$ of $G$, and to do so we observe that there are exactly two elements in $\mathrm{GL}_2(\mathbb{F}_3)$ that have square equal to $\sigma$, and they both are in $G$, namely $\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$ as in the statement, and $\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$. We fix $g = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$. Let us consider the representation $\rho_{E,\ell} \otimes \chi^{-1}$. Again by the same proof as in Lemma 4.2, we have that a model for the base change of $E$ to $K(E[3])$ reduces to $y^2 + y = x^3$, thus the Frobenius element of $K(E[3])$, which has inertia degree 2 over $K$, acts as the scalar matrix $(-2)^n \mathrm{Id}_2$. We therefore have that the arithmetic Frobenius of $K$ has distinct eigenvalues $\pm(\sqrt{-2})^n$, so $\rho_{E,\ell} \otimes \chi^{-1}$ factors through $G$. We fix $\mathrm{Frob}_K$ to be the Frobenius element of $K$ that is mapped to $g$ under the quotient map: $\mathrm{Gal}(\overline{K}/K) \to G$. Moreover, the restriction to inertia of $\rho_{E,\ell} \otimes \chi^{-1}$ factors through $I \cong C_4$, and as a representation of $C_4$ it is faithful with trivial determinant. Therefore $\rho_{E,\ell} \otimes \chi^{-1} = \psi_a \oplus \psi_b$, where $\psi_a$ and $\psi_b$ are two of the four one-dimensional representations of $C_8$, which are listed in [7]. Namely, the possible representations are denoted in op. cit. by $\rho_3, \rho_5, \rho_6, \rho_8$, and we identify $g$ with the conjugacy class denoted by 8A, and the eighth root of unity $\zeta_8$ with the complex number $e^{2\pi i/8} = \dfrac{\sqrt{2} + \sqrt{-2}}{2}$. Using that the restriction to inertia has trivial determinant, we deduce that the only possibilities for the set $\{\psi_a, \psi_b\}$ are:

$$\{\rho_3, \rho_5\},\ \{\rho_3, \rho_8\},\ \{\rho_5, \rho_6\},\ \{\rho_6, \rho_8\}, \tag{5.10}$$

and in particular $\psi_b = \overline{\psi_a}$. Let $\psi = \psi_a$. Now we have

$$\rho_{E,\ell}(\mathrm{Frob}_K) = \chi(\mathrm{Frob}_K)(\psi + \overline{\psi})(g). \tag{5.11}$$

Let us fix $\ell = 3$. Then, the reduction modulo 3 of $\rho_{E,\ell}$ is equal to the modulo 3 Galois representation, i.e. the one given by the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[3]$, so we have that $\rho_{E,\ell}(\mathrm{Frob}_K)$ reduces to $g = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \pmod 3$, which has trace 1 and determinant 2. A direct computation shows that the only pair in List 5.10 for which this occurs is $\{\rho_6, \rho_8\}$, so the representation $\rho_{E,\ell}$ is given by

$$\rho_{E,\ell} = \chi \otimes (\rho_6 \oplus \rho_8) \tag{5.12}$$

and this concludes the proof since $\rho_6(g) = \zeta_8^3 = \dfrac{-\sqrt{2} + \sqrt{-2}}{2}$. ∎

CHAPTER 6

# A FAMILY OF HYPERELLIPTIC CURVES WITH LARGE INERTIA IMAGE

In this final chapter, we generalise the main result of Chapter 3 to the family of hyperelliptic curves with potentially good reduction over a $p$-adic field, which have genus $(p-1)/2$, a Weierstrass rational point and the largest possible image of inertia under the $\ell$-adic Galois representation associated to their Jacobian. We will prove that this Galois representation factors as the tensor product of an unramified character and an irreducible representation of a finite group, which can be either equal to the inertia image (in which case the representation is easily determined) or a $C_2$-extension of it. In this second case, there are two suitable representations and we will describe the Galois action explicitly in order to determine the correct one.

This result is surprisingly similar to Theorem 3.1, although the proof requires more general techniques which involve a detailed study of representations of finite groups.

This chapter is a modified version of the author's paper "Wild Galois representations: a family of hyperelliptic curves with large inertia image", currently submitted for publication ([4]).

## 6.1 Introduction

A hyperelliptic curve over a field $K$ is a smooth projective algebraic curve $X$ of genus $g \geq 2$ that has the structure of a degree 2 cover of $\mathbb{P}^1$. The results of this chapter also hold for elliptic curves, and the main theorem is in fact proved in §3, so throughout this chapter we will implicitly include the case of $X$ being an elliptic curve. Similarly as with elliptic curves, we can identify a hyperelliptic curve with an affine Weierstrass equation, i.e. an equation of the form

$$X : y^2 + h(x)y = f(x), \tag{6.1}$$

where $h(x)$ and $f(x)$ are polynomials with coefficients in $K$ with $\deg(h) \leq g$ and $\deg(f) \in \{2g+1, 2g+2\}$. By this, we mean that the function field of $X$ is isomorphic to

$$K(x)[y]/(y^2 + h(x)y - f(x)). \tag{6.2}$$

Note that, if $\mathrm{char}(K) \neq 2$, after a change of coordinates it is always possible to assume that $h(x) = 0$.

One important difference between elliptic curves and higher genus hyperelliptic curves is that the set of points on the latter does not have a group structure. However, it is possible to associate an abelian variety to any curve $X$, namely the Jacobian variety $\mathrm{Jac}(X)$, and study the group structure on it. If $\overline{K}$ is a fixed separable closure of $K$, we denote by $\mathrm{Jac}(X)(\overline{K})$ the set of points defined over $\overline{K}$ and lying on $\mathrm{Jac}(X)$. For the definition of the Jacobian of a curve, see e.g. [16, §1]. In particular we can define, for a prime $\ell$, the $\ell$-adic Tate module, which is

$$T_\ell \mathrm{Jac}(X) = \varprojlim_n \mathrm{Jac}(X)[\ell^n], \tag{6.3}$$

where by $\mathrm{Jac}(X)[m]$ we denote the subgroup of $m$-torsion points of $\mathrm{Jac}(X)(\overline{K})$. It can be proved that, for $\ell$ different from the characteristic of $K$, this is a free $\mathbb{Z}_\ell$-module of rank $2g$.

Let $\mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of $K$. Then we have a linear action on the points of $\mathrm{Jac}(X)$, and an induced action on the Tate modules, thus we can define, for any prime $\ell$ (different from $\mathrm{char}(K)$) a Galois representation

$$\rho_{J,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell \mathrm{Jac}(X)). \tag{6.4}$$

After taking the tensor product with $\overline{\mathbb{Q}}_\ell$, and fixing a basis for $T_\ell \mathrm{Jac}(X) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$, we can and will consider $\mathrm{Aut}(T_\ell \mathrm{Jac}(X))$ as a subgroup of $\mathrm{GL}_{2g}(\overline{\mathbb{Q}}_\ell)$.

From this moment on, we assume that $K$ is a non-archimedean local field of characteristic 0, i.e. a finite extension of $\mathbb{Q}_p$ for some prime $p$; we also assume that $p \neq \ell$. As usual, we denote by $v$ the valuation on $K$, by $\mathcal{O}_K$ the ring of integers, by $\pi_K$ a uniformiser, by $k$ the residue field, with algebraic closure $\overline{k}$, and by $K^{nr}$ the maximal unramified extension of $K$ contained in $\overline{K}$. Let $I_K$ be the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ and $\mathrm{Frob}_K$ be any arithmetic Frobenius of $\mathrm{Gal}(\overline{K}/K)$. In Section 6.4 we fix a precise choice of $\mathrm{Frob}_K$.

