Coppola, N. (2020). Wild Galois representations: elliptic curves over a 2-adic field with non-abelian inertia action. *International Journal of Number Theory*. https://doi.org/10.1142/S179304212050061X

International Journal of Number Theory

Wild Galois representations: elliptic curves over a 2-adic field with non-abelian inertia action

Nirvana Coppola*
School of Mathematics, University of Bristol, Fry Building, University Walk, Bristol, BS8 1UG, United Kingdom
nc17051@bristol.ac.uk

Received
Accepted

In this paper we present a description of the ℓ-adic Galois representation attached to an elliptic curve defined over a 2-adic field K, in the case where the image of inertia is non-abelian. There are two possibilities for the image of inertia, namely Q_8 and $\mathrm{SL}_2(\mathbb{F}_3)$, and in each case we need to distinguish whether the inertia degree of K over $\mathbb{Q}_2$ is even or odd. The result presented here are being implemented in an algorithm to compute explicitly the Galois representation in these four cases.

Keywords: Elliptic curves, local fields, wild ramification, Galois representations

Mathematics Subject Classification 2010: 11G07, 11F80

1. Introduction

Let K be a 2-adic field (i.e. a finite extension of $\mathbb{Q}_2$ or, equivalently, a non-archimedean local field with characteristic 0 and residue characteristic 2) 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 $n = [k : \mathbb{F}_2]$, i.e. n is the inertia degree of K. Suppose that E/K has potential good reduction, that is it has additive reduction and there exists a finite extension of K where E acquires good reduction.

Let $\overline{K}$ be a fixed algebraic closure of K and let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K, which acts on the points of $E(\overline{K})$. This induces a representation ρ on the ℓ-adic Tate module $T_\ell(E)$, which is independent of the prime ℓ as long as $\ell \neq 2$, in the sense of [8, §2 Theorem 2.ii].

More precisely we will denote by ρ_ℓ or simply ρ the following representation:

$$G_K \longrightarrow Aut(T_\ell(E) \otimes \overline{\mathbb{Q}}_\ell),$$

*University of Bristol

which is a 2-dimensional representation over $\overline{\mathbb{Q}}_\ell$, so after fixing a basis for $T_\ell(E)\otimes\overline{\mathbb{Q}}_\ell$ we can identify $Aut(T_\ell(E)\otimes\overline{\mathbb{Q}}_\ell)$ with $\mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$. Let us consider the restriction of ρ to the inertia subgroup $I_K \cong \mathrm{Gal}(\overline{K}/K^{nr})$ of G_K (here K^{nr} is the maximal unramified extension of K). If L is the minimal extension of K^{nr} where E acquires good reduction, which exists by [8, §2 Corollary 3], then $\ker(\rho) = \mathrm{Gal}(\overline{K}/L)$ and the image of inertia is isomorphic to $\mathrm{Gal}(L/K^{nr})$, as a consequence of the Criterion of Néron-Ogg-Shafarevich (see [9, VII §7 Theorem 7.1]). Moreover, it is proved in [6, Theorems 2,3] that the image of inertia can only be one of the following:

$$C_2, C_3, C_4, C_6, Q_8, \mathrm{SL}_2(\mathbb{F}_3). \tag{1.1}$$

For a more explicit approach, see also [5, Part IV §11,12]. In this paper we focus on the cases where I is non-abelian (equivalently non-cyclic), hence it is either Q_8 or $\mathrm{SL}_2(\mathbb{F}_3)$. In [6, Theorem 3], there is a criterion to check whether this holds.

Recall that the quotient G_K/I_K is isomorphic to the absolute Galois group of the residue field, which is pro-cyclic and generated by the Frobenius element, that acts as $x \mapsto x^q$ where $q = |k|$. We call an Arithmetic Frobenius of K, and denote it by Frob_K, any fixed choice of an element of G_K that reduces to the Frobenius element modulo I_K. In order to compute explicitly the elements in the image of ρ, 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 [4] 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 1.1. *Let E/K be an elliptic curve with potential good reduction over a 2-adic field, let ℓ be a prime different from 2 and let $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ be the ℓ-adic Galois representation attached to E. Suppose that $I = \rho(I_K)$ is non-abelian. Let Δ be the discriminant of a (not necessarily minimal) equation for E and let n be the inertia degree of $K/\mathbb{Q}_2$. Then ρ factors as*

$$\rho = \chi \otimes \psi \tag{1.2}$$

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

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

class	1	2	4A	4B	4C
size	1	1	2	2	2
ψ	2	−2	0	0	0

- *If n is even and Δ is not a cube in K, then ψ 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
ψ	2	−2	−1	−1	0	1	1

  Moreover the image of inertia is Q_8 if Δ is a cube in K^{nr} and $\mathrm{SL}_2(\mathbb{F}_3)$ otherwise.
- *If n is odd and Δ is a cube in K (equivalently the image of inertia is Q_8), then ψ 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
ψ	2	−2	0	0	0	$\sqrt{-2}$	$-\sqrt{-2}$

- *If n is odd and Δ is not a cube in K (equivalently the image of inertia is $\mathrm{SL}_2(\mathbb{F}_3)$), then ψ 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
ψ	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 3.5).