In Section 6.2 we give the statement of the main result of this chapter. In Section 6.3 we describe explicitly the action of inertia in our setting, using [11, Theorem 10.3] and [20, §8.2, Proposition 25]. In Section 6.4 we use a good model for the family of curves we are interested in, to compute the eigenvalues of Frobenius. Finally in Section 6.5 we give details about the proof, in particular in the case where the inertia degree of $K/\mathbb{Q}_p$ is odd, when the work of Sections 6.3 and 6.4 is not sufficient to describe the full Galois representation.

## 6.2 Statement of the main results

Let $K$ be a $p$-adic field as in the previous section and let $X$ be an hyperelliptic curve over $K$ of the form:

$$X : y^2 = f(x) \tag{6.5}$$

with $f \in K[x]$ monic, of degree $p$. (Recall that the genus $g$ of the curve satisfies $p = 2g+1$). Suppose that $X$ has potentially good reduction over $K$, i.e. there exists a finite extension $F/K$ such that the base changed curve $X \times_K F$ has good reduction. Then by the Criterion of Néron-Ogg-Shafarevich (see [19, §2, Theorem 2(ii)]), the Galois representation $\rho_{J,\ell}$ restricted to inertia factors through a finite quotient. We assume that this quotient has the largest possible size. The first result characterises the hyperelliptic curves that satisfy these assumption. Let $\alpha_1, \ldots, \alpha_p \in \overline{K}$ be the roots of $f$, $\Delta$ be the discriminant of $f$, and let $G = \mathrm{Gal}(K(\{\sqrt{\alpha_i - \alpha_j}\}_{i \neq j})/K)$. Moreover let $I$ be the inertia subgroup of $G$.

**Proposition 6.1.** *Let $X : y^2 = f(x)$ be a hyperelliptic curve such that $\deg(f) = p$ over a $p$-adic field $K$, with potentially good reduction, and let $\rho_{J,\ell}$ be the $\ell$-adic Galois representation associated to it. Then $|\rho_{J,\ell}(I_K)|$ is maximal and equal to $2p(p-1)$ if and only if*

- *the Galois group of the splitting field of $f$ over $K^{nr}$ is isomorphic to the Frobenius group $C_p \rtimes C_{p-1}$, and*
- *$v(\Delta)$ is odd.*

*Furthermore, $\rho_{J,\ell}(I_K) \cong I$. The structure of the group $I$ when these two conditions hold is that of the semidirect product $C_p \rtimes C_{2(p-1)}$ of $C_p$ and $C_{2(p-1)}$ which has a degree 2 quotient isomorphic to the Frobenius group $C_p \rtimes C_{p-1}$.*

The first condition in this proposition is expensive to check computationally, however the following result gives two conditions that imply those above and are easier to verify. Throughout the rest of the chapter we will assume for simplicity that these two new conditions hold, however they can be replaced by the general ones, in fact the main theorem of this chapter holds whenever the image of inertia is maximal, in the sense of Proposition 6.1. Notice furthermore that, since the characteristic of $K$ is 0, the existence of a defining equation for $X$ satisfying $\deg(f) = p$ is equivalent to $X$ having genus $(p-1)/2$ and a rational Weierstrass point.

**Proposition 6.2.** *The conditions in Proposition 6.1 are implied by the following two:*

- *$f$ is irreducible over $K$;*
- *$(v(\Delta), p-1) = 1$.*

For the proof of these statements see Section 6.3.

Let $F = K(\alpha_1, \ldots, \alpha_p, \sqrt{\alpha_2 - \alpha_1})$. We will prove that if the conditions in Proposition 6.2 hold, $F/K$ is totally ramified and $X$ acquires good reduction over $F$. Moreover if the absolute inertia degree $f_{K/\mathbb{Q}_p}$ of $K$ is even, then $F = K(\{\sqrt{\alpha_i - \alpha_j}\}_{i \neq j})$ and so $G = I$, otherwise $G$ is isomorphic to a semidirect product of the form $I \rtimes C_2$. Let us now fix a numbering on the roots and an element $\sigma \in I$ such that:

$$\sigma : \alpha_1 \mapsto \alpha_2 \mapsto \cdots \mapsto \alpha_p \mapsto \alpha_1 \tag{6.6}$$

and $\sigma(\sqrt{\alpha_i - \alpha_j}) = \sqrt{\sigma(\alpha_i) - \sigma(\alpha_j)}$ for all $i, j$. Moreover, for odd $f_{K/\mathbb{Q}_p}$, let $\phi$ be the non-trivial element of $G$ that fixes the field $F$. For each prime $\ell \neq p$ we fix an embedding $\overline{\mathbb{Q}}_\ell \to \mathbb{C}$. In particular we identify $\sqrt{p}$ with the positive real square root of $p$, $\sqrt{-p}$ with the complex number $i\sqrt{p}$.

We will prove the following main result.

**Theorem 6.3.** *Let $X/K : y^2 = f(x)$ be a hyperelliptic curve over a $p$-adic field of genus $(p-1)/2$ and a rational Weierstrass point with potentially good reduction and let $\rho_{J,\ell}$ be the $\ell$-adic Galois representation attached to* Jac$(X)$*, for $\ell \neq p$. Suppose that $f$ is irreducible over $K$ and that the valuation of the discriminant of $f$ is coprime to $p-1$. Let $G, I, \sigma, \phi$ be as above.*

*Then $\rho_{J,\ell}$ is irreducible and factors as $\rho_{J,\ell} = \chi \otimes \psi$, where:*

$$\begin{aligned} \chi : \mathrm{Gal}(\overline{K}/K) &\to \overline{\mathbb{Q}}_\ell^\times \\ I_K &\mapsto 1 \\ \mathrm{Frob}_K &\mapsto \left(\sqrt{\left(\frac{-1}{p}\right)p}\right)^{f_{K/\mathbb{Q}_p}} \end{aligned} \tag{6.7}$$

*and:*

- *if $f_{K/\mathbb{Q}_p}$ is even, $\psi$ is the unique irreducible faithful representation of $G = I$ of dimension $p-1$;*
- *if $f_{K/\mathbb{Q}_p}$ is odd, $\psi$ is the unique irreducible faithful representation of $G \cong I \rtimes C_2$ of dimension $p-1$ such that* $\mathrm{tr}(\psi(\sigma\phi)) = -\sqrt{\left(\frac{-1}{p}\right)p}$.

In order to prove this theorem, we follow this strategy: first we determine the Galois representation restricted to inertia, then we find a model of $X \times_K F$ reducing to $y^2 = x^p - x$ over the residue field, and use this to determine the action of $\rho_{J,\ell}(\mathrm{Frob}_K)$. If $f_{K/\mathbb{Q}_p}$ is even, then this information is enough to determine the full Galois action, otherwise there are two representations that, when restricted to inertia, give the same result, and the two only differ by the trace of the elements that are products of Frobenius with a wild inertia automorphism. We will compute explicitly the trace of one such element, namely $\sigma\,\mathrm{Frob}_K$ where $\sigma$ is defined above, using again the good model $y^2 = x^p - x$, to conclude.

**Remark 6.4.** *Such curves exist: for example let* $X/\mathbb{Q}_p : y^2 = f(x) = x^p - p$. *Then* $f$ *is irreducible over* $\mathbb{Q}_p$ *and* $v(\Delta) = 2p-1$ *is relatively prime to* $p-1$.

## 6.3 The inertia action

In this section we prove Propositions 6.1, 6.2 and we use Proposition 25 in [20, §8.2] to determine the restriction to inertia of $\rho_{J,\ell}$.

### 6.3.1 Proof of Propositions 6.1 and 6.2

**Remark 6.5** (Cluster picture for the curve)**.** *Recall that for a hyperelliptic curve of the form* $y^2 = f(x)$, *a cluster is a subset of the set of all roots of* $f$ *in* $\overline{K}$ *with the property that the difference of any two different elements of it has valuation* $\leq \delta$, *for some* $\delta \in \mathbb{R}$. *For more detailed definitions, see [11, §1].*

*Suppose that* $X : y^2 = f(x)$, *with* $f(x) \in K[x]$ *of degree* $p$ *and roots* $\alpha_1, \ldots, \alpha_p \in \overline{K}$; *note in particular that, if* $g$ *is the genus of the curve, then* $p = 2g+1$. *By [11, §10, Theorem 10.3], we have that* $X$ *has potentially good reduction if and only if the cluster picture consists of a unique cluster* $R$ *of size* $p$ *containing all the roots. In this case,* $\mathrm{Jac}(X)$ *also has potentially good reduction.*

By the Criterion of Néron-Ogg-Shafarevich (see [19, §2, Theorem 2(ii)]), the Galois representation $\rho_{J,\ell}$ on $T_\ell \mathrm{Jac}(X)$, restricted to inertia, has finite image, independent of $\ell$ if $\ell \neq p$. Moreover by Corollary 3 in the same paper, this image is isomorphic to $\mathrm{Gal}(K^{nr}(\mathrm{Jac}(X)[m])/K^{nr})$ for any $m \geq 3$ coprime to $p$, and $K^{nr}(\mathrm{Jac}(X)[m])$ is the minimal extension of $K^{nr}$ over which $\mathrm{Jac}(X)$ acquires good reduction. We can fix $m = 4$; then by [25, Theorem 1.1], we have that

$$L := K^{nr}(\mathrm{Jac}(X)[4]) = K^{nr}(\{\sqrt{\alpha_i - \alpha_j}\}_{i,j \in \{1,\ldots,p\}}). \tag{6.8}$$

We denote by $C_p \rtimes C_{2(p-1)}$ the semidirect product of $C_p$ and $C_{2(p-1)}$ which has a degree 2 quotient isomorphic to the Frobenius group $C_p \rtimes C_{p-1}$.

**Lemma 6.6.** *Suppose that* $X : y^2 = f(x)$ *is a hyperelliptic curve with* $\deg(f) = p$ *over a* $p$*-adic field* $K$ *with potentially good reduction and let* $\rho_{J,\ell}, \mathrm{Gal}(\overline{K}/K), I_K, L$ *be as above. Assume that* $f$ *is irreducible over* $K^{nr}$. *Then* $\rho_{J,\ell}(I_K) \cong \mathrm{Gal}(L/K^{nr})$ *is isomorphic to a subgroup of* $C_p \rtimes C_{2(p-1)}$.

**Proof.** Let $L' = K^{nr}(\mathrm{Jac}(X)[2])$, and consider the tower of field extensions $L/L'/K^{nr}$. Notice that $L'$ is the splitting field of $f$ over $K^{nr}$, by [1, Lemma 2.1].

For all $i$, $\alpha_i \in L'$, therefore $L$ is obtained from $L'$ by adjoining square roots of some elements of $L'$. So the Galois group of $L/L'$ is a direct product of some copies of $C_2$. However, it is a totally ramified extension since $L' \supseteq K^{nr}$, and it is tame since $p$ is odd, therefore it must be cyclic. So $L/L'$ can only be trivial or quadratic.

Now let us consider $L'/K^{nr}$. Since $f$ is irreducible over $K^{nr}$, we have that $\mathrm{Gal}(L'/K^{nr})$ has a cyclic subgroup of order $p$. Therefore $\mathrm{Gal}(L'/K^{nr})$ injects into $S_p$, the group of permutations on $p$

elements, and since $p$ divides $|S_p|$ exactly once, necessarily the $p$-Sylow subgroup of $\mathrm{Gal}(L'/K^{nr})$ is isomorphic to $C_p$. So, the wild inertia subgroup of $\mathrm{Gal}(L'/K^{nr})$ is isomorphic to $C_p$, and the quotient by $C_p$ is the Galois group of the maximal tamely ramified subextension of $L'/K^{nr}$, so it is cyclic. Now the image of it in $S_p$ is contained in the normaliser of $C_p$, that is equal to $C_p \rtimes C_{p-1}$. Therefore $\mathrm{Gal}(L'/K^{nr})$ injects into $C_p \rtimes C_{p-1}$.

Putting all this together, if $f$ is irreducible over $K^{nr}$ then $\mathrm{Gal}(L/K^{nr})$ has at most order $2p(p-1)$, with wild inertia subgroup of order $p$ and a cyclic quotient of order at most $2(p-1)$, corresponding to the maximal tame subextension. Since $L'/K^{nr}$ is an intermediate subextension with Galois group isomorphic to a subgroup of the Frobenius group $C_p \rtimes C_{p-1}$, this concludes the proof. ■

This lemma shows that, for a curve acquiring good reduction over a wildly ramified extension, the size of the image of inertia under $\rho_{J,\ell}$ is at most $2p(p-1)$. In fact equality can be achieved, and in this case we say that the curve has maximal inertia image. We now complete the proof of Proposition 6.1.

**Proof of Proposition 6.1** In Lemma 6.6, we proved that $|\rho_{J,\ell}(I_K)|$ divides $2p(p-1)$, and that (with the same notation used in the proof) $[L:L'] \leq 2$ and $[L':K^{nr}] \leq p(p-1)$. Clearly, the second inequality is an equality precisely when the Galois group of the splitting field of $f$ over $K^{nr}$ is $C_p \rtimes C_{p-1}$. Moreover, we have:

$$L = L'(\sqrt{\alpha_2 - \alpha_1}) = K(\alpha_1, \ldots, \alpha_p, \sqrt{\alpha_2 - \alpha_1}), \tag{6.9}$$

in fact at most one of the elements $\sqrt{\alpha_i - \alpha_j}$ is sufficient to generate $L$ over $L'$ and by Remark 6.5 any of these elements works as they all have the same valuation. More precisely, the extension $L/L'$ is quadratic if and only if $\alpha_2 - \alpha_1$ is not a square in $L'$, or equivalently it has odd valuation. We denote by $v_L$, $v_{L'}$ the normalised valuations on $L$ and $L'$ respectively. Then $v_L(\sqrt{\alpha_2 - \alpha_1}) = \frac{1}{2}[L:L']v_{L'}(\alpha_2 - \alpha_1)$ and since by definition $\Delta = \prod_{i>j}(\alpha_i - \alpha_j)^2$, we have:

$$v_L(\Delta) = \binom{p}{2} 2 v_L(\alpha_2 - \alpha_1) = \binom{p}{2} 4 v_L(\sqrt{\alpha_2 - \alpha_1}) = 2p(p-1) v_L(\sqrt{\alpha_2 - \alpha_1}); \tag{6.10}$$

on the other hand since the valuations on $K^{nr}$ and $K$ agree on the elements of $K$ we have $v_L(\Delta) = [L:K^{nr}]v(\Delta)$.

Suppose that $|\rho_\ell(I_K)| = 2p(p-1)$, so $[L:K^{nr}] = 2p(p-1)$. In particular, $[L:L'] = 2$ and by the observation above this means $v_{L'}(\alpha_2 - \alpha_1)$ is odd. Then simplifying from the equalities above we obtain that $v(\Delta) = v_L(\sqrt{\alpha_2 - \alpha_1}) = v_{L'}(\alpha_2 - \alpha_1)$ is odd and, as we already noted, $\mathrm{Gal}(L'/K^{nr}) \cong C_p \rtimes C_{p-1}$. Conversely suppose that $\mathrm{Gal}(L'/K^{nr}) \cong C_p \rtimes C_{p-1}$ and that $v(\Delta)$ is odd. Then comparing the two expressions for $v_L(\Delta)$ and using that $[L':K^{nr}] = p(p-1)$ we obtain

$$[L:L']v(\Delta) = 2 \cdot \frac{1}{2}[L:L']v_{L'}(\alpha_2 - \alpha_1), \tag{6.11}$$

so $v_{L'}(\alpha_2-\alpha_1)=v(\Delta)$ is odd, which implies $[L:L']=2$ and therefore $[L:K^{nr}]=2p(p-1)$.