This theorem is almost completely proved in [3, §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 ψ 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 ψ. In this work we prove that, with the definition of χ made in the statement of Theorem 1.1, only one of the two possible cases occur for elliptic curves. The method of proof consists of describing explicitly a generator of the class $8A$ and computing the trace of ψ on it.

2. The good model

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

Lemma 2.1. *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 Δ 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 λ_P be the slope of the tangent line at P. Then after applying the change of coordinates

$$\begin{cases} x \mapsto x + x_P \\ y \mapsto y + \lambda_P x + y_P \end{cases} \tag{2.1}$$

we get an equation for E over F with the same discriminant Δ, of the form

$$y^2 + Axy + By = x^3, \tag{2.2}$$

with $B \neq 0$ (for a detailed computation see [7, §2, Proposition 2.22 and Corollary 2.23]).

Next we prove that $\sqrt[3]{B} \in F$. Note that the discriminant of equation (2.2) is given by

$$\Delta = -27B^4 + (AB)^3; \tag{2.3}$$

since Δ and $-B^3$ are cubes in F, we have that also $27B - A^3 = 27B\big(1 - \frac{A^3}{27B}\big)$ 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 $z^3 - \big(1 - \frac{A^3}{27B}\big)$ has a root in F.

We know by [8, §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 [8], 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 [9, 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 $v_F\big(\frac{A^3}{27B}\big) \leq 0$, or equivalently $3v_F(A) \leq v(B)$. By direct computation,

$$j = \frac{A^3(A^3 - 24B)^3}{B^3(A^3 - 27B)} \tag{2.4}$$

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

$$v_F(j) \leq 12v_F(A) - 3(v_F(B) + v_F(A)) = 3(3v_F(A) - v_F(B)) \leq 0, \tag{2.5}$$

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.

$$\begin{cases} x \mapsto \big(\sqrt[3]{B}\big)^2 x \\ y \mapsto \big(\sqrt[3]{B}\big)^3 y \end{cases} \tag{2.6}$$

After applying this transformation to the curve (2.2), we get the model $y^2 + A'xy + y = x^3$, with $A' = A/\sqrt[3]{B}$. By the computation above, $v_F(A) > v_F(B)/3$,

so $v_F(A') > 0$ and the valuation of the discriminant is $v_F(-27B^4 + (AB)^3) - 12v_F(\sqrt[3]{B}) = 0$. 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, λ_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 [2, Theorem 1]):

$$\gamma(t) = t^8 + 18a_4t^4 + 108a_6t^2 - 27a_4^2. \tag{2.7}$$

If λ_P is a root of γ, 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 extension then by [8, §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 Δ, which by an easy computation can be expressed in terms of these coordinates, so $F^{nr} \subseteq L$ (see [7, §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 $\ker(\rho) = \mathrm{Gal}(\overline{K}/L)$ 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 γ defined above is irreducible over K^{nr}.

There are several cases to consider:

- if Δ is a cube in K, then the degree of F/K is exactly 8;
- if Δ is a cube in K^{nr} but not in K, then $[L : K^{nr}] = 8$ and $[F : K] = 24$;
- if Δ 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 ζ_3 is a primitive 3-rd 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 Δ is a cube in K^{nr} but not in K, otherwise the extension $K(\sqrt[3]{\Delta}, \zeta_3)$ would be unramified and not cyclic.

3. Proof of the main theorem

We will use the same notation as in Section 2. Since I is non-abelian, then the group $\mathrm{Gal}(L/K)$ is also non-abelian. By [3, §2 Lemma 1], the representation ρ factors as

$\chi \otimes \psi$, where χ is the following character:

$$\chi : G_K \to \overline{\mathbb{Q}}_\ell^\times \tag{3.1}$$

$$\mathrm{Frob}_K \mapsto \sqrt{-2}^n; \tag{3.2}$$

$$I_K \mapsto 1, \tag{3.3}$$

and $\psi : G_K \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ 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, ψ is irreducible and faithful, and it is given by $\psi(g) = \dfrac{1}{\chi(g)}\rho(g)$. The definition of χ is suggested by the following lemma.