We now prove that $\rho_\ell(I_K)\cong I$, where $I$ is as in Section 6.2. Let $F=K(\alpha_1,\dots,\alpha_p,\sqrt{\alpha_2-\alpha_1})$. The extension $F/K$ is totally ramified of degree $2p(p-1)$, since the ramification index is $2p(p-1)$ and since $[F:K]$ is at most $2p(p-1)$, again by the Proof of Lemma 6.6. The Galois closure of $F/K$ is given by $K(\{\sqrt{\alpha_i-\alpha_j}\}_{i\neq j})$. Therefore the inertia subgroup $I$ of the Galois group of this field over $K$ is isomorphic to $\mathrm{Gal}(L/K^{nr})$, hence to the image of inertia $\rho_{J,\ell}(I_K)$. This concludes the proof of Proposition 6.1. ■

To conclude this subsection, we prove Proposition 6.2.

**Proof of Proposition 6.2** We need to prove that if $f$ is irreducible over $K$ and $(v(\Delta),p-1)=1$ then $\mathrm{Gal}(L'/K^{nr})\cong C_p\rtimes C_{p-1}$, where $L'$ is as in the proofs of Lemma 6.6 and Proposition 6.1. We clearly also have that $v(\Delta)$ is odd since $p-1$ is even.

Let us denote by $M$ the splitting field of $f$ over $K$. First of all, since $f$ is irreducible over $K$ then $\mathrm{Gal}(M/K)$ contains a subgroup of order $p$. Moreover this subgroup is normal, in fact if we see it as a subgroup of $S_p$, it consists of all the $p$-cycles in $\mathrm{Gal}(M/K)$ and the conjugation of any $p$-cycle is a $p$-cycle.

Now consider the element $\Delta^{1/(p-1)}$. Using the expression of $\Delta$ in terms of the roots $\alpha_1,\dots,\alpha_p$ of $f$ and the fact that $\alpha_i-\alpha_j$ all have the same valuation, we can prove that $\Delta^{1/(p-1)}\in L'$. More precisely, we have

$$\Delta^{1/(p-1)}=(\alpha_2-\alpha_1)^p u^{1/(p-1)},\quad \text{where } u=\prod_{i>j}\left(\frac{\alpha_i-\alpha_j}{\alpha_2-\alpha_1}\right)^2; \tag{6.12}$$

note that $u$ is an element of $L'$ with valuation 0 and so its $(p-1)$-st root gives an unramified, hence trivial, extension of $L'$. Since $(v(\Delta),p-1)=1$, we also have that $[K^{nr}(\Delta^{1/(p-1)}):K^{nr}]=p-1$. Therefore $p-1$ divides both $[L':K^{nr}]$ and $[M:K]$. Now the inertia subgroup of $\mathrm{Gal}(M/K)$ is isomorphic to $\mathrm{Gal}(L'/K^{nr})$, and it is normal with cyclic quotient. Therefore it must contain the subgroup of $\mathrm{Gal}(M/K)$ isomorphic to $C_p$. This proves that $p,p-1\mid[L':K^{nr}]$ and as in the proof of Lemma 6.6 we conclude that $\mathrm{Gal}(L'/K^{nr})\cong C_p\rtimes C_{p-1}$. ■

### 6.3.2 The irreducible representations of the group $I$

We now fix a set of generators for $I$; let $\sigma$ be defined as in Section 6.2. The tame inertia is generated by an element $\tau$ such that $\{\sigma,\tau^2\}$ generates the Galois group of the splitting field of $f$, which is the Frobenius group $C_p\rtimes C_{p-1}$. So $I$ is presented as

$$I=\langle\sigma,\tau\,|\,\sigma^p=\tau^{2(p-1)}=1,\tau\sigma\tau^{-1}=\sigma^b\rangle, \tag{6.13}$$

for some $b$ coprime to $p$. The exact value of $b$ will not be relevant for the rest of the chapter. Finally, we denote by $\nu$ the element $\tau^{p-1}$; it generates the extra $C_2$ contained in $I$, and acts as:

$$\sqrt{\alpha_i-\alpha_j}\mapsto-\sqrt{\alpha_i-\alpha_j}. \tag{6.14}$$

Note that $\nu$ is the only element of the subgroup $C_{2(p-1)}$ of $I$ (except the identity) that commutes with $\sigma$.

We now want to describe the representation induced from $\rho_{J,\ell}$ on $I$. We claim that it is irreducible of dimension $p-1$ and faithful. We only have to prove that it is irreducible, since it is clearly faithful by the definition of $I$, and the dimension of $\rho_{J,\ell}$ (hence of the restriction to inertia) is $2g = p-1$. In order to do it, we make a digression on the irreducible representations of the group $I$.

The group $I$ is the semidirect product of two abelian groups, $A = C_p$ and $H = C_{2(p-1)}$, so we are in the setting of [20, §8.2]. Consider a set of representatives for the orbits of $H$ in the group of characters of $A$. We have that this set consists of two elements only, namely the trivial representation $\mathbf{1}$ and a non-trivial character $\eta$. Let $H_{\mathbf{1}}$ (resp. $H_\eta$) denote the subgroup of $H$ consisting of the elements that stabilise $\mathbf{1}$ (resp. $\eta$). Then $H_{\mathbf{1}} = H$ and $H_\eta = \langle \nu \rangle \cong C_2$. Now, for any irreducible representation $\xi$ of $H_\bullet$ we obtain a representation of $G$ given by $\mathrm{Ind}_{AH_\bullet}^{I} \bullet \otimes \xi$. By [20, §8.2, Proposition 25] the representations obtained in this way are exactly all the irreducible representations of $I$.

In particular, $I$ has $2(p-1)$ irreducible representations of dimension 1, corresponding to the $2(p-1)$ irreducible representations of $H_{\mathbf{1}} = H$, and two representations of dimension $[I : AH_\eta] = p-1$ corresponding to the two irreducible representations of $H_\eta \cong C_2$.

**Lemma 6.7.** *The restriction to inertia of the representation $\rho_{J,\ell}$ is irreducible.*

**Proof.** Suppose that $\rho_\ell\big|_{I_K}$ is reducible. Then, since it has dimension equal to $p-1$, it is the sum of $p-1$ one-dimensional representations, but in this case the image would be abelian. However, this representation factors through $I$ and is faithful as an $I$-representation, so since $I$ is non-abelian we have a contradiction. Therefore $\rho_{J,\ell}\big|_{I_K}$ must be irreducible. ■

Note that, as a consequence of this lemma, the representation $\rho_{J,\ell}$ is also irreducible.

We can furthermore identify $\rho_{J,\ell}\big|_{I_K}$ among these two $(p-1)$-dimensional irreducible representations. Since $H_\eta \cong C_2$, the representation $\xi$ needed for the construction described above is either the trivial representation of $H_\eta$, or the representation sgn, defined by $\mathrm{sgn}(\nu) = -1$. So we obtain the two representations $\mathrm{Ind}_{C_{2p}}^{I} \eta$ and $\mathrm{Ind}_{C_{2p}}^{I} \eta \otimes \mathrm{sgn}$.

- The representation $\mathrm{Ind}_{C_{2p}}^{I} \eta$ is not faithful. In fact, $\mathrm{tr}(\mathrm{Ind}_{C_{2p}}^{I} \eta)(1) = \mathrm{tr}(\mathrm{Ind}_{C_{2p}}^{I} \eta)(\nu) = p-1$.
- The representation $\mathrm{Ind}_{C_{2p}}^{I} \eta \otimes \mathrm{sgn}$ is faithful. In fact we have, for $s \in I$ and for $t_1, \ldots, t_{p-1}$ a set of representatives for $I/C_{2p}$:

$$\mathrm{tr}(\mathrm{Ind}_{C_{2p}}^{I} \eta \otimes \mathrm{sgn})(s) = \sum_{i : t_i s t_i^{-1} \in C_{2p}} \eta(t_i s t_i^{-1}) \mathrm{sgn}(s). \tag{6.15}$$

For the terms occurring in this sum (which are at most $p-1$) we have that $\eta(t_i s t_i^{-1})$ is some root of unity, and it is 1 if and only if $s = 1$. So for $s \neq 1$ we have a sum of at most $p-1$

roots of unity, different from 1, and therefore $\mathrm{tr}(\mathrm{Ind}_{C_{2p}}^{I}\,\eta\otimes\mathrm{sgn})(s)\neq p-1$, or equivalently the representation is faithful.

This proves the following.

**Lemma 6.8.** *The representation $\rho_{J,\ell}$ restricted to inertia factors through $I\cong C_p\rtimes C_{2(p-1)}$ and, as a representation of $I$, it is the unique irreducible faithful representation of dimension $p-1$.*

**Remark 6.9.** *By [11, §10, Theorem 10.1], we have an alternative description of the representation $\rho_{J,\ell}\big|_{I_K}$. Since the cluster picture of $X$ only contains the cluster $R$, we have that up to isomorphism of inertia modules, $\rho_{J,\ell}$ is given by*

$$\gamma\otimes(\mathbb{Q}_\ell[R]\ominus\mathbf{1}), \tag{6.16}$$

*where $\gamma$ is a certain character of order $2(p-1)$. More precisely, the isomorphism is with the first étale cohomology group, which as a Galois representation is dual to $\rho_{J,\ell}$. However, since the restriction to inertia has integer characters, the result is the same.*

## 6.4 The good model and the action of Frobenius

In this section we show that any hyperelliptic curve satisfying the hypotheses of Theorem 6.3 has a good model over the field $F$ defined in Section 6.2, that reduces to

$$y^2=x^p-x \tag{6.17}$$

on the residue field. We then prove that the action of Frobenius is diagonalisable, with eigenvalues:

- all equal to $\left(\left(\frac{-1}{p}\right)p\right)^{f_{K/\mathbb{Q}_p}/2}$, if $f_{K/\mathbb{Q}_p}$ is even;
- half equal to $\left(\left(\frac{-1}{p}\right)p\right)^{f_{K/\mathbb{Q}_p}/2}$ and half equal to $-\left(\left(\frac{-1}{p}\right)p\right)^{f_{K/\mathbb{Q}_p}/2}$, if $f_{K/\mathbb{Q}_p}$ is odd.

In particular we deduce that the full Galois action is completely determined by these data when $f_{K/\mathbb{Q}_p}$ is even.

As observed in Section 6.3, the extension $F/K$ is totally ramified, so the residue fields of $F$ and $K$ are both equal to $k$. Therefore we will identify the action of $\mathrm{Frob}_K$ with that of $\mathrm{Frob}_F$, which is well defined.

**Lemma 6.10.** *The base change of $X$ on $F$ has a model reducing to $y^2=x^p-x$ on $k$.*

**Proof.** Over $F$, we can define the following change of variables:

$$\begin{cases} x & \mapsto & (\alpha_2-\alpha_1)x+\alpha_1 \\ y & \mapsto & (\sqrt{\alpha_2-\alpha_1})^p\,y. \end{cases} \tag{6.18}$$

Then applying this change of variables to $X \times_K F$ we have the following equation:

$$y^2 = \prod_{1 \le i \le p} \left( x - \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1} \right). \tag{6.19}$$

Note that for each $i \in \{2, \dots, p\}$, we have

$$\alpha_i - \alpha_1 = \sum_{j=0}^{i-2} \sigma^j(\alpha_2 - \alpha_1)$$

and since $\sigma$ is a wild inertia element, $\dfrac{\sigma^j(\alpha_2 - \alpha_1)}{\alpha_2 - \alpha_1}$ reduces to 1 on $k$ (see Lemma 3.5), therefore the reduction of $\prod_{1 \le i \le p} \left( x - \dfrac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1} \right)$ is $\prod_{1 \le i \le p}(x - (i-1)) = x^p - x$. ■

**Remark 6.11.** *We know from the Criterion of Néron-Ogg-Shafarevich ([19, §2, Theorem 2(ii)]) that* $\mathrm{Jac}(X)$ *acquires good reduction over $F$; this lemma shows that the curve $X$ itself acquires good reduction over the same extension.*

Since $F/K$ is totally ramified of degree $2p(p-1)$, there is an intermediate extension $F'$ such that $F/F'$ is wild of degree $p$ and $F'/K$ is tame of degree $2(p-1)$. Hence there exists some uniformiser $\pi_K$ of $K$ such that a $2(p-1)$-th root of it generates $F'/K$. Now, since $K$ is a finite extension of $\mathbb{Q}_p$, it contains all the $(p-1)$-th roots of unity; moreover $K$ also contains a primitive $2(p-1)$-th root of unity if and only if the unramified part of the extension $K/\mathbb{Q}_p$ has even degree, i.e. if $f_{K/\mathbb{Q}_p}$ is even. Therefore the Galois closure of $F/K$ (which, as observed in Section 6.3, is equal to $K(\mathrm{Jac}(X)[4])$) is given by $F(\zeta_{2(p-1)})$, where $\zeta_{2(p-1)}$ is a primitive $2(p-1)$-th root of unity. In particular $F/K$ is Galois if and only if $f_{K/\mathbb{Q}_p}$ is even, and if it is odd then $[F(\zeta_{2(p-1)}) : F] = 2$.

We are now ready to compute $\rho_{J,\ell}(\mathrm{Frob}_F)$, hence $\rho_{J,\ell}(\mathrm{Frob}_K)$.

### 6.4.1 The action of Frobenius

Suppose first that $n = f_{K/\mathbb{Q}_p}$ is even. Then $\mathrm{Frob}_F$ is central in $\mathrm{Gal}(L/K)$ (recall $L = F^{nr}$), therefore $\rho_{J,\ell}(\mathrm{Frob}_F)$ is a scalar matrix. Let $\lambda \in \overline{\mathbb{Q}}_\ell$ be such that $\rho_{J,\ell}(\mathrm{Frob}_F) = \lambda \mathrm{Id}_{2g}$. Then we know $\det(\rho_{J,\ell}(\mathrm{Frob}_F)) = |k|^g = p^{ng}$ and so $\lambda^{2g} = p^{ng}$. On the other hand, since $\rho_{J,\ell}(\mathrm{Frob}_F)$ is a scalar matrix, then its characteristic polynomial is precisely $(T - \lambda)^{2g}$, and by [5, Theorem 1.6] it has integral coefficients, so $\lambda \in \mathbb{Z}$ and in particular $\lambda \in \{\pm p^{n/2}\}$. Finally, since $F/K$ is Galois, we have $F = K(\mathrm{Jac}(X)[4])$, so $\rho_{J,\ell}(\mathrm{Frob}_F)$ acts trivially modulo 4 and $\lambda \equiv 1 \pmod 4$. Hence

$$\lambda = \left( \left( \frac{-1}{p} \right) p \right)^{f_{K/\mathbb{Q}_p}/2}.$$