Lemma 3.1. *Let* Frob_F *be the Arithmetic Frobenius of* F*; then the eigenvalues of* $\rho(\mathrm{Frob}_F)$ *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. Suppose that $f_{F/\mathbb{Q}_2} = 1$. By Lemma 2.1 we can compute the trace of Frob_F via point-counting on the reduced curve $y^2 + y = x^3$, getting

$$\mathrm{tr}(\rho(\mathrm{Frob}_F)) = |k| + 1 - |\tilde{E}_F(k)| = 2 + 1 - 3 = 0. \tag{3.4}$$

Then by [9, V §2 Proposition 2.3], the characteristic polynomial of $\rho(\mathrm{Frob}_F)$ is

$$T^2 + 2, \tag{3.5}$$

with roots $\pm\sqrt{-2}$. For general $f_{F/\mathbb{Q}_2}$, the eigenvalues of $\rho(\mathrm{Frob}_F)$ are the $f_{F/\mathbb{Q}_2}$-th powers of the roots of the polynomial above, hence for odd $f_{F/\mathbb{Q}_2}$ we get $\sqrt{-2}^{f_{F/\mathbb{Q}_2}}$, $-\sqrt{-2}^{f_{F/\mathbb{Q}_2}}$, and for even n there is only one double eigenvalue $(-2)^{f_{F/\mathbb{Q}_2}/2}$. □

We have that for even n, $F(\zeta_3) = F$ and so Frob_F is central in the group $\mathrm{Gal}(L/K)$, so it acts as a scalar matrix, with eigenvalue given by Lemma 3.1. Moreover, for any n, if $\sqrt[3]{\Delta} \notin K^{nr} \setminus K$, then F and K have the same residue field and so $f_{F/\mathbb{Q}_2} = n$; in this case $\rho(\mathrm{Frob}_K) = \rho(\mathrm{Frob}_F)$. Otherwise, the unramified part of the extension F/K is given by $\sqrt[3]{\Delta}$ and therefore has degree 3, so $f_{F/\mathbb{Q}_2} = 3n$. In particular $\rho(\mathrm{Frob}_F) = \rho(\mathrm{Frob}_K)^3$.

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

Theorem 3.2. *If* K *is a* 2*-adic field with even inertia degree* n *over* $\mathbb{Q}_2$*, then Theorem 1.1 is true for any elliptic curve* E/K *with potential good reduction such that the image of inertia under* ρ *is non-abelian and* $\sqrt[3]{\Delta} \notin K^{nr} \setminus K$*.*

Proof. Since n is even, G is equal to its inertia subgroup since either $\sqrt[3]{\Delta} \in K$ or $\sqrt[3]{\Delta} \notin K^{nr}$. As noticed above, Frob_K acts as the multiplication by a scalar with eigenvalue $(-2)^{n/2} = \chi(\mathrm{Frob}_K)$, therefore ψ is given by the representation ρ 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 [8, §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 [4], we deduce that each of these groups only has one such representation, the one given in the statement. □

For the case $\sqrt[3]{\Delta} \in K^{nr} \setminus K$, 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 ψ, getting a result surprisingly similar to the one in Theorem 3.2.

Theorem 3.3. *If K is a 2-adic field with even inertia degree over $\mathbb{Q}_2$ and E is an elliptic curve with potential good reduction over K such that the image of inertia under ρ is non-abelian and $\sqrt[3]{\Delta} \in K^{nr} \setminus K$, then Theorem 1.1 holds for E.*

Proof. The difference between G and its inertia subgroup is determined by 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 3.2.

Recall that χ 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 $\rho(\mathrm{Frob}_F) = \rho(\mathrm{Frob}_K)^3$, therefore using the relation $\rho = \chi \otimes \psi$ and the fact that $\rho(\mathrm{Frob}_F)$ is a scalar:

$$(-2)^{3n/2} id = ((-2)^{n/2}\psi(\mathrm{Frob}_K))^3; \tag{3.6}$$

so the eigenvalues of $\psi(\mathrm{Frob}_K)$ are 3-rd roots of unity (not necessarily primitive) in $\overline{\mathbb{Q}}_\ell$; moreover the order of $\psi(\mathrm{Frob}_K)$ is exactly 3 since ψ 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 3-rd roots of unity, with trace -1. Hence the representation ψ 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 ψ is an irreducible faithful representation of dimension 2 of G, which is either SD_{16} if Δ is a cube in K, or $\mathrm{GL}_2(\mathbb{F}_3)$ otherwise. Again by looking at the character tables of these two groups on [4], we obtain two possible such representations, both of which extend the representation of inertia described in the proof of Theorem 3.2. 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 subgroup of G, so we may assume for simplicity that the whole group is SD_{16}. If $G = \mathrm{GL}_2(\mathbb{F}_3)$ the wild 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 σ 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 σ 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 ϕ of order 2; applying the same construction, we see that ϕ acts as Frobenius on the reduced curve. Now fix $\ell = 3$ and consider the representation $\overline{\rho}$ which is the 3-adic representation modulo 3. This is the Galois representation induced by ρ on $E[3]$; after fixing a basis $\{P, Q\}$ for $E[3]$ as a $\mathbb{F}_3$-vector space, $\overline{\rho}$ takes values in $\mathrm{GL}_2(\mathbb{F}_3)$. In [7, §4 Figure 4.2] there is a visual interpretation of this action. Note that 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 ψ.