Suppose now that $n = f_{K/\mathbb{Q}_p}$ is odd. Assume for simplicity that $n = 1$, then for general $n$, $\rho_{J,\ell}(\mathrm{Frob}_F)$ acts as the $n$-th power of the linear operator we obtain for $n = 1$. Then the square of $\mathrm{Frob}_F$ is central in $\mathrm{Gal}(L/K)$, hence $\rho_{J,\ell}(\mathrm{Frob}_F)^2$ is of the form $\mu \mathrm{Id}_{2g}$. As a consequence of the Weil Conjectures (see again [5, Theorem 1.6]) we also have that the trace of $\rho_{J,\ell}(\mathrm{Frob}_F)$ is given

by $p+1-|\tilde{X}_F(\mathbb{F}_p)|$ where $\tilde{X}_F$ is the reduction modulo $p$ of $X\times_K F$. Since for each $x\in\mathbb{F}_p$, $x^p-x=0$, we have precisely $p$ affine points on $\tilde{X}_F$, so $\mathrm{tr}(\rho_{J,\ell}(\mathrm{Frob}_F))=0$. Therefore the characteristic polynomial of $\rho_{J,\ell}(\mathrm{Frob}_F)$ has $g$ roots equal to $\sqrt{\mu}$ and $g$ roots equal to $-\sqrt{\mu}$, hence it is $(T^2-\mu)^g$, and again it has constant term equal to $p^g$ and integer coefficients, hence $\mu\in\{\pm p\}$. As in the previous case, we have $\mu\equiv 1 \pmod 4$ and so $\mu=\left(\frac{-1}{p}\right)p$. Putting all this together, the eigenvalues of $\rho_{J,\ell}(\mathrm{Frob}_F)$ for generic odd $f_{K/\mathbb{Q}_p}$ are

$$\pm\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)^{f_{K/\mathbb{Q}_p}},$$

each occurring $g$ times.

Now we can prove Theorem 6.3 in the case of even $f_{K/\mathbb{Q}_p}$.

**Proof of Theorem 6.3 for even inertia degree.** Since $f_{K/\mathbb{Q}_p}$ is even, we know $F/K$ is Galois with Galois group isomorphic to its inertia subgroup. We furthermore have $\mathrm{Gal}(L/K)=\mathrm{Gal}(F/K)\times\mathrm{Gal}(K^{nr}/K)$, since $L=F^{nr}=FK^{nr}$. If we define $\chi$ as in the statement of Theorem 6.3 we have that $\rho_{J,\ell}(\mathrm{Frob}_K)=\chi(\mathrm{Frob}_K)\mathrm{Id}_{2g}$ and therefore if we let $\psi=\rho_{J,\ell}\otimes\chi^{-1}$, then $\psi$ factors through $\mathrm{Gal}(F/K)$, which is isomorphic to $I$, and as a representation of this group it is irreducible, faithful and $(p-1)$-dimensional. By Lemma 6.8, there exists a unique such representation. ■

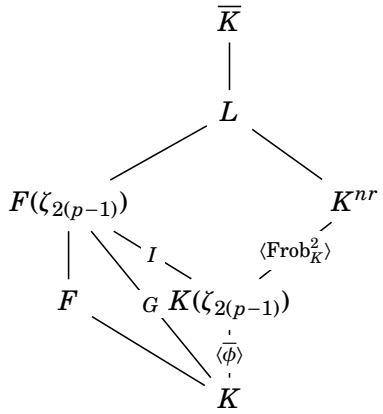
## 6.5 The case of odd inertia degree

In this final section, we complete the proof of Theorem 6.3 for the case when $f_{K/\mathbb{Q}_p}$ is odd, computing explicitly $\psi$.

Let $\chi$ be as in the statement of Theorem 6.3. Then we can fix a basis of $T_\ell\,\mathrm{Jac}(X)$ such that the matrix representing $\psi(\mathrm{Frob}_K)=\dfrac{1}{\chi(\mathrm{Frob}_K)}\rho_{J,\ell}(\mathrm{Frob}_K)$ in this basis is diagonal with the first $g$ coefficients equal to 1 and the last $g$ coefficients equal to $-1$. In particular $\psi(\mathrm{Frob}_K^2)=\mathrm{Id}_{2g}$ and so $\mathrm{Frob}_K^2\in\ker(\psi)$. Therefore we have that $\ker(\psi)=\mathrm{Gal}(\overline{K}/F(\zeta_{2(p-1)}))$ and so $\psi$ factors through $G=\mathrm{Gal}(F(\zeta_{2(p-1)})/K)$, and it is faithful as a representation of $G$. Now $G$ is generated by $I$ and the element $\phi$ defined in Section 6.2, with $G\cong I\rtimes\langle\phi\rangle$. Note that $\phi$ is the reduction of $\mathrm{Frob}_K$ modulo its square. The group $G$ has the following presentation:

$$G=\langle\sigma,\tau,\phi|\sigma^p=\tau^{2(p-1)}=\phi^2=1,\tau\sigma\tau^{-1}=\sigma^b,\sigma\phi=\phi\sigma,\phi\tau\phi=\tau^p\rangle. \tag{6.20}$$

In the diagram below we show the relations among the fields $K,K(\zeta_{2(p-1)}),F,F(\zeta_{2(p-1)}),L,\overline{K}$ and we highlight the relevant Galois groups (here $\overline{\phi}$ is the image of $\phi$ in $G/I$).




**Lemma 6.12.** *The group $G$ is isomorphic to a semidirect product*

$$C_p \rtimes (C_{2(p-1)} \rtimes C_2).$$

**Proof.** Since $\langle \phi \rangle \cong C_2$, we know that $G \cong (C_p \rtimes C_{2(p-1)}) \rtimes C_2$. Moreover the subgroup given by wild inertia is normal, so $G$ has a normal subgroup isomorphic to $C_p$. We only need to prove that $G$ also has a subgroup isomorphic to $C_{2(p-1)} \rtimes C_2$. The field $K(\alpha_1)$ is an intermediate extension of degree $p$ over $K$, and $\mathrm{Gal}(F(\zeta_{2(p-1)})/K(\alpha_1)) \cong C_{2(p-1)} \rtimes C_2$ is a subgroup of $G$. ■

In particular $G$ is of the form $A \rtimes H$, with $A$ abelian, as in [20, §8.2]. Again we can use Proposition 25 of op. cit. to describe the irreducible representations of $G$.

### 6.5.1 The irreducible representations of the group $G$

A set of representatives for the orbits of $H$ in the group of characters of $A$ consists, as in Section 6.3, only of the two elements $\mathbf{1}$ and $\eta$, for $\eta$ any non-trivial character. It is easy to check that, with the same notation as in Section 6.3, $H_{\mathbf{1}} = H$ and $H_\eta = \langle \phi, \nu \rangle \cong C_2^2$. All the representations of $H_{\mathbf{1}}$ give rise to a representation of $G$ of the same dimension. Now $H_{\mathbf{1}} \cong C_{2(p-1)} \rtimes C_2$ is itself a semidirect product of two abelian subgroups, so using Proposition 25 of [20] we have that all its irreducible representations have dimension dividing the order of the second subgroup, that is either 2 or 1. However, $\psi$ is irreducible of dimension $p-1$ (since $\rho_{J,\ell}$ is), so unless $p = 3$ it cannot arise from such a representation. For $p = 3$ we need a more direct approach, e.g. direct inspection of the character table of the group, but this case is already dealt with in Chapter 3, so we can assume $p \neq 3$.

Now let us consider the representations arising from $H_\eta$. Since this group is abelian, it only has 1-dimensional irreducible representations, namely those given by the following characters:

| class | $1$ | $\nu$ | $\phi$ | $\nu\phi$ |
|---|---|---|---|---|
| $\xi_1$ | 1 | 1 | 1 | 1 |
| $\xi_2$ | 1 | 1 | −1 | −1 |
| $\xi_3$ | 1 | −1 | 1 | −1 |
| $\xi_4$ | 1 | −1 | −1 | 1 |

The irreducible representations arising from these four representations are

$$\mathrm{Ind}_{C_p\times C_2^2}^G \xi_j \otimes \eta$$

for $j \in \{1,\dots,4\}$ (note that the subgroup of $G$ isomorphic to $C_p \rtimes C_2^2$ is in fact a direct product). In particular these representations have dimension equal to $[G : C_p \times C_2^2] = p-1$. Following the same proof as that of Lemma 6.8 we have that only the representations arising from $\xi_3$ and $\xi_4$ are faithful, so $\psi$ is one of these two.

Let $\sigma, \tau$ be the generators of $I$, as in Section 6.3. Before proving the following lemma, we fix $\eta$ such that $\eta(\sigma) = e^{2\pi i/p}$, seen as a complex number; this can be done since $\eta(\sigma)$ is a primitive $p$-th root of unity.

**Lemma 6.13.** *The representations $\psi_1 = \mathrm{Ind}_{C_p\times C_2^2}^G \xi_3 \otimes \eta$ and $\psi_2 = \mathrm{Ind}_{C_p\times C_2^2}^G \xi_4 \otimes \eta$ are such that* $\mathrm{tr}(\psi_1(\sigma\phi)) = -\mathrm{tr}(\psi_2(\sigma\phi)) = \sqrt{\left(\frac{-1}{p}\right)p}$.

**Proof.** First of all, it is easy to check that $C_p \times C_2^2$ is a normal subgroup of $G$. Moreover a set of representatives for $G/(C_p \times C_2^2)$ is given by $\tau, \tau^2, \dots, \tau^{p-1}$. We have

$$\mathrm{tr}(\psi_j(\sigma\phi)) = \sum_{i=1}^{p-1} (\xi_{j+2}\otimes\eta)(\tau^i\sigma\phi\tau^{-i}) = \sum_{i=1}^{p-1} \xi_{j+2}(\tau^i\phi\tau^{-i})\eta(\tau^i\sigma\tau^{-i}).$$

By the relation $\phi\tau\phi = \tau^p$ we deduce $\tau^2\phi = \phi\tau^2$; so if $i$ is even then $\xi_{j+2}(\tau^i\phi\tau^{-i}) = \xi_{j+2}(\phi)$, and if $i$ is odd then $\xi_{j+2}(\tau^i\phi\tau^{-i}) = \xi_{j+2}(\phi\nu) = -\xi_{j+2}(\phi)$ (recall that $\nu = \tau^{p-1}$). On the other hand, since $\tau\sigma\tau^{-1} = \sigma^b$, then $\eta(\tau^i\sigma\tau^{-i})$ varies among all the powers of $\eta(\sigma) = e^{2\pi i/p}$. Note that

$$\left(\frac{b^i}{p}\right) = (-1)^i = \frac{\xi_{j+2}(\tau^i\phi\tau^{-i})}{\xi_{j+2}(\phi)},$$

so $\mathrm{tr}\,\psi_j(\sigma\phi) = \sum_{i=1}^{p-1}(-1)^i\xi_{j+2}(\phi)\eta(\sigma)^{b^i} = \xi_{j+2}(\phi)\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)(e^{2\pi i/p})^a = \xi_{j+2}(\phi)\sqrt{\left(\frac{-1}{p}\right)p}$, where the last equality follows from Gauss' summation formula. ∎

### 6.5.2 The proof of Theorem 6.3

**Proof.** Let $\beta(x,y) = (x',y')$ be the change of variables described in the proof of Lemma 6.10, red the reduction map: $X(\overline{K}) \to \tilde{X}(\overline{k})$ and lift be any section of red. Then we can compute the action of a Galois automorphism $\gamma$ on the reduced curve $\tilde{X}(\overline{k})$ via the composition $\mathrm{red}\circ\beta^{-1}\circ\gamma\circ\beta\circ\mathrm{lift}$. In particular we will do it for $\gamma = \sigma\,\mathrm{Frob}_K$; then we have that

$$\mathrm{tr}(\rho_{J,\ell}(\sigma\,\mathrm{Frob}_K)) = |k| + 1 - A$$

where $A$ is the number of points on the reduced curve fixed by the map $\mathrm{red}\circ\beta\circ\sigma\,\mathrm{Frob}_K\circ\beta^{-1}\circ\mathrm{lift}$ constructed above (see [13, Theorem 1.5 and Remark 1.7] and [12, §6.5]).

Let $(\tilde{x},\tilde{y}) \in \tilde{X}(\overline{k})$, then since $\sigma$ is a wild inertia element we have

$$\begin{aligned}
(\tilde{x},\tilde{y}) &\xrightarrow{\text{lift}} (x,y) \xrightarrow{\beta} \left(x(\alpha_2-\alpha_1)+\alpha_1, y(\sqrt{\alpha_2-\alpha_1})^p\right) \\
&\xrightarrow{\sigma\,\mathrm{Frob}_K} \left(\sigma(\mathrm{Frob}_K(x))\sigma(\alpha_2-\alpha_1)+\alpha_2, \sigma(\mathrm{Frob}_K(y))(\sigma(\sqrt{\alpha_2-\alpha_1}))^p\right) \\
&\xrightarrow{\beta^{-1}} \left(\frac{\sigma(\mathrm{Frob}_K(x))\sigma(\alpha_2-\alpha_1)+\alpha_2-\alpha_1}{\alpha_2-\alpha_1}, \sigma(\mathrm{Frob}_K(y))\frac{(\sigma(\sqrt{\alpha_2-\alpha_1}))^p}{(\sqrt{\alpha_2-\alpha_1})^p}\right) \\
&= \left(\sigma(\mathrm{Frob}_K(x))\frac{\sigma(\alpha_2-\alpha_1)}{\alpha_2-\alpha_1}+1, \sigma(\mathrm{Frob}_K(y))\frac{(\sigma(\sqrt{\alpha_2-\alpha_1}))^p}{(\sqrt{\alpha_2-\alpha_1})^p}\right) \xrightarrow{\text{red}} \left(\tilde{x}^{|k|}+1, \tilde{y}^{|k|}\right).
\end{aligned} \tag{6.21}$$

Here we use the facts that for every $x$ in the ring of integers of $F$, $x$ and $\sigma(x)$ reduce to the same element of $\overline{k}$ as $\sigma \in I_K$, and furthermore since $\sigma$ is wild, if $x \neq 0$ we also have that $\sigma(x)/x$ reduces to 1 (by Lemma 3.5), and finally by definition $\mathrm{Frob}_K(x)$ reduces to $\tilde{x}^{|k|}$. Then $A$ is equal to the number of solutions (including the point at infinity) of the following system of equations:

$$\begin{cases} x &= x^{|k|}+1 \\ y &= y^{|k|} \\ y^2 &= x^p - x; \end{cases} \tag{6.22}$$

As in Section 6.4.1, let $n = f_{K/\mathbb{Q}_p}$, so $|k| = p^n$. If $n = 1$, then this system has 0 affine solutions if $p \equiv 3 \pmod 4$ and $2p$ affine solutions if $p \equiv 1 \pmod 4$, so $A = 1$ or $2p+1$ respectively. Therefore

$$\mathrm{tr}(\rho_{J,\ell}(\sigma\,\mathrm{Frob}_K)) = -\left(\frac{-1}{p}\right)p, \tag{6.23}$$

$$\text{and so } \mathrm{tr}(\psi(\sigma\phi)) = \frac{\mathrm{tr}(\rho_{J,\ell}(\sigma\,\mathrm{Frob}_K))}{\chi(\mathrm{Frob}_K)} = \frac{-\left(\frac{-1}{p}\right)p}{\sqrt{\left(\frac{-1}{p}\right)p}} = -\sqrt{\left(\frac{-1}{p}\right)p}.$$