Lemma 3.4. *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 2.1. 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:

$$(0,0), (0,1), (\overline{\zeta_3}, \overline{\zeta_3}), (\overline{\zeta_3}, \overline{\zeta_3}^2), (1, \overline{\zeta_3}), (1, \overline{\zeta_3}^2) \text{ and } (\overline{\zeta_3}^2, \overline{\zeta_3}), (\overline{\zeta_3}^2, \overline{\zeta_3}^2), \tag{3.7}$$

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

After applying the change of coordinates described in Lemma 2.1, 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 $\overline{\rho}$, 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 3.5. *If K is a 2-adic field with odd inertia degree n over $\mathbb{Q}_2$, then Theorem 1.1 is true for any elliptic curve E/K with potential good reduction such that the image of inertia under ρ is non-abelian.*

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

$$P \mapsto Q - P \tag{3.8}$$

$$Q \mapsto P + Q. \tag{3.9}$$

It exists since Q_8 is contained in the image of inertia under $\overline{\rho}$, therefore every element of $\mathrm{GL}_2(\mathbb{F}_3)$ with determinant 1 and 2-power order is in the image of inertia. Then $\overline{\rho}(\sigma)$ 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 $\operatorname{tr}\psi(\phi\sigma)$, we determine the irreducible representation ψ. To compute this trace, we look at the trace of $\rho(\mathrm{Frob}_K\,\sigma)$. Let a be the reduction of $\rho(\mathrm{Frob}_K\,\sigma)$ modulo 3. Then $a = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$, with trace 1. This means that $\operatorname{tr}(\rho(\mathrm{Frob}_K\,\sigma)) \equiv 1 \pmod 3$. 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 [4]).

By looking at the character table of the group SD_{16} in [4], we deduce that $\operatorname{tr}\psi(\phi\sigma)$ is either $\sqrt{-2}$ or $-\sqrt{-2}$, so

$$\operatorname{tr}\rho(\mathrm{Frob}_K\,\sigma) = \chi(\mathrm{Frob}_K)\operatorname{tr}(\psi(\phi\sigma)) \in \{\sqrt{-2}^n \cdot (\pm\sqrt{-2})\}. \tag{3.10}$$

Only one of this two numbers is congruent to 1 modulo 3, namely the one we obtain if $\operatorname{tr}\psi(\phi\sigma) = +\sqrt{-2}$. Therefore we have the following character for ψ (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			ϕ			$\phi\sigma$	$\phi\sigma^{-1}$
ψ	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 ψ:

class	1	2A	2B	3	4	6	8A	8B
size	1	1	12	8	6	8	6	6
generator			ϕ				$\phi\sigma$	$\phi\sigma^{-1}$
ψ	2	−2	0	−1	0	1	$\sqrt{-2}$	$-\sqrt{-2}$

as stated. □

4. Notes on the implementation

As explained in [1], the representation described here is the dual of the representation on the étale cohomology of E. In particular the function GaloisRepresentation implemented in MAGMA computes the Galois representation on the étale cohomology. Concretely, the two only differ by the character value of ψ on the elements of the two conjugacy classes $8A$ and $8B$. The function is currently being improved implementing the result presented here.

Theorem 1.1 and Theorems 3.1 and 3.2 of [1] give a method to describe completely the ℓ-adic Galois representation of an elliptic curve with potential good reduction and non-abelian inertia action.

Acknowledgments

The author thanks her supervisor Tim Dokchitser for the useful conversations and corrections. This work was supported by EPSRC.

Bibliography

[1] N. Coppola, Wild Galois representations: Elliptic curves over a 3-adic field, *arXiv e-prints* (2018) arXiv:1812.05651.
[2] T. Dokchitser, Ranks of elliptic curves in cubic extensions, *Acta Arithmetica* **126**(4) (2007) 357–360.
[3] 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.
[4] T. Dokchitser Group names, (groupnames.org).
[5] N. Freitas and A. Kraus, On the symplectic type of isomorphisms of the p-torsion of elliptic curves, *Memoirs of AMS* (to appear)
[6] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, *Manuscripta mathematica* **69**(4) (1990) 353–386.
[7] W. Robson, Connections between torsion points of elliptic curves and reduction over local fields, (unpublished MSc thesis, University of Bristol, 2017).
[8] J.P. Serre and J. Tate, Good reduction of abelian varieties, *Annals of Mathematics* **88**(3) (1968) 492–517.
[9] J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, Graduate Texts in Mathematics **106** (1986).