For general odd $n$, we obtain the same system of equations independently on the curve $X$ we use, as long as it is defined over a $p$-adic field $K$ with $f_{K/\mathbb{Q}_p} = n$ and it satisfies the conditions of Theorem 6.3. Let $X/\mathbb{Q}_p : y^2 = x^p - p$ as in Remark 6.4, and let $X_K$ be the base change of $X$ to the field $K$ equal to the unique unramified extension of $\mathbb{Q}_p$ of degree $n$. The polynomial $x^p - p$ is irreducible over $K$, as any root gives a ramified extension, and the valuation of $\Delta$ on $\mathbb{Q}_p$, and hence $K$, is $2p-1$, coprime to $p-1$. Let $\rho'_{J,\ell}$ be the $\ell$-adic Galois representation attached to $\mathrm{Jac}(X)$ and let $\rho_{J,\ell}$ be the $\ell$-adic Galois representation attached to $\mathrm{Jac}(X_K)$; then:

- the restriction to the inertia subgroups of the two representations $\rho'_{J,\ell}$ and $\rho_{J,\ell}$ coincide;
- $\rho_{J,\ell}(\mathrm{Frob}_K)$ acts as the $n$-th power of $\rho'_{J,\ell}(\mathrm{Frob}_{\mathbb{Q}_p})$.

So $\rho_{J,\ell}(\sigma)\rho_{J,\ell}(\mathrm{Frob}_K) = \rho'_{J,\ell}(\sigma)\rho'_{J,\ell}(\mathrm{Frob}_{\mathbb{Q}_p})^n$. Notice that, by Section 6.4.1, since $n-1$ is even, we have that $\rho'_{J,\ell}(\mathrm{Frob}_{\mathbb{Q}_p})^{n-1}$ is the scalar matrix with eigenvalue $\left(\left(\frac{-1}{p}\right)p\right)^{(n-1)/2}$. Therefore

$$\mathrm{tr}(\rho_{J,\ell}(\sigma\,\mathrm{Frob}_K)) = \left(\left(\frac{-1}{p}\right)p\right)^{(n-1)/2} \mathrm{tr}(\rho'_{J,\ell}(\sigma\,\mathrm{Frob}_{\mathbb{Q}_p})) = -\left(\left(\frac{-1}{p}\right)p\right)^{(n+1)/2}.$$

We can now conclude, since $\operatorname{tr}(\psi(\sigma\phi)) = \dfrac{\operatorname{tr}(\rho_{J,\ell}(\sigma\,\mathrm{Frob}_K))}{\chi(\mathrm{Frob}_K)} = \dfrac{-\left(\left(\frac{-1}{p}\right)p\right)^{(n+1)/2}}{\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)^n} = -\sqrt{\left(\frac{-1}{p}\right)p}$. ■

## 6.6 Applications and examples

In this section we present a few examples and applications of Theorem 6.3 and of the tools used throughout the chapter.

- By the computation made in Section 6.5.2, we find the number $A-1$ of affine solutions of the system (6.22), which is

  $$A - 1 = |k| - \operatorname{tr}(\rho_{J,\ell}(\sigma\,\mathrm{Frob}_K)) = p^n + \left(\left(\frac{-1}{p}\right)p\right)^{(n+1)/2}. \tag{6.24}$$

  This result is analogous to Lemma 3.7.

- We can express the representation $\psi$ given in Theorem 6.3 in terms of the characters introduced in Section 6.5.1. With the same notation, we have that

  $$\psi = \psi_2 = \mathrm{Ind}_{C_p \times C_2^2}^{G} \xi_4 \otimes \eta.$$

  A few examples are the following:

  - For $p = 5$, the group $I$ is isomorphic to $C_5 \rtimes C_8$ in [7]. The restriction of $\rho_{J,\ell}$ to inertia is given by $\rho_{10}$. For odd $f_{K/\mathbb{Q}_p}$, we have $G \cong C_2^2 \cdot F_5$ in [7], with $\psi = \rho_{13}$ (here the class denoted $10A$ is the one generated by $\sigma\phi$).
  - For $p = 7$, $I \cong C_7 \rtimes C_{12}$ and the corresponding representation is $\rho_{14}$. For odd $f_{K/\mathbb{Q}_p}$, we have $G \cong \mathrm{Dic}_7 \rtimes C_6$ with $\psi = \rho_{18}$ (here the class $14A$ is the one generated by $\sigma\phi$).

# BIBLIOGRAPHY


[1] G. Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. **77** (2001) 241–246.

[2] N. Coppola, *Wild Galois Representations: elliptic curves over a 3-adic field*, Acta Arithmetica **195**(3) (2020) 289–303.

[3] N. Coppola, *Wild Galois Representations: elliptic curves over a 2-adic field with non-abelian inertia action*, International Journal of Number Theory **16**(6) (2020) 1199–1208.

[4] N. Coppola, *Wild Galois representations: a family of hyperelliptic curves with large inertia image*, arXiv e-prints (2020) arxiv:2001.08287.

[5] P. Deligne, *La conjecture de Weil : I*, Publications Mathématiques de l'IHÉS, **43** (1974) 273–307.

[6] L. Dembélé, N. Freitas and J. Voight, *On Galois inertial types of elliptic curves over* $\mathbb{Q}_\ell$, preprint.

[7] T. Dokchitser *Group names*, (groupnames.org).

[8] T. Dokchitser, *Ranks of elliptic curves in cubic extensions*, Acta Arithmetica **126**(4) (2007) 357–360.

[9] T. Dokchitser and V. Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bulletin of the London Mathematical Society **40**(3) (2008) 516–524.

[10] T. Dokchitser and V. Dokchitser, *Euler factors determine local Weil representations*, in: Journal für die reine und angewandte Mathematik, (2016) (717) 35–46.

[11] T. Dokchitser, V. Dokchitser, C. Maistret and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, arXiv e-prints (2018) arxiv:1808.02936.

[12] T. Dokchitser and V. Dokchitser, *Quotients of hyperelliptic curves and etale cohomology*, Quaterly J. Math. **69**(2) (2018), 747–768.

[13] T. Dokchitser, V. Dokchitser and A. Morgan, *Tate module and bad reduction*, Proc. Amer. Math. Soc. (to appear).

[14] N. Freitas and A. Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Memoirs of AMS (to appear).

[15] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, in: Manuscripta mathematica, (1990) 69(4) 353–385.

[16] J. Milne, *Jacobian Varieties, Arithmetic Geometry* §7, (Springer, New York, 1986) 167–212.

[17] W. Robson, *Connections between torsion points of elliptic curves and reduction over local fields*, (unpublished MSc thesis, University of Bristol, 2017).

[18] D. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Centre de Recherque Mathématiques, CRM Proceedings and Lecture notes, (1994) Vol. 4.

[19] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics, (1968) 88(3) 492–517.

[20] J.P. Serre, *Linear Representations of Finite Groups*, (1997) Springer-Verlag, New York.

[21] J.-P. Serre, *Local Fields*, (1995) Springer-Verlag New York.

[22] J.-P. Serre, *Abelian $\ell$-adic representations and elliptic curves*, Research Notes in Mathematics, (1998) Vol 7. Peters.

[23] J.H. Silverman, *The arithmetic of elliptic curves*, (Springer-Verlag, New York, Graduate Texts in Mathematics **106** 1986).

[24] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, (1994) Graduate texts in mathematics, Springer-Verlag.

[25] J. Yelton, *An abelian subextension of the dyadic division field of a hyperelliptic Jacobian*, Mathematica Slovaca **69**(2) (2019) 357–370.